UiT
NORGES ARKTISKE UNIVERSITET

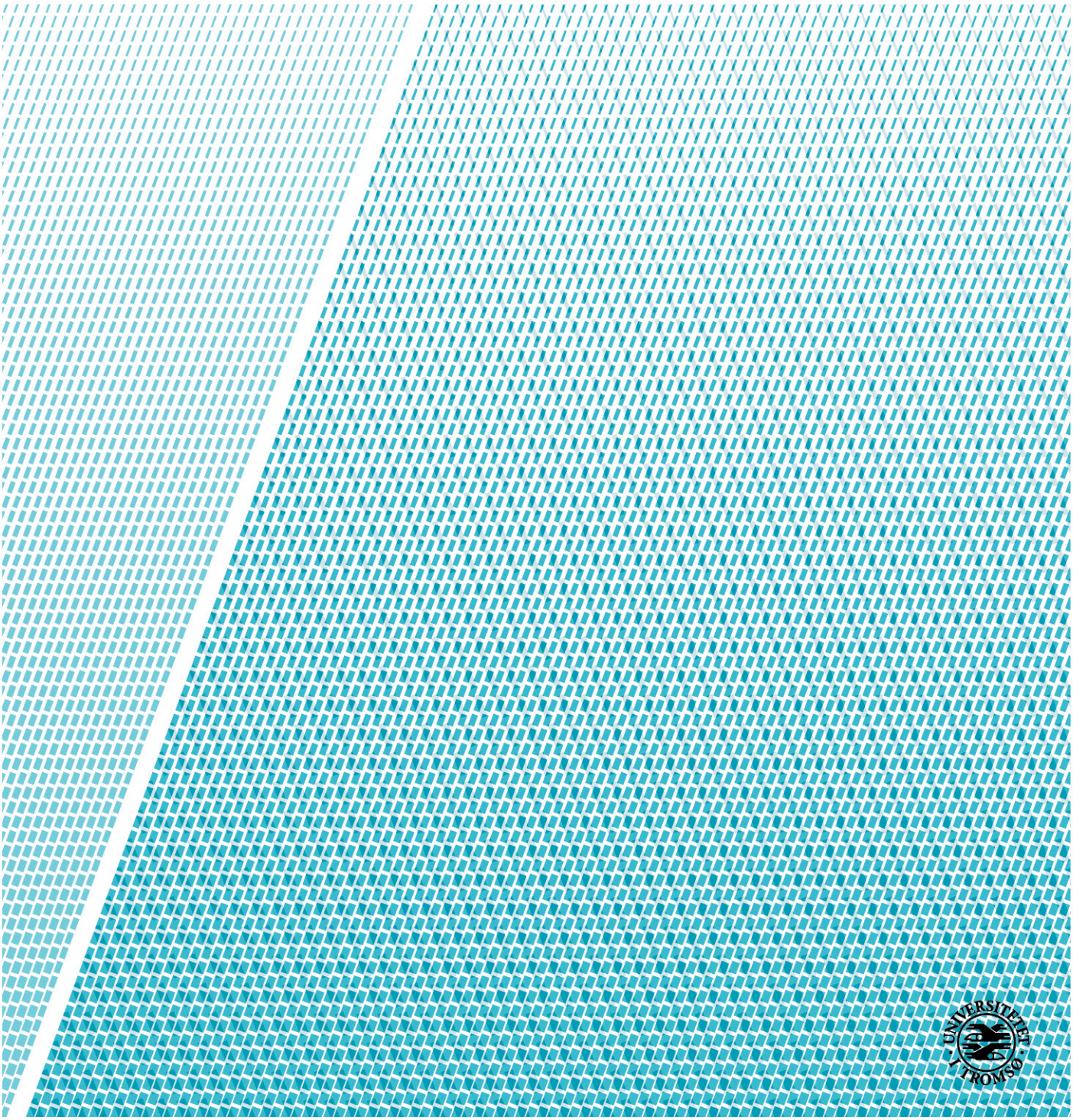
Det juridiske fakultet

Politiets adgang til å benytte dataavlesning i etterforskingsøyemed

—

Camilla Toften

Liten masteroppgave i rettsvitenskap høst 2018



Innholdsfortegnelse

Tiden er moden for å tilpasse lovgivningen til teknologien og gjeldende trusselbilde.

- *Benedicte Bjørnland* (PST-sjef, Aftenposten, 2016)

1 Innledning

1.1 Tema og problemstilling

Temaet for denne avhandlingen er dataavlesning. Dataavlesning er en metode og et tvangsmiddel som gir politiet adgang til opplysninger i et datasystem uten at personen som bruker datasystemet vet om det. Det er altså et svært inngripende tvangsmiddel, og politiets adgang til å benytte det er og må være snever. I denne avhandlingen er målet å klarlegge hvilken adgang politiet har til å benytte dataavlesning i etterforskingsøyemed slik dette er regulert i straffeprosessloven (heretter strpl.) §§ 216 o og 216 p.[1]

Denne avhandlingen omhandler kun dataavlesning i etterforskingsøyemed etter strpl. §§ 216 o og 216 p. Dataavlesning i forebyggende øyemed etter politiloven § 17 d skal ikke behandles. I forbyggende øyemed er poenget *å forhindre* at en fremtidig straffbar handling blir utført, mens i etterforskingsøyemed er poenget dataavlesningen *å avklare* om det er begått en straffbar handling i fortiden.

Reglene om dataavlesning ble tilføyd ved lov 17. juni 2016 nr. 54, og trådte i kraft 9. september 2016. Dataavlesning er derfor et relativt nytt begrep i norsk rett. Det er ikke et entydig juridisk begrep, eller en klar avgrenset teknologisk fremgangsmåte.[2] Kjernen i begrepet «dataavlesning» er imidlertid at det er en fremgangsmåte som brukes for å innhente informasjon i et datasystem.[3] Et eksempel på dataavlesning er bruk av såkalt "trojanere". Dette innebærer at en spesiell programvare plasseres inn i mistenktes datasystem, og gir politiet tilgang til vedkommendes kommunikasjon, lagret informasjon og andre opplysninger som fremkommer ved bruk av datasystemet.[4]

---

[1] Lov av 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker straffeprosessloven.
[2] Prop. 68 L (2015-2016) side 224.
[3] Prop. 68 L (2015-2016) side 224.
[4] Prop. 68 L (2015-2016) side 12.

Et annet eksempel på hvordan dataavlesning kan utføres, er ved såkalt "key-logging" som innebærer at tastetrykkene på et tastatur registreres.[5] Andre eksempler på dataavlesning er etablering av signalstrøm mellom tilkoblet skjerm og datautstyret, avlesning av data i fysiske og virtuelle minneområder, og lydstrøm som sendes ut fra en tilknyttet mikrofon til operativsystemets drivere.[6] Dette er bare noen eksempler. Å beskrive alle de ulike variantene av dataavlesning i detalj er ikke bare tidkrevende, men en opplisting kan også bli misvisende, fordi den teknologiske utviklingen skjer så raskt og at den fort kan bli utdatert.[7]

Dataavlesning tilhører kategorien "*skjulte tvangsmidler"* som er et samlebegrep for lovregulerte politimetoder som brukes uten at den metodebruken retter seg mot kjenner til det.[8] Andre skjulte tvangsmidler er ransaking,[9] utleveringspålegg, beslag med utsatt underretning,[10] kommunikasjonsavlytting og annen kommunikasjonskontroll,[11] sikringspålegg,[12] romavlytting, skjult kameraovervåking og teknisk sporing.[13] De ulovfestede politimetodene spaning, bruk av informanter, infiltrasjon og provaksjon omfattes også av uttrykket skjulte tvangsmidler.[14] Politiet benytter skjulte tvangsmidler for å finne informasjon og avdekke og/eller bevise et straffbart forhold. Et klart skille mellom skjulte tvangsmidler og andre vanlige tvangsmidler er at prinsippet om at den som rammes skal informeres ikke ivaretas. Dataavlesning gir politiet tilgang til store mengder personlig informasjon uten at personen som rammes kan kontrollere eller forhindre at det skjer.[15]

Av de skjulte tvangsmidlene er dataavlesning et av de klart mest inngripende.[16] Det er særlig "key-logging" som har skapt debatt. "Key-logging" innebærer at det installeres utstyr på PC som leser all informasjon som går fra tastaturet til datamaskinen, uavhengig av om det lagres eller ei.[17] Ved denne bruken av dataavlesning vil, som påpekt av Datatilsynet, "tanker,

---

[5] Prop. 68 L (2015-2016) side 247.
[6] Flere måter dataavlesning kan gjennomføres på er beskrevet på side 224 i forarbeidene Prop.68 L (2015-2016).
[7] Prop. 68 L (2015-2016) side 247.
[8] Se kapittel 16 d i straffeprosessloven og i lov av 4.august 1995 nr. 53 (politiloven) og NOU 2009: 15 s. 21.
[9] Ransaking etter strpl. § 200 a foretas uten at mistenkte (eller andre) får underretning om det, og tilhører derfor kategorien skjulte tvangsmidler.
[10] Strpl. kapittel 15 og 16.
[11] Strpl. kapittel 16a.
[12] Strpl. kapittel 16a.
[13] Strpl. §§ 216 m, 202 a, 202 b og 202 c.
[14] Ot.prp. nr. 60 (2004-2005) side 45 og Bruce og Haugland (2018) side 15.
[15] Bruce og Haugland (2018) side 17.
[16] Prop. 68 L (2015-2016) side 243 og Bruce og Haugland (2018) side 17.
[17] Prop. 68 L (2015-2016) side 247.

assossiasjoner og ønsker som kanskje engang aldri var tenkt kommunisert til noen andre blir gjenstand for politiets behandling".[18]

Dataavlesning gir altså politiet en mulighet til å overvåke hvert steg en mistenkt foretar på den enhet som blir avlest. Dette kan virke svært inngripende og kontroversielt. Ved bruk av dataavlesning vil det gjøres inngrep i mistenktes rett til privatliv, som er vernet av både Grunnloven § 102 og EMK artikkel 8.[19] Et krav om hjemmel i lov eller ved forskrift med hjemmel i lov gjelder også generelt ved all form for integritetsinngrep. Dette følger av det alminnelige legalitetsprinsippet som er etablert ved konstitusjonell sedvanerett, og som nå kommer til uttrykk i Grunnloven § 113.

Skjult dataavlesning fra politiets side står i kontrast til enkeltindividers grunnleggende rett til respekt for privatlivet. Alle mennesker har i utgangspunktet rett til et privatliv, men av hensyn til behovet for effektiv kriminalitetsbekjempelse vil denne rettigheten i noen tilfeller kunne innskrenkes. Det handler om å finne et balansepunkt hvor skjult tvangsmiddelbruk kan rettferdiggjøres. I dette balansepunktet er hensynene til kriminalitetsbekjempelse, personvern og rettssikkerhet sentrale. Disse hensynene vil redegjøres nærmere for underveis i avhandlingen.

En av utfordringene politiet stod ovenfor før dataavlesning ble innført som selvstendig tvangsmiddel, var krypteringer. Dataavlesning løser flere av de utfordringene politiet hadde med krypteringer før det ble innført som selvstendig tvangsmiddel. Ved innføringen av dataavlesning som tvangsmiddel ble det eksplisitt uttrykt i forarbeidene at adgangen til bruk ikke skal overgå det som er nødvendig for å møte behovet for effektiv kriminalitetsbekjempelse.[20]

I en rettsstat er det viktig at borgerne har tillit til staten, at kriminalitet bekjempes og at personvern og rettsikkerhet beskyttes. Det kan være vanskelig å bekjempe kriminalitet på en effektiv måte, og samtidig ivareta personvern og rettsikkerhet til den som er mistenkt for å ha begått den kriminelle handlingen. Borgerne ønsker at kriminalitet bekjempes, men kan miste tillit til staten hvis virkemidlene blir for inngripende. Staten må derfor ha et balansert bruk av

---

[18] Prop. 68 L (2015-2016) side 252.
[19] Lov av 17. Mai 1814 Kongeriket Norges Grunnlov og Europarådets konvensjon 4. november 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter (heretter forkortet EMK).

[20] Prop. 68 L (2015-2016) side 258.

virkemidler for å bekjempe kriminalitet, som ikke går for langt inn i borgernes frihetsfølelse. Dette er et viktig aspekt å ha med seg i den videre fremstillingen.[21]

1.2 Bakgrunn og aktualitet

Det ble brukt lang tid på å utforme reglene for bruk av dataavlesning som nå utgjør straffeprosessloven §§ 216 o og 216 p. Første gang spørsmålet om behovet for dataavlesning ble tatt opp var i Lund-utvalget i NOU 2003:18, senere ble spørsmålet fulgt opp i NOU 2004:6, NOU 2007:2 og til slutt i NOU 2009:15 før man i Prop. 68 L (2015-2016) fastslo å innføre dataavlesning som et selvstendig straffeprosessuelt tvangsmiddel. De vanskelige problemstillingene angående personvern og vern av privatlivet var hovedgrunner til at lovgivningsprosessen tok lang tid.

Den raske teknologiske utviklingen i samfunnet har imidlertid gitt oss nye måter å opprette og sende informasjon på. Kryptering av informasjon er en metode som brukes for å skjule informasjon slik at bare den som har autorisasjon kan avsløre innholdet. Dette var en av flere grunner som gjorde at flere instanser, slik som politiet og Kripos,[22] ønsket å innføre dataavlesning som tvangsmiddel. De erfarte at mye informasjon som de egentlig hadde rettslig adgang til gjennom tvangsmidlene kommunikasjonsavlytting og hemmelig ransaking ikke var tilgjengelig, fordi informasjonen var blitt skjult gjennom kryptering. Et annet eksempel er at det blir laget en e-post konto hvor flere har tilgang og informasjonen lagres kun på denne uten å sendes, slik at informasjonen blir utvekslet på den måten. Dette medfører at informasjonen ikke kan bli fanget opp ved bruk av for eksempel kommunikasjonsavlytting, selv om det utvilsomt er en form for kommunikasjon.[23]

Selv om dataavlesning er et forholdsvis nytt tvangsmiddel, er det ikke slik at dette tvangsmiddelet gir politiet tilgang til vesentlig mer informasjon, dersom man sammenligner med den informasjonen politiet hadde tilgang til før dataavlesning ble innført. For eksempel gir bestemmelsene om ransaking og beslag politiet tilgang til personlige notater i form av skriftlige dagbøker.[24]

---

[21] Bruce og Haugland (2018) side 32 og 33.
[22] Prop. 68 L (2015-2016) side 249.
[23] Prop. 68 L (2015-2016) side 260.
[24] Prop. 68 L (2015-2016) side 265.

Dataavlesning har foreløpig ikke blitt benyttet i særlig stor grad. I årsrapport for 2017 fra Kontrollutvalget for kommunikasjonskontroll ble det bare rapportert om én sak hvor dataavlesning har vært benyttet. Til sammenligning ble tvangsmiddelet kommunikasjonskontroll benyttet i 160 saker.[25] I samme rapport fremkommer det at dataavlesning er et nytt og inngripende tvangsmiddel, og at det er usikkert hvilket omfang bruken vil få over tid.[26] Til tross for at dataavlesning til nå ikke har blitt benyttet i særlig grad, er utfordringer ved bruk av tvangsmiddelet viktig å se nærmere på. I 2018 fikk Norge blant annet nye personvernregler som er begrunnet med viktigheten av at personopplysninger ikke skal misbrukes på grunn av vernet om privatliv.[27]

1.3 Metode

Formålet med avhandlingen er, som nevnt innledningsvis, å klarlegge innholdet i de reglene som regulerer politiets adgang til å benytte dataavlesning i etterforskingsøyemed. Avhandlingen er derfor av rettsdogmatisk karakter. Det skal avklares hva gjeldende rett er når det kommer til dette spørsmålet, og dette løses på bakgrunn av alminnelige rettskildelære.[28]

Det finnes per dags dato ingen tilgjengelig rettspraksis angående strpl. §§ 216 o og 216 p.[29] Analysen av reglene om dataavlesning vil derfor bero på ordlyd, forarbeider, juridisk litteratur, reelle hensyn samt rettspraksis angående andre bestemmelser om skjulte tvangsmidler som kan brukes som støtteargumenter.

---

[25] Kontrollutvalget for kommunikasjonskontroll, Årsrapport 2017 side 12.
[26] Kontrollutvalget for kommunikasjonskontroll, Årsrapport 2017, side 21.
[27] Jf. personvernopplysningsloven og https://www.forbrukerradet.no/siste-nytt/dette-betyr-de-nye-personvernreglene-for-deg/ (sist sett 09.12.18)
[28] Rettskildelæren angir normer for hvordan rettsanvendere skal løse rettslige spørsmål. Det finnes flere ulike fremstillinger angående rettskildelæren, men i denne avhandlingen er det i hovedsak benyttet læren fra Eckhoff (2001) og Nygaard (2004).
[29] Per dags dato er: 22.02.19.

2 Dataavlesning i etterforskingsøyemed

2.1 Etterforsking vs. forebygging

Etterforsking er en viktig del av politiets oppgaver jf. politiloven § 2 nr. 3. Reglene for politiets etterforsking av straffbare forhold reguleres av straffeprosessloven. Kapittel 18 i straffeprosessloven tar for seg de generelle reglene for etterforsking, og etter strpl. § 224 følger det at:

> *"Etterforsking foretas når det som følge av anmeldelse eller andre omstendigheter er rimelig grunn til å undersøke om det foreligger straffbart forhold som forfølges av det offentlige."*

Ved etterforsking skal det skaffes opplysninger som kan avklare om det er begått et straffbart forhold, og i all hovedsak foregår etterforsking *etter* en straffbar handling eventuelt er begått.[30]

Forskjellen mellom at politiet jobber med etterforskingen av saken, i motsetning til i forebyggende øyemed, er blant annet at det er PST som utfører arbeidet. Dette er fordi PST er spesialisert til å håndtere slike saker.

2.2 Objektet for dataavlesning

Objektet for dataavlesningen er et «datasystem» og i forarbeidene til strpl. § 216 o fremkommer det at «datasystem» skal forstås som enhver innretning bestående av maskinvare og data, som foretar behandling av data ved hjelp av dataprogrammer.[31] Eksempler på dette kan være smarttelefoner, datamaskiner og andre anlegg for elektronisk kommunikasjon som foretar behandling av data ved hjelp av dataprogrammer. Begrepet «datasystem» ble valgt fordi det er teknologinøytralt og vil kunne endre betydning i tråd med den teknologiske utviklingen.[32]

I strpl. § 216 o fjerde ledd henvises det også til "*brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester"* som også er objektet for dataavlesning. Forskjellen mellom dette og et "datasystem" er at brukerkontoer er ikke bundet til en bestemt enhet, men

[30] Ot.prp. nr. 60 (2004-2005) side 34.
[31] Prop. 68 L (2015-2016) side 270.
[32] Prop. 68 L (2015-2016) side 270.

kan benyttes på flere forskjellige datasystemer. En naturlig språklig forståelse av ordlyden tilsier at det er snakk om tjenester som kan knyttes til en tjeneste med brukernavn og passord, eksempelvis nettverkstjenester som e-post, Facebook, Skype eller skylagringstjenester. I forarbeidene er det beskrevet som "et virtuelt avgrenset område som er identifisert med brukernavn og som kan brukes fra hvilket som helst datasystem med nødvendig nettverksforbindelse og programvare".[33] Grunnen til at dette også utgjør objektet for dataavlesning er at den mistenkte kan benytte seg av en slik tjeneste på datasystem som er utenfor politiets kontroll, for eksempel flere forskjellige datasystem på offentlige steder.[34]

2.3 Bestemte datasystemer

Det følger videre av strpl. § 216 o fjerde ledd at det kun er "*bestemte datasystemer eller brukerkontoer (...)"* som den mistenkte besitter eller kan antas å ville bruke som kan avleses. Ordlyden "bestemt" tilsier at det må kunne pekes nøyaktig på hvilket objekt som skal avleses.

I forarbeidene fremkommer det at ordlyden "*bestemte*" innebærer at det er et krav om at det datasystemet som skal avleses må identifiseres i politiets begjæring, i rettens kjennelse eller i en eventuell hastebeslutning.[35] Denne identifiseringen må være så presis som mulig slik at det ikke skal være tvil om hvilket datasystem som kan avleses.[36] Eksempler på slik identifikasjon er IMEInummeret dersom datasystemet er en mobiltelefon,[37] brukernavn dersom det er en brukerkonto, eller en e-postadresse om det er en e-postkonto. Slik identifisering kan også være opplysning om utstyrets fabrikat eller hvor utstyret befinner seg geografisk og hvilken person som har rådighet over utstyret.[38]

2.4 "Besitter eller kan antas å ville bruke"

Dataavlesning kan videre kun rettes mot datasystemer eller brukerkontoer som den mistenkte "*besitter eller kan antas å ville bruke*". Begrepet "besitter" byr neppe på særlig tvil da det tilsier at vedkommende eier eller har datasystemet eller brukerkontoen i hende. Når det gjelder uttrykket "bruke" sikter det til direkte bruk av eksempelvis datamaskin, smarttelefon

[33] Prop. 68 L (2015-2016) side 270.
[34] Prop. 68 L (2015-2016) side 270.
[35] Se mer om dette i avhandlingens kapittel 4.
[36] Prop. 68 L (2015-2016) side 270.
[37] IMEI står for International Mobile Equipment Identity og kan kalles for mobiltelefonens fingeravtrykk jf. https://www.tek.no/artikler/dette_er_imei-koden/7597 (sist sett 22.02.19)
[38] Prop. 68 L (2015-2016) side 270.

osv.[39] Dette innebærer at all informasjonen som er lagret på datamaskinen lokalt eller et annet sted avleses. Det som derimot ikke er lov, er å foreta direkte avlesning av servere hos tjenesteleverandører som vedkommende bare indirekte gjør bruk av.[40]

Terskelen for når vedkommende "kan antas" å ville bruke datasystemet/brukerkontoen kan være noe problematisk. Ordlyden er vag og kan i prinsippet innebære alle mulige datasystemer det er sannsynlig at en person kan bruke. Det er åpenbart en for lav terskel. I forarbeidene er det lagt til grunn at det, på bakgrunn av objektive kriterier må konstateres en viss sannsynlighet for at mistenkte vil bruke datasystemet eller brukerkontoen som ønskes avlest. Det kreves ikke sannsynlighetsovervekt, men det må være objektive holdepunkter for at mistenkte vil bruke datasystemet, og rene formodninger er ikke tilstrekkelig.[41] Forarbeidene viser også til at tilsvarende formulering er brukt når det gjelder kommunikasjonsavlytting etter strpl. § 216 a tredje ledd, og at kriteriet skal forstås på samme måte når det gjelder dataavlesning.[42] Av Rt. 2006 s.1546 følger det at selv om en telefon ble brukt av en tredjemann ga ikke det grunnlag for at kommunikasjonskontroll kunne benyttes i foreliggende sak.

[39] Prop. 68 L (2015-2016) side 270 og 271.
[40] Prop. 68 L (2015-2016) side 270 og 271.
[41] Prop. 68 L (2015-2016) side 271.
[42] Prop. 68 L (2015-2016) side 270.

3 Vilkår for å benytte dataavlesning

3.1 Ulike typer vilkår

Vilkårene for å kunne benytte dataavlesning er regulert i strpl. §§ 216 o av (i noen grad) 216 p, som er teknisk og relativt omfattende bestemmelser. Vilkårene er i stor grad samme type som for øvrige straffeprosessuelle tvangsmidler. Det er strenge vilkår for å benytte skjulte tvangsmidler. Det gjelder et såkalt "mistankekrav", "kriminalitetskrav", et "forholdsmessighetskrav", et "indikasjons og subsidiaritetskrav", et "kompetansekrav", og et krav om domstolskontroll. I det følgende skal det redegjøres for disse.

3.2 Mistankekravet

Mistankekravet går, som begrepet tilsier, ut på at det kreves en viss mistanke for at en person har gjort eller forsøkt å gjøre en handling som er ulovlig. Kravet finnes for alle de ulike tvangsmidlene etter loven, men graden av mistanke som kreves er ulik etter hvor inngripende tvangsmiddelet ansees. Det kreves "*skjellig grunn*" til mistanke for å benytte dataavlesning etter strpl. § 216 o, som er veldig inngripende, mens til sammenligning det kun kreves "rimelig grunn" til mistanke for å avlytte samtaler med tekniske midler etter strpl. § 216 l som ansees som mindre inngripende.

Begrepet "skjellig grunn" skal forstås på samme måte som ellers i straffeprosessloven.[43] Som allerede antydet ligger det noe mer i en "skjellig" grunn enn i en "rimelig" grunn. Det følger av Rt.1993 s.1302 at det skal "*være mer sannsynlig at siktede har begått den straffbare handling saken gjelder enn at han ikke har det*".[44] Dette blir omtalt som et krav om sannsynlighetsovervekt,[45] og omfatter i utgangspunktet alle straffbarhetsvilkårene.[46] Det følger imidlertid av § 216 o annet ledd at dataavlesning kan brukes til tross for at personen er utilregnelig eller under den kriminelle lavalder.

---

[43]Prop. 68 L (2015-2016) side 283.
[44] Avgjørelsens side 1303. Se også Rt. 2011 s. 946 avsnitt 13.
[45] Rt. 2004 s.887 (avsnitt 11 og 12) og Rt. 2006 s.582 (avsnitt 19).
[46] Etter norsk strafferett er det fire grunnleggende vilkår som må være oppfylt for å straffes. For det første må den objektive gjerningsbeskrivelsen i et straffebud være overtrådt. Videre må gjerningspersonen har utvist tilstrekkelig subjektiv skyld i gjerningsøyeblikket. Gjerningspersonen må også inneha strafferettslig skyldevne (tilregnelighet) i gjerningsøyeblikket. Til sist er det et vilkår om at straffrihetsgrunner må være fraværende.

3.3 Kriminalitetskravet

Videre er det et krav til hvilke straffbare handlinger mistanken må knytte seg til for at dataavlesning kan iverksettes.[47] Vilkåret blir ofte omtalt som «kriminalitetskravet» eller «strafferammekravet», og fremkommer i strpl. § 216 o første ledd bokstav a og b.[48] Handlingen eller forsøket på handlingen må være av den type kriminalitet som omtales i bokstav a eller b.

Bokstav a retter seg mot lovbrudd som "*kan medføre fengsel i ti år eller mer*". Strafferammen for lovbruddet er ti år eller mer, men dette betyr ikke at lovbruddet *må* føre til fengsel i ti år eller mer ved endelig dom. For eksempel er strafferammen inntil 15 år fengsel *"for den som forsettlig eller grovt uaktsomt forurenser luft, vann eller grunn slik at livsmiljøet i et område blir betydelig skadet eller trues av slik skade"* etter straffeloven § 240. Her er strafferammekravet inntil 15 år. Strafferammekravet for bruk av dataavlesning i etterforskingsøyemed er dermed oppfylt. I den rettspraksis som foreligger angående denne bestemmelsen, har imidlertid alle blitt idømt vesentlig mindre straff (3 år eller mindre).[49] Så lenge lovbruddet har en strafferamme på ti år eller mer, er kriminalitetskravet oppfylt.

I strpl. § 216 o, bokstav b er det opplistet spesifikke lovbrudd i form av konkrete paragrafhenvisninger. Blant de lovbruddene som fremkommer i bokstav b er for eksempel lovbrudd mot statens selvstendighet og sikkerhet, avsløring av statshemmeligheter, deltagelse i voldelig sammenslutning med mer. Disse lovbruddene kan medføre etterforskningsmessige utfordringer, som gjør at det er tillatt å bruke skjulte tvangsmidler også for de. Sakstypene som dekkes av bokstav b er ofte knyttet til virksomhet som er godt organisert og er gjort på måter som er vanskelig å avdekke. Dette gjelder særlig saker som menneskesmugling, menneskehandel og overgrepsbilder av barn. Ved slike saker er det også slik at den fornærmede i saken sjelden har evne eller vilje til å bidra til oppklaring.[50]

Kriminalitetskravet er omtrent det samme som for bestemmelsene om kommunikasjonskontroll og hemmelig ransaking, og er i forarbeidene begrunnet med at innføringen av dataavlesning skulle kompensere for at disse metodene har mistet noe av

[47] Prop. 68 L (2015-2016) side 267.
[48] Prop. 68 L (2015-2016) side 42.
[49] Se for eksempel HR-2016-1857-A.
[50] Prop. 68 L (2015-2016) side 268.

effekten sin på grunn av den teknologiske utviklingen.[51] Videre er det begrunnet med at graden av inngrep ved bruk av dataavlesning er omtrent det samme som ved bruk av kommunikasjonskontroll og hemmelig ransaking, og også at dataavlesning kan fremstå enda mer inngripende enn disse to. Et lavere strafferammekrav var derfor ikke aktuelt.[52]

I Prop. 68 L (2015-2016) ble det gjort utvidelser i hvilke lovbrudd som kan gi grunnlag for bruk av skjulte tvangsmidler. Det ble åpnet for bruk av skjulte tvangsmidler ved skjellig grunn til mistanke om overtredelse av straffeloven § 136 om oppfordring, rekruttering og opplæring til terror (straffeloven 1902 § 147 c), § 254 om frihetsberøvelse (straffeloven 1902 § 223), § 311 om overgrepsbilder av barn (straffeloven 1902 § 204 a) og § 257 om menneskehandel (straffeloven 1902 § 224), samt utlendingsloven § 108 femte ledd om grov menneskesmugling.[53] Begrunnelsen var alvorligheten av slike handlinger, og på grunn av vanskeligheter med å skaffe bevis. Alle de straffbare handlingene som ble tilføyd er også lovbrudd som er blitt mer aktuelle de senere årene, og er blitt mye omtalt i media. Dette er nok også med på å gjøre terskelen for å gripe inn lavere. Tilføyelsen av reglene om oppfordring, rekruttering og opplæring til terror som lovbrudd etter bokstav b, kom på bakgrunn kom på bakgrunn av høringsnotat 12. juli 2012 om kriminalisering av forberedelse til terror, organisert kriminalitet og utvidet adgang til tvangsmiddelbruk. Dette var en direkte følge av terrorangrepene 22.juli 2011 på regjeringskvartalet og Utøya. Utvidelsen av åpningen av bruk av skjulte tvangsmidler må derfor sees i sammenheng med det økte trusselbildet.

3.4 Indikasjons- og subsidiaritetskrav

3.4.1 Generelt

Videre følger det av strpl. § 216 o tredje ledd at tillatelse til dataavlesning bare kan gis dersom det for det første: ”*må antas at dataavlesning vil være av vesentlig betydning for å oppklare saken*”. Dette blir gjerne kalt for ”indikasjonskravet”. For det andre kreves det at ”*oppklaring ellers i vesentlig grad bli vanskeliggjort*”. Dette blir gjerne kalt for subsidiaritetskravet. Kravene skal forstås på samme måte som tilsvarende uttrykk i §§ 200 a annet ledd (hemmelig ransaking), 216 c første ledd (kommunikasjonskontroll) og 216 m

[51] Prop. 68 L (2015-2016) side 267.
[52] Prop. 68 L (2015-2016) side 268.
[53] Prop. 68 L (2015-2016) side 268-269 jf. punkt 7.4 (side 94 og utover).

tredje ledd (romavlytting).[54] Derfor er forarbeider, rettspraksis og andre relevante rettskildefaktorer knyttet til disse bestemmelsene, relevante ved redegjørelsen av kravene. Indikasjonskravet og subsidiaritetskravet kommer i tillegg til forholdsmessighetskravet i strpl. § 170 a,[55] og kan sees på som et utslag av et mer overordnet nødvendighetskrav.[56] I ordlyden ligger det implisitt et krav om at bruken av dataavlesning må være nødvendig. En viktig forutsetning for politiets adgang til skjult tvangsmiddelbruk, er at dette ikke benyttes i større grad enn det er behov for.[57]

3.4.2 Nærmere om indikasjonskravet

Det første kravet som fremkommer i strpl. § 216 o tredje ledd er altså det såkalte indikasjonskravet. Ordlyden "*må antas*" innebærer ifølge forarbeidene at det må være en viss grad av sannsynlighet for at dataavlesning vil gi opplysninger. Det er likevel lagt opp til en vurdering fra sak til sak, der graden av sannsynlighet kan variere.[58] I noen tilfeller vil det kreves sannsynlighetsovervekt for at dataavlesningen vil føre til opplysninger som gir mer oppklaring av saken, mens i andre tilfeller kan det være nok med en realistisk mulighet for et slikt bidrag.[59] Det fremkommer ikke opplysninger i forarbeidene for hva denne variasjonen innebærer i praksis. Her vil nok alvorligheten av lovbruddet som er begått være av betydning. Jo mer alvorlig et lovbrudd er, jo mindre sannsynlig kan det være at dataavlesningen faktisk vil gi opplysninger.

I tillegg må det sees på hvor "vesentlig" opplysningene vil bidra til oppklaring av saken. Ordlyden "vesentlig" tilsier at bidraget må være av en viss betydning, og gir en relativt høy terskel for hvilke opplysninger som hører inn under begrepet. Det kan ikke være bagatellmessige opplysninger, men opplysninger som faktisk fører til en fremgang i saken. [60]

3.4.3 Nærmere om subsidiaritetskravet

Subsidiaritetskravet innebærer at dataavlesning ikke skal benyttes dersom samme resultat må antas å kunne oppnås ved mindre inngripende tiltak. Dette kalles gjerne "minste inngreps

---

[54] Prop. 68 L (2015-2015) side 269.
[55] Se avhandlingens punkt 3.5.
[56] Bruce (2018) side 260 og 261.
[57] Bruce (2018) side 25.
[58] Ot. prp. Nr. 60 (2004-2005) side 70.
[59] Ot. prp. Nr. 60 (2004-2005) side 71.
[60] Prop. 68 L (2015-2015) side 88.

prinsipp".[61] Poenget er at det må fastslås at det er et reelt behov for å benytte dataavlesning. Dersom opplysninger som søkes innhentet ved hjelp av dataavlesning kan innhentes på en mindre integritetskrenkende måte, skal ikke dataavlesning benyttes.[62] Ved å ta dette inn som et eget krav, markeres betydningen av at et tvangsmiddel kun skal tillattes dersom andre måter ikke vil føre frem.[63] Dette markerer også betydningen av at alle i utgangspunktet har rett til privatliv.

Subsidiaritetskravet innebærer imidlertid ikke at andre metoder må ha vært forsøkt, og heller ikke at dataavlesning alltid vil være mer inngripende enn for eksempel kommunikasjonskontroll. Det er de konkrete omstendigheter i hvert enkelt tilfelle som vil være avgjørende for om dataavlesning fremstår som mer eller mindre inngripende enn andre tvangsmidler.[64] Å ha et absolutt krav om at andre tvangsmidler måtte vært forsøkt før dataavlesning, ville derfor kunne virket mot sin hensikt. Det ble videre konstatert som for krevende for retten å gjøre en slik vurdering.[65] Det vil derfor være opp til påtalemyndigheten ved begjæring om tillatelse til dataavlesning å gi retten informasjon som er tilstrekkelig for at den kan foreta en reell vurdering av behovet for tvangsmiddelbruken.[66]

3.5 Ytterligere hjemmel for målrettet dataavlesning

For å gjøre hjemmelen for dataavlesning enda mer målrettet, finnes det ytterligere et vilkår etter strpl. § 216 o tredje ledd siste punktum. Her fremkommer det at § 216 c annet ledd gjelder også gjelder ved dataavlesning. Dette innebærer at det må foreligge "*særlige grunner"* for å tillatte bruk av dataavlesning dersom datasystemet som skal avleses er "*tilgjengelig for et større antall personer,"* eller dersom dataavlesningen gjelder for datasystem *"som tilhører advokat, lege, prest eller andre som erfaringsmessig fører samtaler av svært fortrolig art"* … "*såfremt vedkommende ikke selv er mistenkt i saken*".[67]

I slike situasjoner må det altså foreligge "særlige grunner" for å tillatte dataavlesning, som setter en ytterligere terskel for bruken. Ordlyden "*særlige grunner*" tilsier at det må være en spesiell situasjon som gjør at dataavlesning skal tillattes, til tross for at det er andre personer

[61] Bruce (2018) side 261.
[62] Prop. 68 L (2015-2015) side 269 o g Ot.prp. nr. 60 (2004-2005) side 71.
[63] Ot.prp. nr. 60 (2004-2005) side 71.
[64] Prop. 68 L (2015-2015) side 269.
[65] Prop. 68 L (2015-2015) side 269.
[66] Prop. 68 L (2015-2015) side 269.
[67] Prop. 68 L (2015-2016) side 269.

enn mistenkte som rammes av integritetskrenkelsen. At det foreligger "særlige grunner" skal etter forarbeidene forstås som at de hensyn som ellers begrunner adgang til dataavlesning gjør seg særlig sterkt gjeldene. Eksempler på dette er dersom det fremstår som klart at dataavlesning er nødvendig for å oppklare saken, eller fordi det straffbare forholdet er av høy alvorlighetsgrad. Selv om det finnes et krav om særlige grunner, skal dette ikke tolkes så strengt at en aldri skal kunne foreta dataavlesning i slike situasjoner.[68] Forarbeidene som refereres til her er angående kommunikasjonskontroll, men det legges til grunn at samme gjelder for dataavlesning, siden ingen annen forståelse er kommentert ved innføringen av dataavlesning.

Ordlyden "*tilgjengelig for et større antall personer*" indikerer at det må være et datasystem flere personer har tilgang til. I forarbeidene er datamaskiner som hele studentmassen ved et lærested kan benytte seg av brukt som eksempel.[69] Et annet eksempel kan være en datamaskin i et hjem hvor flere familiemedlemmer benytter seg av den.

Her kan det også vises til strpl. § 216 p siste ledd første punktum hvor det fremkommer at "*Dataavlesingen skal innrettes slik at det ikke unødig fanges opp opplysninger om andre enn mistenktes bruk av datasystemet*". Vilkåret skal etter forarbeidene forstås som at avlesningen skal være så målrettet som mulig.[70]

Tilsvarende uttrykk finnes ikke i eksplisitt i andre bestemmelser om skjult tvangsmiddelbruk, men ville nok kunne inngå i en drøftelse i det generelle forholdsmessighetskravet etter straffeprosessloven § 170 a.[71] At kravet ved dataavlesning er tatt inn som en egen bestemmelse, var for å understreke viktigheten av at det ikke gjøres større inngrep i noens privatliv enn nødvendig.[72]

[68] Prop. 147 L (2012-2013) side 174.
[69] Ot.prp.nr.64 (1998-1999) side 159.
[70] Prop. 68 L (2015-2016) side 272.
[71] Bruce og Haugland (2018) side 261.
[72] Prop. 68 L (2015-2016) side 272.

3.6 Forholdsmessighetskravet

Et krav som gjennomgående kommer til uttrykk i samtlige vilkår redegjort for er kravet om at inngrepet må være nødvendig. Dette kravet følger ikke direkte av straffeprosessloven, men vil være foreligge i forholdsmessighetsvurderingen etter strpl. § 170 a.[73]

I straffeprosessloven § 170 a fremkommer det generelle forholdsmessighetskravet som skal vurderes ved bruk av alle tvangsmidler. Bestemmelsen lyder slik:

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

Her fremkommer det to vilkår, hvor det ene er at inngrepet må ha "tilstrekkelig grunn" og det andre er at inngrepet ikke må være "uforholdsmessig".

En naturlig språklig forståelse av ordlyden "*tilstrekkelig*" tilsier at det må være en sterk eller god grunn som er hensiktsmessig. Eksempel på hvordan en slik vurdering kan foretas finnes i Rt. 2012 s.1645. I avsnitt 19 i avgjørelsen fremkommer det at spørsmålet om politiet hadde plikt til å foreta speilkopiering av databeslag måtte avgjøres ut fra en interesseavveining av kostnader, mulig bevisforspillelse og siktedes behov for beslaget. At tvangsmiddelet bare kan anvendes når det er "tilstrekkelig grunn til det" skal sees på som en sikkerhetsventil. Vanligvis vilkåret være oppfylt dersom bruken er nødvendig og forholdsmessig.[74]

I vurderingen av om tvangsmiddelet er "uforholdsmessig" kan flere momenter være av betydning. Det må se på hvor stort behov det er for å anvende tvangsmiddelet. Videre må det vurderes hvor inngripende bruken av tvangsmiddelet i den konkrete saken er ut fra saken i sin helhet.[75]

Bestemmelsen i strpl. § 170 a har betydning for om tvangsmiddelet i det hele tatt kan benyttes, men også for om det skal avsluttes før fristen som er satt for bruken er utløpt.[76]

Mange av de momentene som spiller inn i den generelle forholdsmessighetsvurderingen etter strpl. § 170 a er ytterligere forsterket i reglene som fremkommer av strpl. §§ 216 o og p. Forholdsmessighetsvurderingen er nokså lik den som fremkommer i EMK artikkel 8 annet

[73] Øyen (2016) side 179.
[74] Øyen (2016) side 179.
[75] Øyen (2016) side 179.
[76] Prop. 68 L (2015-2016) side 66.

ledd. Etter denne bestemmelsen må inngrepet være ”nødvendig i et demokratisk samfunn”. Kravet vil derfor bli drøftet ytterligere i avhandlingens kapittel 5 som tar for seg betydningen av Grunnloven § 102 og EMK artikkel 8.

4 Prosessuelle vilkår for å benytte dataavlesning

4.1 Generelt

De personelle og prosessuelle vilkårene for bruk av dataavlesning er også regulert i strpl. §§ 216 o og p. I tillegg fremkommer det i strpl. § 216 o siste ledd at §§ 216 d til 216 k også gjelder for dataavlesning.[77] Reglene om bruk av dataavlesning er også omfattet av kommunikasjonskontrollforskriften.[78]

4.2 Hvem har kompetanse til å beslutte dataavlesning?

Etter strpl. § 216 p første ledd er det retten som har kompetanse til å beslutte bruk av dataavlesning. Unntak fra dette fremkommer etter strpl. § 216 d hvor det fremkommer at dersom det ved opphold er fare for at etterforskningen vil lide vil tillatelse til å benytte dataavlesning kunne gis av påtalemyndigheten. Dette kalles såkalt "hastekompetanse".[79] Bruk av hastekompetanse må informeres til retten innen 24 timer etter det er besluttet.[80]

Kompetansen til å beslutte bruk av dataavlesning er fordelt mellom domstolene og påtalemyndighetene jf. strpl § 216 o første og femte ledd. Domstolene kan tillatte bruk av dataavlesning etter begjæring fra påtalemyndighetene, og avgjørelsen treffes ved kjennelse. Det er i utgangspunktet retten som skal avgjøre om dataavlesning skal tillattes fordi

For at politiet skal kunne ta i bruk dataavlesning er de i utgangspunktet avhengig av "godkjenning" fra domstolen. Dersom politiet ønsker å benytte dataavlesning må de sende inn en begjæring til domstolen. Domstolen tar da stilling til om dataavlesning skal tillattes i den konkrete saken, og treffer en avgjørelse ved kjennelse.

4.2.1 Hastekompetanse

Et unntak fra at det er retten som gir tillatelse til bruk av dataavlesning er ved såkalt "hastekompetanse". Dersom det ved opphold er stor fare for at etterforskingen vil lide, kan ordre fra påtalemyndigheten tre istedenfor kjennelse av retten jf. strpl. § 216 d. Denne utvidede fullmakten forutsetter at påtalemyndigheten utøver et skjønn basert på rettssikkerhet

[77] Reglene gjelder i utgangpunktet for bruk av kommunikasjonskontroll.
[78] Forskrift 9. september 2016 nr. 1047 om kommunikasjonskontroll, romavlytting og dataavlesning.
[79] Prop. 68 L (2015-2016) side 49.
[80] Jf. strpl. § 216 d annet punktum.

og personvern, og at det kun brukes i saker hvor det er strengt nødvendig.[81] Begrunnelsen for dette er blant annet at, i saker hvor påtalemyndigheten bruker hastekompetanse kan ikke retten ved den etterfølgende kontroll, forhindre inngrepet. Inngrepet vil allerede være gjort.[82]

Bruk av hastekompetanse skal informeres til domstolen *senest* innen 24 timer etter det er besluttet jf. strpl § 216 d første ledd annet punktum. Dersom fristen ender på et tidspunkt utenom rettens ordinære kontortid, blir fristen forlenget til retten åpner igjen, jf. bestemmelsens første ledd tredje punktum.

I informasjonen som sendes til domstolen skal det fremkomme hvorfor det ble besluttet å benytte hastekompetanse jf. bestemmelsens første ledd fjerde punkt.[83]

4.3 Stedlig kompetanse

Ved begjæring om bruk av dataavlesning skal saken bringes inn for tingretten på det sted hvor det mest praktisk kan skje jf. strpl. § 216 e første ledd. Denne avgjørelsen treffes uten at den mistenkte eller den som avgjørelsen ellers rammer, gis adgang til å uttale seg, og kjennelsen blir heller ikke meddelt dem jf. strpl. § 216 e siste ledd.[84]

4.4 Rettigheter for den dataavlesning blir benyttet mot

Ved bruk av dataavlesning vil den som inngrepet rettes mot først i ettertid (og noen ganger heller ikke da jf. strpl § 216 j 3. ledd 2. punktum), få vite at det er benyttet tvangsmiddel mot han/henne. For å ivareta mistenktes interesser skal det derfor ved behandlingen av saker om dataavlesning opprettes en offentlig advokat jf. strpl. § 100 a. Videre finnes det ulike kontrollorganer som fører helhetlig tilsyn med bruken i ettertid, slik som kontrollutvalget for kommunikasjonskontroll og EOS-utvalget.[85] Datatilsynet kan i denne sammenhengen også nevnes som et uavhengig forvaltningsorgan som skal sørge for at den enkelte ikke blir krenket ved bruk av opplysninger som kan knyttes til dem.[86]

---

[81] Ot. Prp. Nr. 64 (1998-1999) side 63.
[82] Ot. Prp. Nr. 64 (1998-1999) side 63.
[83] Se også kommunikasjonskontrollforskriften § 1 annet ledd annet punktum.
[84] Her kommer imidlertid reglene om offentlig oppnevnt forsvarer jf. strpl. § 100 a inn i bildet. Se punkt 4.3.1.
[85] Prop. 68 L (2015-2016) side 259.
[86] https://www.datatilsynet.no/om-datatilsynet/oppgaver/ (sist sett 31.12.18).

4.4.1 Straffeprosessloven § 100 a offentlig oppnevnt forsvarer

I saker hvor dataavlesning iverksettes er noe av essensen i valget av tvangsmiddelet at personen ikke får vite at det blir benyttet mot han/henne. Etter strpl. § 82 tredje ledd fremkommer det at personen da ikke får stilling som «siktet». Reglene som status som «siktet» kommer derfor ikke til anvendelse. Dette gjelder blant annet reglene om å krav på å varsles til rettsmøtene jf. strpl. § 86 og retten til å være stede under forhandlingene jf. strpl. § 92.

I stedet for at den mistenkte selv kan ivareta sine rettigheter, er det et lovfestet krav om at retten skal oppnevne en offentlig advokat for den mistenkte i saken etter strpl. § 100 a jf. § 102. Det blir da denne advokaten sin oppgave å ivareta rettighetene til den mistenkte på etterforskingsstadiet. Advokaten skal oppnevnes straks det besluttes å ta i bruk dataavlesning, fordi det er viktig at han/hun får tid til å forberede seg.[87] Dette skal ivareta hensynet til kontradiksjon som er et viktig hensyn i straffeprosessen.

Strpl. § 100 a er plassert i strpl. kapittel 9 om "forsvareren" og de øvrige bestemmelsene i dette kapittelet gjelder så langt de passer.[88] Etter bestemmelsens første ledd skal advokaten oppnevnes selv om den mistenkte allerede har forsvarer (f.eks. i forbindelse med en annen straffesak). Bakgrunnen for dette er advokatetiske retningslinjer hvor det er en lojalitetsplikt mellom advokat og klient som vil brytes dersom forsvareren ikke kunne opplyse om at det blir benyttet dataavlesning mot vedkommende.

Det følger av bestemmelsens annet ledd at oppgaven til advokaten er å ivareta mistenktes og eventuelt tredjepersoners rettigheter når retten behandler begjæringen om å bruk av dataavlesning. Videre følger det at ved en eventuell begjæring om forlengelse av dataavlesning skal samme advokat benyttes så langt det er mulig.

Advokaten skal gjøres kjent med begjæringen, og hva som er grunnlaget for den, altså de faktiske omstendigheter som ligger til grunn for begjæring om dataavlesning. Videre skal han varsles til rettsmøter som behandler begjæringen, og han har rett til å uttale seg før det treffes

[87] Ot.prp.nr. 64 (1998-1999) side 144.
[88] Ot.prp.nr. 64 (1998-1999) side 144.

en avgjørelse. Advokaten har også rett til å legge frem dokumenter og annet skriftlig materiale, selv om det ikke er uttrykkelig nevnt i bestemmelsen.[89]

4.5 Dataavlesningens tidsperiode

Etter strpl. § 216 f skal tillatelse til bruk av dataavlesning gis for et bestemt tidsrom, som ikke må være lenger enn strengt nødvendig. Det kan maksimalt gis tillatelse til bruk av dataavlesning for to uker om gangen.[90] Dette skiller seg fra reglene om tillatelse til bruk av kommunikasjonskontroll, som kan gis for fire uker om gangen. Grunnen til at det dataavlesning kun kan gis for to uker om gangen er ifølge forarbeidene at de etter omstendighetene kan fremstå som et større integritetsinngrep enn kommunikasjonskontroll. På grunn av dette ønsket departementet å legge til rette for en hyppigere prøving av om det er grunnlag for å fortsette dataavlesningen.[91]

Det følger videre av strpl. § 216 f annet ledd at dataavlesningen skal stanses før utløpet av fristen som er satt i rettens kjennelse, dersom vilkårene for avlesningen ikke lenger antas å være til stede, eller dersom avlesningen ikke lenger anses hensiktsmessig. I forarbeidene brukes det som eksempel at politiet, etter at avlesningen er iverksatt, mottar opplysninger som viser at det ikke lenger er skjellig grunn til mistanke mot den avlesningen er rettet mot.[92] Begrensningen som kommer til uttrykk i denne bestemmelsen kan nok også utledes av forholdsmessighetsprinsippet etter 170 a, men departementet mente det var hensiktsmessig å synliggjøre dette ytterligere gjennom denne henvisningen til § 216 f annet ledd.[93]

4.6 Taushetsplikt

I en sak om dataavlesning skal alle involverte bevare taushet om at det er begjært eller besluttet bruk av dataavlesning, og om de opplysninger som fremkommer ved avlesningen jf. strpl. § 216 i første ledd.

[89] Se Ot.prp.nr 64 (1998-1999) side
[90] Jf. strpl. § 216 o siste ledd første punktum.
[91] Prop.68 L (2015-2016) side 273.
[92] Prop.68 L (2015-2016) side 273.
[93] Prop.68 L (2015-2016) side 273.

4.7 Oppbevaring, sperring og sletting av materiale innhentet ved bruk av dataavlesning

Ved bruk av dataavlesning blir innhentet materiale oppbevart for en viss tid etter inngrepet har funnet sted. Oppbevaringen i seg selv utgjør et inngrep i Grl. § 102 og EMK art. 8.[94] Derfor finnes det egne regler for politiets oppbevaring, sperring og sletting av materiale innhentet ved bruk av dataavlesning som fremkommer i strpl. § 216 g og kommunikasjonskontrollforskriften §§ 8 og 9.

I strpl. § 216 g fremkommer det at påtalemyndigheten i utgangspunktet ved bruk av dataavlesning skal slette materialet etter en viss tid. Unntakene fra denne regelen fremkommer i bestemmelsens a og b og er dersom det: a) er uten betydning for forebyggelsen eller etterforskningen av straffbare forhold eller b) gjelder uttalelser som retten etter reglene i §§ 117 til 120 og 122 ikke vil kunne kreve vedkommendes vitneforklaring om, med mindre vedkommende mistenkes for en straffbar handling som kunne gitt selvstendig grunnlag for kontrollen.[95]

[94] Rt. 2014 side 1105 avsnitt 28. Se nærmere om dette i avhandlingens kapittel 5.
[95] Mer om dette i avhandlingens punkt 5.3.3.

5 Betydningen av Grunnloven § 102 og EMK artikkel 8

They who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.

- Benjamin Franklin, 1755

5.1 Innledning og problemstilling

I dette kapittelet skal det redegjøres for betydningen av Grunnloven (heretter Grl.) § 102 og EMK art. 8. Det skal avklares om reglene om bruk av dataavlesning samsvarer med retten til respekt for privatliv etter disse bestemmelsene. Hovedproblemstillingen dette kapittelet skal svare på er: *Utgjør politiets bruk av dataavlesning i etterforskingsøyemed en krenkelse av retten til respekt for privatliv etter Grl. § 102 og EMK art.8?*

5.2 Generelt om Grunnloven § 102 og EMK artikkel 8

Grl. § 102 ble endret i forbindelse med grunnlovsreformen (res. 14.mai 2014 nr. 628), og trådte i kraft 18.mai 2014. Grl. § 102 lyder slik:

> *Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.*

Tidligere § 102 i Grl. representerte også et begrenset utslag av retten til vern om privatliv. Ved endringen av bestemmelsen i 2014, var det meningen å gi vernet en enda større plass i norsk rett, og forsterke den rettslige forankringen, ved å tilføye vernet om rett til privatliv i den høyeste rettskilden i Norge.[96] Høyesterett har behandlet flere saker om retten til privatliv

[96] Dokument 16 (2011-2012) side 175-176.

jf. Grl. § 102 etter at bestemmelsen ble endret,[97] og i disse sakene blir bestemmelsen sett i sammenheng med EMK artikkel 8 som lyder slik:

> ***Art 8.Right to respect for private and family life***
>
> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

5.2.1 Forholdet mellom Grunnloven § 102 og EMK art. 8

Grl. § 102 er av grunnlovs rang, som innebærer at det er den høyeste rangen en rettskilde i Norge kan ha. Dette betyr at den ved motstrid går foran alle lover av mindre rang. EMK art. 8 er inkorporert i norsk lov etter menneskerettsloven § 3,[98] og er derfor av lavere rang. Tidligere innebar dette at retten til respekt for privatliv etter EMK art. 8 kunne oppheves ved ordinær lovgivning. Når retten til respekt for privatliv nå fremkommer i Grunnloven, er det vanskeligere å endre eller sette til side bestemmelsen jf. Grl. § 121.[99]

Nå som Grl. § 102 er grunnlovfestet vil det også ha betydning for den videre tolkningen av retten til respekt for privatliv. Der en før var avhengig av avgjørelser fra Den europeiske menneskerettsdomstols praksis (heretter EMD) ved forståelsen av vernet til privatliv, kan nå Høyesterett selv utvikle den videre praksisen. Selvfølgelig vil praksis fra EMD fortsatt være relevant, da vi fortsatt er forpliktet til å følge konvensjonen (med tilhørende praksis). Likevel vil det at retten til privatliv nå er forankret i Grunnloven kunne redusere belastningen av saker for de internasjonale konvensjonsorganene. Per dags dato er EMD overbelastet med saker, og

[97] Se for eksempel Rt. 2014 s. 1105 avsnitt 28 og 29, og Rt. 2015 s. 93 avsnitt 57. Nærmere redegjort for i avhandlingens punkt 5.3.
[98] Lov 21 mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett.
[99] Dokument 16 (2011-2012) side 51.

etter Interlaken Declaration av 19. februar 2010 er Norge forpliktet til ta et større nasjonalt ansvar for ivaretakelsen av menneskerettighetene.[100]

Etter at forholdet mellom Grl. § 102 og EMK art. 8 nå er nærmere klarlagt vil jeg i det videre behandle reglene samlet. Når det sees hen til praksis knyttet til EMK art. 8 vil dette kunne supplere hvilken forståelse Høyesterett benytter ved tolkning av Grl. § 102. Høyesterett trenger imidlertid ikke komme frem til samme resultat som EMD hva angår politiets bruk av dataavlesning. Dette vil gjelder i det tilfelle at en person saksøker politiet for angivelig brudd på Grl. § 102 i fremtiden. Da kan det være Høyesterett kommer fram til annet resultat enn EMD ville gjort.

5.3 Rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon

5.3.1 Omfanget av privatlivsbegrepet i Grl. § 102 og EMK art. 8

Det generelle vernet av privatlivets fred fremkommer altså både av Grl. § 102 og EMK art. 8. I bestemmelsene fremgår det uttrykkelig at vernet omfatter den enkeltes privatliv, familieliv, hjem og kommunikasjon/korrespondanse.[101] De ulike rettighetene er i liten grad skilt fra hverandre av EMD,[102] og vil i mange tilfeller gli over i hverandre. Begrepene familieliv, hjem og kommunikasjon fungerer som spesifiserte eksempler på elementer som omfattes av privatlivet.[103]

Privatlivsbegrepet er ment å favne vidt og det finnes ikke en konkret definisjon,[104] men det gir uttrykk for en av de mest grunnleggende rettighetene alle mennesker har. Som enkeltmenneske har alle i utgangpunktet behov for en privat sfære hvor man kan leve uten innblanding fra myndighetene, næringsdrivende etc. eller andre personer.[105] Den private

[100] Dokument 16 (2011-2012) side 51.
[101] I Grl. § 102 er formuleringen ”kommunikasjon” brukt i stedet for ”korrespondanse”, fordi det er en moderinisering av ordet ”korrespondanse” slik det fremkommer i EMK. Ved å bruke ordet ”kommunikasjon” i stedet for ”korrespondanse” skal det være utvilsomt at vernet også omfatter nye digitale medier, telefon, epost og sms. Jf. Dokument 16 (2011-2012) side 178.
[102] Prop. 68 L (2015-2016) side 38.
[103] Bruce og Haugland (2018) side 40.
[104] Rt. 2012 s. 2039 avsnitt 70.
[105] Prop.68 L (2015-2016) side 19.

sfære er et sentralt element både i den personlige integritet og personvernet, og det er en forutsetning for menneskets dannelsesprosess og myndiggjøring.[106]

Videre omfatter privatlivsbegrepet blant annet en persons fysiske og psykiske integritet.[107] Dette innebærer at EMK art. 8 skal sikre utvikling av enhver persons personlighet og mellommenneskelige relasjoner, i utgangspunktet uten utenforstående sin innblanding.[108]

Politiets bruk av dataavlesning vil potensielt kunne gripe inn i forskjellige sider av privatlivets sfære, vernet av Grl. § 102 og EMK art. 8. Mest åpenbart er det at dataavlesning berører retten til privatliv og korrespondansen. Virkemiddelet kan også tenkes å gripe inn i den enkeltes fysiske og psykiske integritet, så vel som i ens private hjem hvor vernet om privatliv etter EMK art. 8 er særlig sterkt.[109]

5.3.2 Kan det gjøres inngrep i retten til respekt for privatliv etter Grl. § 102?

Ved innføringen av ny Grl. § 102 i 2014 ble det rettslige vernet av privatlivet mer direkte og utførlig omtalt ved at ordlyden omtaler retten til respekt for privatliv uttrykkelig. I den nye ordlyden til Grl. § 102 fremkommer det imidlertid ikke om det kan gjøres inngrep i retten til respekt for privatliv, slik det kan etter EMK art. 8 nr. 2. Det har imidlertid kommet en del avgjørelser fra Høyesterett etter at ny Grl. § 102 ble innført. I de neste to avsnittene vil det redegjøres for to dommer Rt. 2014 s. 1105 "Acta-kjennelsen" og Rt. 2015 s. 93 "Maria-saken" som viser noe hvordan Høyesterett tar stilling til spørsmål som gjelder retten til privatlivet i sammenheng med skjult tvangsmiddelbruk.

5.3.3 Rt. 2014 s. 1105 "Acta-kjennelsen"

Acta-saken er aktuell fordi det er første gang Høyesterett tok stilling til Grl. § 102 etter grunnlovsreformen, og fordi den gjaldt bruk av skjulte tvangsmidler. Saken gjaldt overskuddsmateriale ved kommunikasjonskontroll.

Hovedproblemstillingen var om overskuddsmaterialet, som var lovlig innhentet, og som etter nye regler i utgangspunktet også var tillatt som bevis, måtte avskjæres. Dette fordi det er spørsmål om materialet innhentet ved kommunikasjonskontroll etter tidligere regler skulle

---

[106] Prop.68 L (2015-2016) side 19.
[107] Se Von Hannover mot Tyskland 24.juni 2004 (saksnummer 59320/00) avsnitt 50.
[108] Se Von Hannover mot Tyskland 24.juni 2004 (saksnummer 59320/00) avsnitt 50.
[109] Prop. 68 L (2015-2016) side 238.

vært slettet, eller fordi de nye reglene ikke kunne anvendes i en sak som allerede stod for domstolen.[110]

I saken var det sju personer som var tiltalt for blant annet overtredelser av verdipapirhandelloven, i form av innsidehandel og kursmanipulasjon. De hadde i en dom fra 2012 blitt dømt til fengselsstraffer fra ett til ti år. Deretter ble det startet ankebehandling i 2014, som pågikk i åtte måneder.

I 2008 hadde det under etterforskingen blitt gjennomført kommunikasjonskontroll fordi siktelsen også omfattet straffeloven § 60a om straffbar handling utøvet som ledd i aktivitetene til en organisert kriminell gruppe. Denne delen av siktelsen ble imidlertid frafalt i 2010. Etter dagjeldende lovverk kunne materialet som ble innhentet gjennom kommunikasjonskontrollen ikke benyttes som bevis for tingretten da tiltale ble tatt ut i 2011. Etter siktelsen ble frafalt ble materialet innhentet i kommunikasjonskontrollen regnet som "overskuddsmateriale". Dette ble ikke slettet.

Det alminnelige forbudet mot bruk av overskuddsmateriale som bevis ble ved lov av 21.juni 2013 nr. 86 opphevet. Den nye regelen er nå at materiale innhentet ved kommunikasjonskontroll, på visse vilkår, kan benyttes som bevis også ved iretteføring av straffbare forhold som ikke i seg selv kunne ha begrunnet kommunikasjonskontroll.[111] I 2014 varslet påtalemyndighetene at de ønsket bruke overskuddsmaterialet brukt som bevis under ankebehandlingen. Lagmannsretten tillot materialet som bevis. Deretter anket tre av de tiltalte denne avgjørelsen til Høyesterett. Også en av de tiltaltes ektefelle anket at materialet hvor hun selv deltok måtte avskjæres som bevis. En fjerde av de tiltalte var enig med påtalemyndigheten, og mente materialet kunne tillates ført som bevis. Ankesaken ble overført av Høyesterett i avdeling med fem dommere, jf. domstolloven § 5 første ledd andre punktum.

I avgjørelsens avsnitt 23-30 redegjøres det for hvilket hjemmelsgrunnlag som ligger til grunn for at overskuddsmaterialet skulle vært slettet. Det er også her de mest relevante poengene i forhold til kapittelets tema fremkommer.

[110] Avgjørelsens avsnitt.
[111] Jf. strpl. § 216 i første ledd bokstav d.

Høyesterett redegjør for det første om at utgangspunktet for politiets innhenting, oppbevaring og bruk av materiale som er ervervet ved kommunikasjonskontroll må ha hjemmel.[112] Hjemmelen må fremkomme direkte av lov, eller ved forskrift med hjemmel i lov.[113] Videre redegjøres det for Grl. § 102 og dens betydning ved innhenting av materiale som griper inn i bestemmelsens vernede rettigheter. Det vises til Innst. 186 S (2013-2014) side 27 hvor det fremkommer at Grl. § 102 «skal leses som at systematisk innhenting, oppbevaring og bruk av opplysninger om andres personlige forhold bare kan finne sted i henhold til lov, benyttes i henhold til lov eller informert samtykke og slettes når formålet ikke lenger er til stede».[114]

Videre blir det i dommen lagt til grunn at i tillegg til disse kravene vil «hvorvidt en lov som griper inn i privat- og familielivet, hjemmet, kommunikasjonen eller den personlige integritet, er forenlig med § 102, også beror på om loven ivaretar et legitimt formål og er forholdsmessig».[115] Som eksempel på dette vises det til det faktum at overskuddsmaterialet må "slettes når formålet ikke lenger er til stede", er en konsekvens av forholdsmessighetskravet som gjelder for lovhjemlede og saklig begrunnede inngrep i rettighetene og frihetene fastsatt i Grunnlovens menneskerettsbestemmelser.[116]

Av denne avgjørelsen kan det for det første utledes at det kan gjøres inngrep i retten til privatliv i Grl. § 102, men også at dette kun kan rettferdiggjøres dersom det oppfyller vilkår om forholdsmessighet, lovmessighet og legitim begrunnelse.

5.3.4 Rt. 2015 s. 93 "Maria-saken"

I Rt. 2015 s. 93 "Maria-saken" blir det (i avsnitt 57) lagt til grunn at Grl. § 102 skal tolkes i lys av EMK art. 8. Videre gis det uttrykk for at fremtidig praksis fra de internasjonale håndhevingsorganene "*ikke har samme prejudikatsvirkning ved grunnlovstolkningen som ved tolkningen av de parallelle konvensjonsbestemmelsene: Det er etter vår forfatning Høyesterett – ikke de internasjonale håndhevingsorganene – som har ansvaret for å tolke, avklare og utvikle Grunnlovens menneskerettighetsbestemmelser*".

Videre fremkommer det i avgjørelsen avsnitt 60 at: "*grunnlovsvernet kan ikke være –og er heller ikke –absolutt.*" Med dette menes at det også er et adgang til å gjøre inngrep i

[112] Avgjørelsens avsnitt 24.

[114] Avgjørelsens avsnitt 28.
[115] Avgjørelsens avsnitt 28.
[116] Avgjørelsens avsnitt 28.

grunnlovsvernet, og videre fremkommer det at "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 legitimt formål og er forholdsmessig". Dette viser at det er adgang til å gjøre inngrep i vernet etter Grunnloven § 102, og dette samsvarer med regelen etter EMK artikkel 8 nr. 2.

5.3.5 Utgjør politiets bruk av dataavlesning i etterforskingsøyemed et inngrep i retten til respekt for privatliv?

Innhenting av informasjon om enkeltpersoner ved bruk av skjulte tvangsmidler er flere ganger vurdert som et inngrep i retten til respekt for privatliv etter EMK art. 8 av EMD.

Til tross for at EMD ikke eksplisitt har tatt stilling til om tvangsmiddelet *dataavlesning* utgjør et inngrep, kan det ved å sammenligne tvangsmiddelets karakter med de øvrige skjulte tvangsmidler, legges til grunn at dataavlesning åpenbart er å anse som et inngrep i retten til respekt for privatliv. Det interessante spørsmålet er om inngrepet kan rettferdiggjøres etter EMK artikkel 8 nr. 2.[117]

I de neste avsnittene skal det sees nærmere på EMDs praksis tilknyttet EMK artikkel 8 hvor de vurderer bestemmelsen i forhold til straffeprosessuelle tvangsmidler. Dette er relevant for å se hvordan Høyesterett kunne vurdert politiets adgang til bruk av dataavlesning i forhold til retten til respekt for privatliv. Det må likevel tas i betraktning at Høyesterett vil kunne ta nye og annerledes vurderinger enn EMD gjør, og at det da er Høyesteretts vurdering av saken som avgjør om regelen samsvarer med norsk rett.

5.3.6 Positive og negative forpliktelser

EMK pålegger konvensjonsstatene både såkalte "positive" og "negative" forpliktelser, jf. EMK art. 1, hvor det fremkommer at statene skal *sikre* og *respektere* konvensjonens rettigheter.

Et annet aspekt ved EMK er at den pålegger konvensjonsstatene såkalte positive og negative forpliktelser. De negative forpliktelsene utgjør den tradisjonelle plikten en stat har for ikke å gjøre inngrep i de nedfelte rettighetene og frihetene som følger direkte av EMK. At en stat har en negativ forpliktelse etter konvensjonen betyr at de offentlige myndighetene skal unnlate å

[117] Dette redegjøres for i avhandlingens punkt. 5.4.

utøve myndighet eller annen adferd som griper inn i de interesser som er beskyttet etter konvensjonen. Med positive forpliktelser menes at statene pålegges aktivt å iverksette beskyttende tiltak som medfører at konvensjonsrettighetene blir praktiske og effektive i alle tilfeller, ikke kun der statene selv avstår fra inngrep.

Artikkel 8 har i EMD´s praksis både blitt tolket som en positiv og en negativ forpliktelse. Grensedragningen mellom statens positive og negative forpliktelser i artikkel 8 er ikke klart. På den ene siden vil dataavlesning gripe inn i retten til respekt for privatliv etter bestemmelsen. På den annen siden kan dataavlesning bekjempe alvorlig kriminalitet slik som terrorisme, og på den måten sikre enkeltpersoners rettigheter etter EMK art. 8.

5.4 Hva kreves for å kunne gjøre inngrep i retten til respekt for privatliv?

5.4.1 Tre kumulative hovedvilkår

I forrige avsnitt ble det konstatert at det kan gjøres inngrep i retten til respekt for privatliv. I dette avsnittet skal det klarlegges hva som skal til for å gjøre et slik inngrep. For at det skal kunne gjøres inngrep i det rettslige vernet som fremkommer i Grl. § 102 og EMK art. 8 stilles det tre kumulative hovedvilkår:

1. **Inngrepet må være foreskrevet i lov (lovkravet)**
2. **Inngrepet må ivareta anerkjennelsesverdige formål**
3. **Inngrepet må være nødvendig i et demokratisk samfunn (forholdsmessighetskravet)**

Reglene rundt bruk av dataavlesning i etterforskingsøyemed generelt og anvendelsen av den i hver enkelt sak må altså tilfredsstille disse vilkårene.[118] Disse vilkårene utledes av EMK art. 8 nr. 2, men også av Høyesterett og EMDs praksis.[119] Ut fra dette slås det fast at de også gjelder for å kunne gjøre inngrep i retten til privatliv etter Grl. § 102.

I de neste tre avsnittene skal de tre forskjellige hovedvilkårene for å kunne gjøre inngrep i retten til privatliv redegjøres for nærmere. Det skal klarlegges om reglene om politiets bruk av dataavlesning på et generelt grunnlag tilfredsstiller vilkårene. Det vil ikke diskuteres om

---

[118]

[119] Se for eksempel

anvendelsen i en konkret sak tilfredsstiller kravene, slik det vil kunne gjøres dersom en person saksøker politiet for angivelig brudd på Grl. § 102/ EMK art. 8 i fremtiden.

5.4.2 Ivaretar inngrepet anerkjennelsesverdige formål?

Første spørsmålet som skal besvares er om politiets bruk av dataavlesning i etterforskingsøyemed er begrunnet i anerkjennelsesverdige formål. Dette vilkåret behandles først fordi i EMDs praksis blir dette vilkåret som regel behandlet kortfattet, og er ofte uproblematisk.[120]

EMK art. 8 nr. 2 nevner flere formål, blant annet «national security», «public safety» og «the prevention of crime». Det følger av høyesteretts praksis at et tilsvarende krav om "legitimt formål" også gjelder for Grl. § 102.[121] De formålene som fremkommer i bestemmelsen dekker de fleste tilfeller hvor statene vil kunne ha behov for å gjøre inngrep.[122] Hva angår politiets bruk av dataavlesning i etterforskingsøyemed er det liten tvil om at inngrep for å etterforske kriminalitet faller innunder formålsangivelsen "*the prevention of disorder or crime"* i EMK art. 8 nr. 2.

Formålet med inngrepet vil imidlertid ha innvirkning på forholdsmessighetsvurderingen. I forholdsmessighetsvurderingen vil det blant annet sees på hvor tungtveiende samfunnshensyn det er tale om og i hvilken grad formålet med inngrepet er vurdert. Dette vil igjen kun avgjøre om inngrepet ansees akseptabelt etter EMK.[123]

5.4.3 Lovskravet

Neste spørsmål som skal besvares er politiets bruk av dataavlesning i etterforskingsøyemed oppfyller lovskravet etter EMK art. 8 nr. 2.

Inngrep fra myndighetene overfor den enkelte må etter norsk rett ha grunnlag i lov jf. Grl. § 113. Det fremkommer av det allmenne legalitetsprinsippet, som var ulovfestet frem til grunnlovsendringen i 2014. Kravet følger også av EMK art. 8 nr. 2 jf. ordlyden " *in accordance with the law".* EMK stiller derimot ikke krav om formell lov, slik det gjøres etter norsk rett. Dette fordi konvensjonsstatene har forskjellige rettstradisjoner på dette området. Storbritannia baserer seg for eksempel i stor grad på ulovfestet rett ("common law"). I Norge

[120] Bruce og Haugland (2018) side 43.
[121] Se Rt. 2015. 93 avsnitt 60.
[122] Bruce og Haugland (2018) side 43.
[123] Jf. for eksempel Buck mot Tyskland avsnitt 45. Dokument nr. 16 (2015-2016) s. 249.

har vi krav om formell lov for å straffe personer. Dette stammer fra den norske rettstradisjon legger vekt på maktfordeling og demokrati samt hensynet til forutberegnelighet. I Norge er det Stortinget som bestemmer hvilke regler som gjelder for inngrep, og det er domstolen som kontrollerer at de overholdt ved hver enkelt sak.[124]

Det er sjeldent problematisk *om* inngrepet har hjemmel,[125] men det stilles imidlertid krav til kvaliteten til hjemmelen som er brukt. Dette fremgår blant annet av avgjørelsen Malone mot Storbritannia,[126] i avsnitt 67 fremkommer det at: "…the phrase "*in accordance with the law*" does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention…" Av dette kan det også utledes at de nasjonale reglene også må være forenelige med rettsstatsprinsippet "the rule of law". Prinsippet går ut på at de nasjonale reglene må være tilgjengelige og forutberegnelige. Rettsreglene må være formulert tilstrekkelig klart og presist slik at borgerne kan innrette seg etter dem.[127]

På området for skjulte tvangsmidler har EMD imidlertid akseptert at reglene om forutberegnelighet ikke kan praktiseres på samme måte som for øvrige områder. Da ville jo noe med poenget med å bruke det skjulte tvangsmiddelet falt bort.[128] Dette fremkommer blant annet av avgjørelsen Roman Zakharov mot Russland i avsnitt 229 hvor EMD uttaler: "Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly."[129]

Risikoen for vilkårlig bruk kan imidlertid være større ved skjult tvangsmiddelbruk,[130] og det stilles derfor krav til å ha to "clear, detailed rules on interception".[131] Videre må den nasjonale loven være: "sufficiently clear to give citizens an adequate indication as to the circumstances

---

[124] Aall (2015) side 118-119.
[125] Et eksempel på en sak hvor det ikke fantes lovhjemmel for inngrep er *A mot Frankrike* hvor det på denne bakgrunnen ble konstatert en krenkelse av EMK art. 8 (jf. Aall 2015 side 122).
[126] Malone mot Storbritannia, 2. august 1984 (saksnummer 8691/79).
[127] Bruce og Haugland (2018) side 44.
[128] Se avhandlingens punkt 1.1.
[129] Roman Zakharov mot Russland, 4. desember 2015 (saksnummer 47143/06)
[130] Fordi den dataavlesning blir benyttet mot ikke vil få vite når virkemiddelet blir benyttet mot han/henne.
[131] Avgjørelsens avsnitt 229.

in which and the conditions on which public authorities are empowered to resort to any such measures."[132]

Ytterligere krav til lovgivningen for hvert enkelt tilfelle fremkommer videre i avgjørelsens avsnitt 224 hvor det fremkommer at loven må angi hvilke type handlinger som danner grunnlag for overvåkingen. Dette innebærer imidlertid ikke at det må være en uttømmende liste over navngitte lovbrudd.[133] Videre stilles det et krav om å definere hvilke kategorier mennesker som kan overvåkes, likevel ikke slik at det kun må være personer som er mistenkt eller anklaget for straffbare handlinger. Personer som besitter relevant informasjon kan også være aktuell ved bruk av skjulte tvangsmidler.[134]

Det er videre krav til at lovgivningen må oppstille en grense for hvor lenge det bruken av det skjulte tvangsmiddelet kan vare, og også om når den skal avsluttes. Lovgivningen må angi prosedyrer for gjennomgangen, bruken og oppbevaring materialet innhentet ved bruken av tvangsmiddelet.[135] Det stilles også krav til prosedyrer tilknyttet eventuelt utleveringer av opplysninger til andre myndigheter, og for når materialet skal slettes.[136]

Det er liten tvil om at politiets bruk av dataavlesning oppfyller første del av lovkravet gjennom Grl. § 113 og at reglene er lovfestet etter strpl. §§ 216 o og p.[137] Det som derimot kan problematiseres er om reglene tilfredsstiller det ekstra kravet til forutberegnelighet som gjelder på området for skjulte tvangsmidler, og videre de ytterligere kravene som stilles til slik lovgivning.

Som redegjort for i avhandlingens øvrige del er strpl. §§ 216 o og p teknisk og relativt omfattende bestemmelser. Det er mange og strenge vilkår for når og under hvilke omstendigheter dataavlesning kan benyttes. Bestemmelsene er utformet for bruk på få og spesielle tilfeller.

Både mistankekravet, kriminalitetskravet, indikasjons og subsidiaritetskravet, kompetansekravet og kravet om domstolkontroll som redegjort for i avhandlingens kapittel 3

---

[132] Avgjørelsens avsnitt 229.
[133] Avgjørelsens avsnitt 224.
[134] Roman Zakharov mot Russland avsnitt 245 og Bruce og Haugland (2018) side 45.
[135] Kennedy mot Storbritannia 18. mai 2010 (saksnummer 26839/05) avsnitt 155-170.
[136] Roman Zakharov mot Russland avsnitt 255-256. Her uttalte EMD at automatisk lagrin i seks måneder av data som ikke er relevante for det formålet de var samlet inn for utgjør en krenkelse av EMK art. 8.
[137] Redegjort for i avhandlingens øvrige del.

er med på å gi enkeltpersoner en tilstrekkelig klar og presis mulighet til å innrette seg til politiets bruk av dataavlesning i etterforskingsøyemed. Videre er også de prosessuelle og personelle vilkårene for politiets bruk av dataavlesning i etterforskingsøyemed redegjort for i avhandlingens kapittel 4 med på å ivareta de kravene som EMD stiller til integritetsinngrep etter EMK art. 8 nr. 2.

Etter dette har jeg kommet fram til at reglene om politiets bruk av dataavlesning oppfyller lovskravet etter EMK art. 8. nr. 2.

5.4.4 Forholdsmessighetskravet

Det siste hovedvilkåret for å kunne gjøre inngrep i privatlivet er at inngrepet må være "*necessary in a democratic society*" jf. EMK art. 8 nr. 2.

Spørsmålet er om politiets bruk av dataavlesning i etterforskingsøyemed er nødvendig i et demokratisk samfunn. Politiets bruk av dataavlesning må i denne sammenheng være egnet til å oppnå det aktuelle formålet, herunder politiets mulighet til ivareta «national security», «public safety» eller «the prevention of crime».[138] I denne vurderingen ser man på hvor stort inngrep i privatlivet dataavlesningen utgjør, sett i forhold til det legitime målet inngrepet skal ivareta.

For at dataavlesningen skal være nødvendig må de formål inngrepet skal ivareta være mer tungtveiende enn de interessene som krenkes ved menneskerettsinngrepet. Når Høyesterett i forbindelse med vurdering av inngrep i Grl. § 102 har uttalt at virkemiddelet må være "forholdsmessig", er det denne målestokken det siktes til.[139] De senere årene har EMD påpekt at det er nær sammenheng mellom lovskravet og forholdsmessighetskravet. EMD har derfor behandlet disse samlet.[140]

For å kunne ta stilling til om politiets bruk av dataavlesning oppfyller forholdsmessighetskravet vil det først sees på en annen faktor som spiller inn ved avgjørelser i EMD; statenes skjønnsmargin.

5.5 Statenes skjønnsmargin

Etter EMDs praksis fremkommer det altså at for at det skal kunne gjøres inngrep i EMK art.

[138] Se avhandlingens punkt 5.4.2.
[139] Rt. 2015 s. 93 avsnitt 60.
[140] Se for eksempel Kennedy mot Storbritannia avnsitt 155. Jf. Bruce (2018) side 43.

8, må den interne loven i konvensjonsstaten være tilstrekkelig klar og presis; være tilgjengelig og forutsigbar, og innlemme tilstrekkelige sikkerhetstiltak for å hindre vilkårlig utøvelse av det skjønn loven formidler.[141] Under vurderingen av dette er statene også gitt en viss grad av frihet til å tolke konvensjonen i tråd med egne forutsetninger, dette kalles statenes skjønnsmargin, såkalt "margin of appreciation". Ved avgjørelser i EMD tas det derfor hensyn til statenes egne forutsetninger når det kommer til for eksempel kultur, historie og filosofi for å belyse statens forståelse av konvensjonen, i forhold til EMDs forståelse.

EMDs prøvingsintensitet beror på blant annet inngrepets formål, rettighetens karakter og graden av europeisk oppfatning. Jo videre skjønnsmargin, desto mer tilbakeholden vil EMD være med å foreta en selvstendig vurdering som erstatter medlemsstatens syn på konvensjonsmessigheten. Medlemsstatens begrunnelse for inngrepet vil også ha betydning for prøvingsintensiteten til EMD. Begrunnelsen vil kunne legitimere inngrepet. Det vil videre være av betydning om inngrepet i konvensjonen er rettet mot en enkeltperson med en spesifikk begrunnelse, eller mot allmennheten på generelt grunnlag.

Selv om statenes skjønnsmargin innebærer at statene har en viss grad av frihet til å tolke konvensjonen i tråd med egne forutsetninger, vil dette basere seg på hvor vid skjønnsmargin statene er tillatt i det konkrete tilfellet. Noen områder er mer i kjernen av EMK art. 8 enn andre. Noen tilfeller faller inn under områder som medlemsstaten er nærmere, eller bedre egnet til, å vurdere på bakgrunn av kultur og tradisjon.

Statenes skjønnsmargin på området for skjulte tvangsmidler er snever. Dette illustreres i det følgende ved å se på EMD avgjørelsene *Robathin mot Østerrike, M.K mot Frankrike, Erdem mot Tyskland og Radaj mot Polen.*

5.5.1 Robathin mot Østerrike og M.K mot Frankrike

I Robathin mot Østerrike og M.K mot Frankrike tas det opp problematikken knyttet til overvåking, ransaking og beslag, som faller inn under ordlyden "*private life*" i EMK art. 8.

5.5.1.1 Robathin mot Østerrike

Robathin mot Østerrike handlet om en ransakelsesordre av en advokats elektroniske data på hans advokatkontor, under etterforskingen av en kriminell handling.[142] EMD slo fort fast at

[141] Harris m.fl (2014) side 587.
[142] Robathin mot Østerrike, 3. juli 2012 (saksnummer 30457/06).

inngrepet var "*in accordance with law",* og at ordren hadde et legitimert formål, nemlig å forhindre kriminalitet.[143] Det som var problematisk i saken var forholdsmessighetskravet, altså om forholdet mellom det mål som ble søkt oppnådd med ransakelsesordren og de midlene som anvendtes kunne betraktes forholdsmessig.[144] Ransakelsesordren i saken var gitt med veldig vide betingelser, mens beskrivelsen av de påståtte kriminelle handlingen kun angikk dokumentene med "R" og "G". Til tross for at de kriminelle handlingene kun knyttet seg til dokumentene "R" og "G", gikk politiet gjennom alle de elektroniske dataene til klageren. Det var videre kun gitt en kort og generell forklaring på hvorfor ransakelsesordren skulle foretas på alle de elektroniske dataene, og det var ikke gitt en spesiell grunn til at søket av alle dataene var nødvendig for etterforskningen. EMD lag vekt på at det bør være gode grunner for å kunne akseptere en ransakelsesordre av annen data enn det som er tilknyttet den kriminelle handlingen. I denne saken forelå det ingen slik begrunnelse. EMD kom derfor fram til at ransakelsesordren gikk lengre enn hva som var nødvendig for å oppnå det legitime målet, og at utgjorde en krenkelse av EMK art. 8.

5.5.1.2 M.K mot Frankrike

M.K mot Frankrike handlet om oppbevaring av fingeravtrykk i forbindelse med en etterforsking av klagerens utførelse av et boktyveri.[145] I avsnitt 29 i avgjørelsen slår EMD kort fast at slik bevaring av fingeravtrykk hos nasjonale myndigheters, utgjør et inngrep i retten til privatliv. Et slikt inngrep må være "*in accordance with the law*", og videre "*necessary in a democratic society*". Videre må det være slik at dersom den nasjonale lov gir tillatelse til et slikt inngrep, må det være passende sikringstiltak for å forhindre at slik bruk av personlig data, er i strid med EMK art. 8.[146] Staten hevdet det var nødvendig for å hindre identitetstyveri at de oppbevarte fingeravtrykkene. EMD mente at en slik oppbevaring var ensbetydende med å rettferdiggjøre lagring av info om hele Frankrikes befolkning. Dette anså EMD å være "*excessive and irrelevant*", og dermed ikke forholdsmessig.

EMD konkluderer med at medlemsstaten hadde overskredet skjønnsmarginen i saken. Dette fordi bevaringen av fingeravtrykkene til en person mistenkt for å begått kriminelle handlinger, men ikke dømt, ikke hadde en rimelig balanse mellom offentlige og private interesser.[147]

---

[143] Avsnitt 40-42 i avgjørelsen
[144] Avsnitt 43 i avgjørelsen.
[145] M.K mot Frankrike, 18. april 2013 (saksnummer: 19522/09)
[146] Avsnitt 35 i avgjørelsen.
[147] Avsnitt 46 i avgjørelsen.

Derfor måtte bevaringen av fingeravtrykkene bli sett på som et uforholdsmessig inngrep i klagerens rett til privatliv, og at det ikke kunne bli ansett som nødvendig i et demokratisk samfunn.

5.5.1.3 Sammenlikning av proporsjonalitetsvurderingene

Proporsjonalitetsvurderingene i avgjørelsene er forskjellige angående hvor inngående EMD går inn i medlemsstatenes vurdering av skjønnsmarginen. Prøvingsintensiteten i Robathin-saken er muligens noe større enn i M.K-saken. Begge avgjørelsene vurderer inngrepene å være uforholdsmessig, da medlemstatene har gjort et for stort inngrep i forhold til hva målet med inngrepet er, og at dette fører til vilkårlighet i bruken av loven.

Bruken av overvåking, ransaking og beslag er en akseptert metode under etterforskning av kriminell aktivitet ifølge EMD. Bruken av slike metoder må likevel ha relevante og saklige/legitime grunner, og må være proporsjonale. Proporsjonalitetskravet går ut på hvorvidt inngrepet er nødvendig i den konkrete saken. Når EMD vurderer hvorvidt et inngrep har vært forholdsmessig ser de først på under hvilke kriterier og omstendigheter inngrepet ble utstedt. Deretter på innholdet og omfanget av ordren, samt måten inngrepet ble gjennomført. Til sist sees det på omfanget av mulige konsekvenser for arbeidet og omdømmet til den part som har blitt rammet av inngrepet. Når EMD vurderer nødvendigheten av tiltaket, undersøker de også om den nasjonale lovgivning og praksis gir tilstrekkelige og effektive sikringstiltak mot overgrep og vilkårlighet.[148]

Det må en god begrunnelse til for at et slikt inngrep kan legitimeres etter EMK art. 8, og inngrepet må ha klare retningslinjer for hvordan det skal utføres. Ved å se på de to avgjørelsene sammen, ser det ut til at begrunnelsen må være ennå mer fremtredende når inngrepet berører mange.

5.5.2 Erdem mot Tyskland og Radaj mot Polen

I Erdem mot Tyskland og Radaj mot Polen tas det opp problematikken i hva angår til vernet om "*...the right to respect for... correspondence"* i EMK art. 8.[149][150] Overvåking, avlytting, eller sensuring av korrespondanse omfattes av vernet mot inngrep i EMK art. 8.

[148] Harris m.fl (2014) side 557.
[149] Erdem mot Tyskland, 5. juli 2001 (saksnummer 38321/97)
[150] Radaj mot Polen, 28. november 2002 (saksnummer 29537/95 og 35453/97)

Inngrepsvilkårene (når det er tillatt å gjøre inngrep) fremkommer av art. 8 (2), og dette er hvis det er "*in accordance with the law*", og videre at inngrepet "*is necessary in a democratic society..*" For at et inngrep art. 8 skal være i henhold til EMK, må den interne loven i konvensjonsstaten være tilstrekkelig klar og presis; være tilgjengelig og forutsigbar, og innlemme tilstrekkelige sikkerhetstiltak for å hindre vilkårlig utøvelse av det skjønn loven formidler.[151]

5.5.2.1 Erdem mot Tyskland

Erdem mot Tyskland handlet om åpningen av lovlig korrespondanse fra en fange mistenkt for terrorhandlinger. Klageren (Erdem) var fengslet ved den tyske landegrensen for blant annet å være medlem i en terrororganisasjon. EMD konkluderte med at det var et inngrep som var omfattet av EMK art. 8 da brev mellom Erdem og hans advokat var åpnet av en utenforstående. Staten hevdet åpningen av brevet (korrespondansen) var "*in accordance with the law*" fordi den var basert på beskyttelse av nasjonal sikkerhet og forebygging av kriminalitet og uorden.

Tysk lov la til rette for at en ekstern dommer som ikke var delaktig i den pågående sak skulle gjennomgå brev for å undersøke at det ikke var informasjon om terrororganisasjonen eller,[152] som er til skade for den offentlige interesse. Tysk rett la videre til rette for at dette skulle gjøres i spesielle tilfeller for enkelte fanger hvor det var ansett som nødvendig. EMD trakk fram poenget om at lovlig korrespondanse bare kan gjøres inngrep i ved unntakstilfeller. EMD kom fram til at en passende balanse mellom hensynet til individet og staten hadde vært truffet i dette tilfellet. Selv om det ikke eksplisitt var uttrykt hva de eksepsjonelle omstendighetene i denne saken var under henvisningen til "*the threat posted by terrorism in all its forms*",[153] tyder dette på at terrorismesammenhengen ga staten en større skjønnsmargin i dette tilfellet. Medlemsstaten hadde i dette tilfellet derfor ikke handlet i strid med konvensjonen.

5.5.2.2 Radaj mot Polen

I saken "Radaj mot Polen" klaget Radaj til EMD, fordi to brev til han var blitt åpnet og lest av administrasjonen i fengslet hvor Radaj var innsatt. Polsk lov åpnet for en automatisk adgang

[151] Harris m.fl (2014) side 587.
[152] Avsnitt 56 i avgjørelsen.
[153] Avsnitt 69 i avgjørelsen.

til å åpne og lese brev til innsatte.[154] Loven hadde ikke satt noe skille mellom fanger som det med et begrunnet motiv ville kunne være nødvendig å gjennomgå brev og andre innsatte hvor et slik behov ikke ville gjøre seg gjeldende. Det var heller ikke lagt til grunn hvordan en slik åpning av brev skulle foregå eller gjennomføres. På bakgrunn av disse forhold kom EMD frem til at polsk rett var i strid med EMK art. 8. En generell og automatisk adgang til å åpne og lese brev er det ikke adgang til etter EMK art. 8. Grunnen til at EMD kom til at polsk lov var i strid med EMK, var at adgangen til å åpne "*correspondence*", gjaldt alle innsatte. Det var altså ikke en lov som angikk spesifikk de fanger hvor det fantes et velbegrunnet behov for et slikt inngrep.

I Radaj mot Polen kom EMD frem til at staten er tillagt en noe snevrere skjønnsmargin når det gjelder et inngrep som angår alle de innsatte, altså en uspesifikk større gruppe. Ut fra dette kan det tolkes at begrunnelsen må være mer fremtredende når et inngrep rammer mange.

5.5.2.3 Resultatet

EMD kom fram til ulike resultat i Erdem og Radaj avgjørelsene. Dette på bakgrunn av begrunnelsen av inngrepet i EMK art. 8; hvor inngripende tiltaket var og hvor mange som ble berørt av inngrepet.

I Radaj-saken ga polsk rett en automatisk adgang til å lese alle innsattes brev, uten noen begrunnelse eller beskrivelse av hvordan tiltaket skulle gjennomføres. Derimot var inngrepet i Erdem-saken velbegrunnet og systemet som gjennomførte tiltaket var gjennomtenkt og bevarte den berørte på best mulig i måte. Det ble dessuten kun gjennomført for fanger av en spesifikk art som ga grunnlag for mistanke, som i den saken var terrorisme.

5.5.2.4 Skjønnsmargin

Ut fra disse avgjørelsene kan det tolkes at EMD legger opp til en snever adgang i statenes skjønnsmargin til å vedta regler om kontroll med posten til innsatte. Når det er en snever adgang til å gjøre inngrep i EMK art. 8 området for korrespondanse, må inngrepet være velbegrunnet og ha klare regler for gjennomførelse. Inngrep kan også kun gjøres i spesielle tilfeller for enkelte fanger, og ikke gjelde for alle innsatte i et fengsel.

Etter disse avgjørelsene synes det og som at avgjørende for om et inngrep kan aksepteres i relasjon til EMK art. 8 nr. 2 er summen av alle rettsikkerhetsgarantiene.

---

[154] Avsnitt 23 i avgjørelsen.

5.6 Vurdering av reglene om politiets bruk av dataavlesning sett i forhold til retten til respekt for privatliv

Det siste spørsmålet som må besvares er om reglene om politiets bruk dataavlesning er nødvendig i et demokratisk samfunn. Spørsmålet er om dataavlesningen er egnet til oppnå formålet om kriminalitetsbekjempelse, og om det utgjør et forholdsmessig inngrep. For å gjøre dette må begrunnelsen for å foreta inngrep i retten til privatliv etter EMK art. 8 nr. 2 være relevant og tilstrekkelig, og ivareta rettsikkerhetsgarantiene.

Innføringen av dataavlesning som selvstendig tvangsmiddel kom på bakgrunn av den stadig økende teknologiske utviklingen som skapte store etterforskningsmessige utfordringer for politiet. For eksempel den økende bruken av kryptering, som førte til at opplysninger politiet rettslig sett hadde adgang til gjennom bruk av kommunikasjonskontroll, men de fikk ikke faktisk adgang til de fordi opplysningene var kryptert. Dataavlesning ble vurdert å være et egnet virkemiddel for å imøtekomme dette. Dersom dataavlesning ikke hadde blitt innført som tvangsmiddel, ville politiet fortsatt ikke hatt mulighet til å etterforske kriminalitet hvor slike etterforskingsutfordringer oppstod. De kriminelle ville lettere slippe unna.

Samtidig innebærer dataavlesning et betydelig inngrep i den enkeltes privatliv når det blir benyttet. Det er ikke bare relevante opplysninger i relasjon til en sak som blir oppdaget, det andre opplysninger som ikke har noen ting med saken å gjøre kan også rammes. Imidlertid er det gjennom de prosessuelle reglene redegjort for i kapittel 4 en rekke bestemmelser som skal ivareta at dataavlesning ikke overgår det som er nødvendig. For det første stilles det krav til at for i det hele tatt iverksette dataavlesningen må det gis tillatelse av en domstol. For det andre er det krav til hvem som har kompetanse til å gjennomføre dataavlesningen. For det tredje blir mistenktes rettigheter ivaretatt gjennom oppnevnelsen av en offentlig advokat som opptrer på vegne av vedkommende under hele utførelsen av dataavlesningen. Ytterligere stilles det særlig strenge vilkår dersom dataavlesning kan ramme andre personer enn mistenkte eller personer i spesielle yrker hvor dette er spesielt uheldig.[155]

Det er også igjen greit å påpeke at politiet er gitt en snever adgang til bruk av dataavlesning i etterforskingsøyemed, og det er angitt spesifikke mål for hva som kan være gjenstand for avlesningen. I avhandlingens kapittel 3 ble vilkårene for politiets bruk av dataavlesning

[155] Avhandlingens punkt 3.1-3.5

gjennomgått. Adgangen til bruk av dataavlesning etter strpl. §§ 216 o og p fremstår ikke som stor, heller tvert i mot. Dette taler for at det er forholdsmessig.

Det er gitt tilstrekkelige og effektive sikringstiltak mot overgrep og vilkårlighet for politiets bruk av dataavlesning. Dette legger jeg til grunn for å være av avgjørende for at dataavlesning på et generelt grunnlag fremstår som forholdsmessig etter EMK art. 8 nr. 2.

5.7 Konklusjon

Jeg har med dette kommet fram til at politiets bruk av dataavlesning i etterforskingsøyemed ikke utgjør en krenkelse av retten til respekt for privatliv etter Grl. § 102 og EMK art. 8.

6 Oppsummering

Under arbeidet med denne avhandlingens tema, fant jeg ut at det var ikke selve reglene for politiets bruk av dataavlesning som skapte hodebry, men de overordnede reglene som fremkommer i Grl. § 102 og EMK art.8.

I seg selv er reglene som fremkommer i strpl. 216 o og p ikke problematiske. Flere hensyn er tatt i betraktning ved utformingen av reglene, og kanskje mest aktuelt i vurderingen har vært rettssikkerhet og personvern. Likevel var det av hensyn til kriminalitetsbekjempelse og den raske teknologiske utviklingen kanskje på tide at vi fikk innført dataavlesning som tvangsmiddel også i norsk rett.

Inngrepsvilkårene for å kunne benytte dataavlesning er strenge, og det skal ligge en mistanke til grunn for å ta i bruk dette tvangsmiddelet. Det er ikke slik at politiet kan gå inn i ethvert menneskets datasystem og foreta dataavlesning, uten grunn, slik jeg på mange måter har oppfattet debatten å dreie seg om. Vi har rettsikkerhetsgarantier som ivaretar at tvangsmiddelet blir benyttet riktig, og begrensningene som følger av Grl. § 102 og EMK art. 8 er med på å forsterke dette ytterligere.

Tiden vil vise hva bruken av dataavlesning vil medføre. Vi vil nok fremover se flere saker hvor dataavlesning blir benyttet, og da vil vi også kunne se om virkemiddelet fungerer etter sin hensikt eller ei.

7 Kildeliste

7.1 Lov

- Kongeriket Norges Grunnlov, gitt i riksforsamlingen på Eidsvoll den 17. mai 1814

- Lov 13 august 1915 nr. 5 om domstolene

- Lov 22 mai 1981 nr. 25 om rettergangsmåten i straffesaker

- Lov 4. august 1995 nr. 53 om politiet

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

- Lov 20 mai 2005 nr. 28 om straff

- Lov 15 juni 2018 nr.38 om behandling av personopplysninger

7.2 Forskrift

- FOR-2016-09-09-1047, Forskrift om kommunikasjonskontroll, romavlytting og dataavlesing

7.3 Offentlige utredninger

- Ot.prp.nr.64 (1998-1999) Om lov om endringer i straffeprosessloven og straffeloven m v (etterforskningsmetoder m v)

- Ot.prp.nr.60 (2004-2005) Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)

- NOU 2009: 15 Skjult informasjon – Åpen kontroll (Metodekontrollutvalget)

- Prop. 147 L (2012-2013) Endringer i straffeprosessloven mv. (behandling og beskyttelse av informasjon).

- Innst.186 S (2013-2014) Innstilling fra kontroll- og konstitusjonskomiteen om grunnlovsforslag, om grunnlovfesting av sivile og politiske menneskerettigheter, med unntak av romertall X og romertall XXIV

- 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.

7.4 Konvensjon

- Europarådets konvensjon 4. november 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter.

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

7.5 Rettspraksis

7.5.1 Høyesteretts praksis

- Rt. 1993 s. 1302

- Rt. 2006 s. 1546

- Rt. 2012 s.1645

- Rt. 2012 s. 2039

- Rt. 2014 s.1105

- Rt. 2015 s.93

- HR-2016-1857-A

7.5.2 Den europeiske menneskerettsdomstols praksis (EMD)

- Klass m.fl mot Tyskland, 6. september 1978 (saksnummer: 5029/71)

- Malone mot Storbritannia, 2. august 1984 (saksnummer 8691/79)

- A mot Frankrike, 23. november 1993 (saksnummer 14838/89)

- Erdem mot Tyskland, 5. juli 2001(saksnummer 38321/97)

- Radaj mot Polen, 28. november 2002 (saksnummer 29537/95) og 35453/97)

- Von Hannover mot Tyskland, 24. juni 2004 (saksnummer 59320/00)

- Kennedy mot Storbritannia, 18. mai 2010 (saksnummer 26839/05)

- Robathin mot Østerrike, 3. juli 2012 (saksnummer 30457/06)

- M.K mot Frankrike, 18. april 2013 (saksnummer: 19522/09)

- Roman Zakharov mot Russland, 4. desember 2015 (saksnummer 47143/06)

7.6 Juridisk litteratur

- Bruce, I. og Haugland, G. S. 2018. 2.utg. Skjulte tvangsmidler. Oslo: Universitetsforlaget

- Harris, O´Boyle og Warbick. 2014. 3.utg. Law of the European Convention on Human rights. Oxford university press.

- Gisle, J. 2007. 3.utg. Jusleksikon. Oslo: H. Aschehough & Co (W.Nygaard) A/S og Gyldendal ASA.

- Aall, J. 2015. Rettsstat og menneskerettigheter. 4. utg. Bergen: Fagbokforlaget

- Øyen, Ø. 2016. Straffeprosess. Bergen: Fagbokforlaget

- Nygaard, N. 2004. Rettsgrunnlag og standpunkt. 2.utg. Oslo: Universitetsforlaget

- Eckhoff, T. 2001. Rettskildelære. 5.utg. Oslo: Universitetsforlaget

- Eskeland, S. 2015. Strafferett. 4. utg. Oslo: Cappelen Damm akademisk.

7.7 Andre kilder

- Årsrapporten 2017 fra Kontrollutvalget for kommunikasjonskontroll: http://www.sivilrett.no/getfile.php/4191952.2254.amkpanuzzpwl77/%C3%85rsrapport+-+kontrollutvalget+for+kommunikasjonskontroll+-+2017.pdf (sist sett 03.12.18).

- Kaldestad, Øyvind H: «Dette betyr de nye personvernreglene for deg» på Forbrukerrådet.no: https://www.forbrukerradet.no/siste-nytt/dette-betyr-de-nye-personvernreglene-for-deg/ (sist sett 09.12.18)

- Senneset, Ingeborg: «Dataavlesning og skjulte tvangsmidler – tidriktige politimetoder» i Aftenposten: https://www.aftenposten.no/meninger/debatt/i/5V01W/Dataavlesing-og-skjulte-tvangsmidler--tidriktige-politimetoder--Benedicte-Bjornland (sist sett 18.01.19)

- Fakta om Datatilsynets oppgaver: https://www.datatilsynet.no/om-datatilsynet/oppgaver/ (sist sett 31.12.18).

- Beskrivelse av IME-nummer: https://www.tek.no/artikler/dette_er_imei-koden/7597 (sist sett 22.02.19)