Om dataavlesing og kontroll mot uberettiget tilgang fra tredjeperson

Blir dataavlesing gjennomført på en måte som etter gjeldende rettssikkerhetsgarantier er tilfredsstillende?

Kandidatnummer: 171

Antall ord: 12 231

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

1. juni 2017

Innholdsfortegnelse

1 Innledning

1.1 Presentasjon av emnet

Dataavlesing ble 9. september 2016 vedtatt som et nytt, skjult tvangsmiddel for politiet og Politiets sikkerhetstjeneste (PST).[1] Metoden kan på ulike vilkår benyttes både i avvergende og forebyggende øyemed, samt som et selvstendig, straffeprosessuelt tvangsmiddel under etterforskning. Metoden er forbeholdt de mest alvorlige lovbrudd, eller forsøk på disse, og krever normalt kjennelse fra retten for å bli iverksatt.[2]

Måten dataavlesing blir gjennomført på, er enkelt fortalt at politiet ved hjelp av programmer eller annet utstyr «hacker» seg inn på en mistenkts datasystem – eksempelvis en datamaskin eller en smarttelefon – og dermed kan avlese opplysninger i et ikke offentlig tilgjengelig informasjonssystem.[3] På denne måten får politiet en uavgrenset tilgang til, og oversikt over, samtlige aktiviteter en mistenkt bedriver på det aktuelle datasystemet, uten at krypteringer og annet setter begrensninger. Politiet foretar en løpende overvåking av all aktivitet på den mistenktes informasjonssystem, og denne informasjonen kan blant annet komme i form av lyd- eller videostrøm, tastetrykklogg eller innholdet på en harddisk eller minnepenn.[4]

Politiet utfører ved dataavlesing et inngrep i en persons innerste, private sfære, og metoden er blitt hevdet å innebære en noe større integritetskrenkelse enn tradisjonell kommunikasjonsavlytting og hemmelig ransaking.[5] Det er dermed viktig at det er etablert tilfredsstillende kontrollmekanismer på alle stadier av avlesingsprosessen for å ivareta personvernet og rettssikkerheten til den mistenkte på en måte som samsvarer med nasjonal lov og menneskerettslige forpliktelser.[6]

Ved utøvelse av dataavlesing kan politiet sies å opptre som lovlige «hackere». Det er derfor grunn til å sette spørsmålstegn ved *hvor* politiet får tilgang til «hacker»-programvare fra og hvordan de sikrer at denne er trygg, *hvordan* de benytter denne programvaren til å uthente

[1] Ved forskrift 9. september 2016 nr. 1046 om delvis ikraftsetting av lov 17. juni 2016 nr. 54 om endringer i straffeprosessloven mv. (skjulte tvangsmidler).
[2] Straffeprosessloven § 216 o første ledd.
[3] Prop. 68 L (2015-2016) s. 224.
[4] Prop. 68 L (2015-2016) s. 224.
[5] Prop. 68 L (2015-2016) s. 265.
[6] Hovedsakelig Grunnloven § 102 og Den europeiske menneskerettskonvensjon artikkel 8.

informasjon, og på *hvilken måte* de sikrer at uberettigede tredjepersoner får tilgang til denne informasjonen. Dette er aspekter ved dataavlesing som i liten grad er adressert i Prop. 68 L (2015-2016), og som på en lite konkret måte blir regulert i de nye lovbestemmelsene. Nettopp dette utgjør et sentralt element i oppgaven – har lovgiver i tilfredsstillende grad evaluert risikoene ved dataavlesing? I en tid hvor datateknologisk utvikling skjer fort og kriminelle til stadighet viser hvor sårbare og gjennomtrengelige datasystemer kan være,[7] tilsier dette at effektive kontrollmekanismer i aller høyeste grad bør være etterstrebet.

I forlengelsen av dette er det, ettersom norske myndigheter ikke produserer en egen, nasjonal hackerprogramvare som politiet benytter, grunn til å anta at politiet kjøper slik programvare av eksterne, ofte utenlandske tilbydere. Politiet blir i så fall en betalende aktør i et omstridt kommersielt gråmarked, og kan da løpe en eventuell risiko for at tilbyderne av dataavlesingsprogramvare kan legge inn en skjult funksjonalitet som innhenter informasjon til andre interessenter enn norsk politi.[8] Dette er problematikk rundt dataavlesing som ikke er adressert i lovproposisjonen overhodet.

Det sentrale formålet med denne oppgaven er følgelig å finne ut hvorvidt kontrollmekanismene rundt selve gjennomføringen av dataavlesing i tilfredsstillende grad oppfyller gjeldende rettssikkerhetsgarantier, og sikrer at uberettigede tredjepersoner ikke får tilgang til informasjonen som fremkommer i etterforskningen.

1.2 Avgrensning mot lignende problemstillinger og begrepsbruk

Dataavlesing er et stort tema som inviterer til mange spennende problemstillinger, og mange av dem kan til tider flyte over i hverandre. Det er derfor nødvendig å avgrense og identifisere oppgavens rammer og formål. Innføringen av dataavlesing som et selvstendig, skjult tvangsmiddel har høstet kritikk fra ulike hold både før og etter lovendringen trådte i kraft. Mye av kritikken går på hvorvidt dataavlesing som etterforskningsmetode i sin helhet er for

[7] Se eksempelvis det siste store, internasjonale hackerangrepet som også rammet Norge. Nærø, Amalie Frøystad, Newth, Magnus og Hvistendahl, Nora Evensmo, *VGs nettutgave,* «Hackerangrep rammet nærmere 100 land» (12. mai 2017), sist lastet ned 12. mai 2017.
[8] Teknologirådets innspill til Prop. 68 L – skjulte tvangsmidler, av 25. mai 2016, s. 2.

inngripende og integritetskrenkende, og strider mot Grunnloven § 102 og Den europeiske menneskerettskonvensjon (EMK) artikkel 8.[9]

Denne oppgaven omhandler kun den *innledende gjennomføringsfasen* ved dataavlesing. Det vil si hvorvidt måten politiet går frem for å anskaffe dataavlesingsprogramvare og installere denne på den mistenktes datasystem – og kontrollen rundt dette – i tilfredsstillende grad ivaretar den mistenktes rettssikkerhet, slik denne grunnleggende rettigheten er forankret i nasjonale og internasjonale regelverk og forpliktelser. Det avgrenses dermed mot å vurdere dataavlesing som skjult tvangsmiddel i sin helhet og hvorvidt metoden er lovlig eller ikke, og fokuseres kun på om metoden – slik som den nå er trådt i kraft – er egnet til ivareta den mistenktes rettssikkerhet på tilfredsstillende måte.

I denne oppgaven vil det for enkelthets skyld kun henvises til politiets anvendelse av dataavlesing som et selvstendig, straffeprosessuelt tvangsmiddel, slik metoden er beskrevet i straffeprosessloven § 216 o og p. Leseren bør imidlertid ha i bakhodet at måten dataavlesing blir gjennomført på er den samme for både politiet og PST, også i avvergende og forebyggende øyemed.[10]

Hva gjelder begrepsbruk, henviser «tredjepersoner» til uberettigede faktiske og juridiske personer som kan få en ikke tiltenkt tilgang til informasjon som anskaffes gjennom dataavlesing. Begrepet må ikke forveksles med utenforstående tredjepersoner i en mistenkts nærmeste omgangskrets, som også blir utsatt for overvåking dersom de benytter samme datasystem som den mistenkte.

Videre kan det til tider være vanskelig å skille mellom innholdet i begrepene «rettssikkerhet» og «personvern». Det er hensynet til disse to begrepene som hele tiden avveies mot hensynet til effektiv kriminalitetsbekjempelse og hvorvidt det kan gjøres inngrep i en persons private sfære, og begge begrepene representerer grunnleggende personlige rettigheter når det kommer til dataavlesing. Disse to begrepene har dog kontinuerlig blitt stilt opp ved siden av hverandre i flere lovforarbeider som omhandler dataavlesing,[11] på en måte som gjør at deres rettighetsinnhold tilsynelatende kan smelte noe sammen. Det er for øvrig nær sammenheng mellom rettssikkerhet og personvern; den grunnleggende verdi som søkes beskyttet i begge

[9] Se blant annet International Commission of Jurists' høringsuttalelse av 6. april 2016.
[10] Se politiloven § 17 d for PSTs hjemmelsgrunnlag og straffeprosessloven § 222 d for politiets hjemmelsgrunnlag for dataavlesing i forebyggende øyemed.
[11] Se for eksempel Prop. 68 L (2015-2016) s. 13.

sammenhenger er den enkelte borgers integritet og autonomi overfor mektige samfunnskrefter.[12] Det er imidlertid nødvendig å separere de to, og avklare hvilket meningsinnhold som ligger i de respektive begrep.

I denne oppgaven vil begrepene bli tillagt samme innhold som Metodekontrollutvalget la til grunn i NOU 2009: 15. Kjernen i begrepet «personvern» innebærer en persons vern mot å bli observert eller overvåket i den innerste personlige sfæren, herunder en rett til å ha kontroll over opplysninger om en selv, særlig opplysninger som oppleves som personlige.[13] Når det gjelder begrepet «rettssikkerhet» og dets kjerne, legges det til grunn at det innbefatter krav om at enkeltindividet skal være beskyttet mot overgrep og vilkårlighet fra myndighetenes side, samtidig som vedkommende skal ha mulighet til å forutberegne sin rettsstilling og forsvare sine rettslige interesser.[14] I punkt 3.1 går jeg nærmere inn på dette begrepet for å bedre stille opp det rettssikkerhetsmessige rammeverket politiet må forholde seg til når det bedriver dataavlesing.

Denne oppgaven fokuserer i all hovedsak på den mistenktes *rettssikkerhet* ved gjennomføring dataavlesing, da jeg mener risikoen for uberettiget tilgang til informasjonen som fremkommer ved dataavlesing best belyses i møte med denne rettigheten. Imidlertid kunne nok oppgaven også vært skrevet kun med en personvernrettslig vinkling, men en rettssikkerhetsmessig vinkling har etter min mening et bredere og mer innbringende nedslagsfelt når det gjelder den aktuelle problemstilling. Det opplyses imidlertid om at risikoer for den mistenktes rettssikkerhet ved gjennomføring av dataavlesing i forlengelsen også kan gjøre seg utslag i risiko for hans eller hennes personvern.

1.3 Aktualitet

Hvorvidt dataavlesing skal innføres som en selvstendig etterforskningsmetode i Norge har, som jeg kommer tilbake til i punkt 2.1.1, lenge vært et tema for diskusjon. Regler om skjulte tvangsmidler bygger på vanskelige vurderinger hvor hensynet til effektiv kriminalitetsbekjempelse må avveies mot hensynet til personvern og rettssikkerhet, og

[12] Prop. 68 L (2015-2016) s. 60.
[13] NOU 2009: 15 s. 21.
[14] NOU 2009: 15 s. 21-22.

ubegrunnede inngrep i den enkeltes rettigheter og private sfære må unngås.[15] Når metoden nå har trådt i kraft, er dette på bakgrunn av flere momenter.

Lovendringen er i hovedsak begrunnet med at politiet har hatt et stort og udekket behov for effektiv tilgang til elektronisk lagret og kommunisert informasjon. I dag blir informasjon i stor grad produsert, bearbeidet, kommunisert og lagret elektronisk og ved bruk av mobile tjenester. Samtidig øker bruken av krypteringsløsninger og andre metoder for beskyttelse av slik informasjon, slik at politiet stadig oftere blir stående uten faktisk tilgang til informasjon som det rettslig sett ellers har adgang til i medhold av de tidligere eksisterende tvangsmiddelbestemmelsene om kommunikasjonsavlytting og hemmelig ransaking. Innføringen av dataavlesing som nytt tvangsmiddel gir politiet mulighet til å oppfylle dette behovet, ved at politiet gis adgang til å følge med på den mistenktes bruk av et datasystem over tid, uavhengig av det tradisjonelle skillet mellom kommunikasjon og lagret informasjon.[16]

Videre er lovendringen begrunnet i et endret kriminalitets- og trusselbilde.[17] Samfunnets behov for beskyttelse defineres av risikoen for kriminalitet som det til enhver tid står overfor. Det er slått fast at utvikling innen organisert kriminalitet viser større mobilitet, mer komplekse lovbrudd, en profesjonalisering av utøvere og større grad av internasjonalisering og multikriminalitet, hvor politiets adgang til skjulte etterforskningsmetoder er en forutsetning for effektiv kriminalitetsbekjempelse.[18] Blant de alvorlige kriminelle handlingene som fremheves som områder hvor dataavlesing kan bidra til en mer effektiv kriminalitetsbekjempelse, trekkes blant annet terrorisme og datakriminalitet som følge av teknologisk utvikling frem.[19]

Den stadig utbredte bruken av krypteringer har som nevnt vanskeliggjort kommunikasjonskontroll fra politiets side, og tilsier at politiet har hatt behov for nye metoder. En tilpassing av regelverk som samsvarer med en ny teknologisk virkelighet har vært nødvendig for at politiets evne til effektiv kriminalitetsbekjempelse skal opprettholdes. På den annen side er det imidlertid også viktig å poengtere at krypteringer styrker samfunnssikkerheten i Norge. Både Utvalget om digitale sårbarheter og

[15] Prop. 68 L (2015-2016) s. 7.
[16] Prop. 68 L (2015-2016) s. 12.
[17] Prop. 68 L (2015-2016) s. 7.
[18] Prop. 68 L (2015-2016) s. 23.
[19] Prop. 68 L (2015-2016) s. 26.

Personvernkommisjonen har blant annet anbefalt at bruken av kryptering ikke bør reguleres eller begrenses.[20] Kryptering gir borgerne nødvendig beskyttelse mot blant annet hacking, identitetstyveri, overvåking og spionasje – spesielt i en tid hvor smarttelefoner, nettbrett og datamaskiner håndterer alt fra banktransaksjoner og helseinformasjon til personlige bilder, e-poster og meldinger. Kryptering er dermed en forutsetning for at innbyggerne i Norge skal ha tillit til sikker kommunikasjon og lagring på sine respektive datasystemer. Dette vil i forlengelse ivareta en ønsket vekst i den digitale økonomien og den økende digitaliseringen av offentlige tjenester.[21]

I lys av at Norges innbyggere i stor grad benytter sine personlige datasystemer til blant annet lagring av sensitiv informasjon og utføring av tjenester som krever slik informasjon, er det essensielt at dataavlesing – hvis informasjonstilgang ikke er begrenset av kryptering – blir gjennomført på en sikker måte. Dette for å sikre at at informasjon som fremkommer under overvåkingen, herunder sensitiv informasjon, ikke kommer på avveie til uberettigede tredjepersoner. Hvorvidt kontrollen rundt dette aspektet ved dataavlesing er god nok, vil gjenstå å se etterhvert som metoden får mer fartstid i det norske politi- og rettsvesen. Det som imidlertid kan sies, er at dette er problemstillinger som i liten grad har blitt berørt og diskutert i både for- og etterkant av lovendringen. Det er dermed en dagsaktuell problemstilling, som det i aller høyeste grad er rom for å diskutere rundt.

1.4 Metodisk tilnærming og den videre fremstilling

Oppgavens formål er som nevnt å forsøke å klargjøre om dataavlesing, slik metoden og dens kontroll mot uberettiget tilgang fra tredjepersoner er implementert og beskrevet i lovverket i dag, blir gjennomført på en måte som tilfredsstiller den mistenktes rettssikkerhet. Det tas dermed sikte på å beskrive gjeldende rett. Vanlig juridisk metode, altså den metoden øverste domsmyndighet i rettssystemet benytter, vil bli anvendt for å gjøre dette.[22] I norsk rett er dette metoden som Høyesterett benytter. Det forutsettes at denne metoden er kjent, og det vil derfor ikke bli redegjort for grunnleggende norsk rettskildelære i det videre. Imidlertid er det visse kildemessige aspekter ved oppgaven det er nødvendig å kommentere innledningsvis.

[20] NOU 2015: 13 s. 16.
[21] Teknologirådets innspill til Prop. 68 L – skjulte tvangsmidler, s. 2.
[22] Se blant annet Mads Henry Andenæs, *Rettskildelære*, 2. utgave, Oslo 2009, og Torstein Eckhoff, *Rettskildelære*, 5. utgave ved Jan E. Helgesen, Oslo 2001.

Mye av det oppgaven omhandler, altså kontroll mot risiko for at uberettigede tredjepersoner får tilgang til informasjon, er i meget liten grad diskutert og problematisert i Prop. 68 L (2015-2016) og de tidligere forarbeidene som omhandler dataavlesing. Dette, i kombinasjon med at lovgivningen er såpass ny at problemstillingen ikke har etterlatt seg spor i rettspraksis enda, gjør at kildetilfanget fra høytstående rettskilder er snevert. På bakgrunn av dette stammer noe av informasjonen fra ekspertorganer innen data og IKT, samt eksempler fra andre land. Imidlertid mener jeg at lovgivers tilnærmede taushet om problemstillingen – sett i lys av det som fremkommer i oppgaven – poengterer og underbygger hvorfor det er viktig å diskutere og sette spørsmålstegn ved nettopp dette aspektet ved dataavlesing.

I det videre vil det i oppgavens del 2 kort forklares hva dataavlesing er, og på hvilke vilkår politiet kan benytte metoden. Oppgavens hoveddel er grovt sett tredelt. Del 3 tar for seg rettssikkerhet og hvilke rettssikkerhetsgarantier som gjør seg gjeldende ved bruk av skjulte tvangsmidler, herunder dataavlesing. Del 4 går inn på hvordan gjennomføring av dataavlesing er lovregulert, samt hvilke kontrollmekanismer som er iverksatt for å avverge risikoen for at informasjonsmateriale fra politiets dataavlesing av mistenkte tilkommer uberettigede tredjepersoner. Oppgavens del 5 omhandler hvilke risikoer for at uberettigede tredjepersoner kan få tilgang til informasjonen som finnes, og i hvor stor grad de kan gjøre seg gjeldende. Denne delen inneholder videre en analyse av hvorvidt kontrollmekanismene på en tilfredsstillende måte ivaretar den mistenktes rettssikkerhet, og om de er effektive sett i lys av de presenterte risikoene. I del 6 vil jeg avslutningsvis forsøke å sammenstille de sentrale poengene og konklusjonene som har kommet frem i løpet av oppgaven, samt presentere noen tanker om veien videre og lovgivningen de lege ferenda.

2 Dataavlesing som skjult tvangsmiddel

2.1 Hva er dataavlesing?

2.1.1 Bakgrunn

Politiets adgang til bruk av skjulte tvangsmidler har vært – og er fortsatt – et omstridt tema på bakgrunn av personverns- og rettsikkerhetsproblematikken som følger med slik bruk.[23] Om dataavlesing bør innføres som politimetode i norsk rett, har vært omtalt og diskutert av flere lovutvalg de siste årene. Bakgrunnen for spørsmålet om innføring av dataavlesing er som nevnt blant annet at kriminalitets- og trusselbildet i Norge de siste årene har endret seg. I tillegg gjør enkeltpersoners økte bruk av krypteringer at de tidligere eksisterende tvangsmidler ikke lengre er formålstjenlige nok til å sikre effektiv kriminalitetsbekjempelse.

I NOU 2003: 18 berørte Lund-utvalget problemstillingen,[24] men kom frem til at spørsmålet lå mer innenfor Datakrimutvalgets kompetanseområde, ettersom metoden reiser kompliserte, tekniske problemstillinger.

Deretter ble spørsmålet igjen drøftet i NOU 2004: 6, hvor Politimetodeutvalgets flertall foreslo å innføre regler som tillater dataavlesing som forebyggende politimetode.[25] Bakgrunnen for dette var at bedre tilgang til moderne krypteringsprogrammer ga mindre informasjon enn tidligere ved bruk av kommunikasjonskontroll som skjult tvangsmiddel. Flertallet fremla at dataavlesing representerer en integritetskrenkelse, men at det burde åpnes for metoden på strenge vilkår. Mindretallet i utvalget mente imidlertid at utvalget ikke var sammensatt for å kunne ta stilling til de kompliserte tekniske spørsmål som flertallets forslag reiste, og mente, som Lund-utvalget, at spørsmålet burde overlates til Datakrimutvalget.[26]

Departementet var, på bakgrunn av de kompliserte tekniske spørsmål rundt metoden, enig i at spørsmålet burde behandles av Datakrimutvalget før det eventuelt ble fremmet forslag om lovendringer. Datakrimutvalget mente på sin side at det måtte utredes nærmere hva metoden

[23] Prop. 68 L (2015-2016) s. 13.
[24] NOU 2003: 19 s. 126-127.
[25] NOU 2004: 6 s. 207-208.
[26] NOU 2004: 6 s. 303.

består av, blant annet fordi begrepet «dataavlesing» er uten et entydig fast innhold. I samråd med Justisdepartementet ble spørsmålet dermed ikke utredet nærmere.[27]

Etter dette ble spørsmålet inntatt i Metodekontrollutvalgets mandat, der utvalget blant annet ble bedt om «å utrede og foreslå regler som tillater at politiet tar i bruk dataavlesing som metode i etterforskingen».[28] Utvalget påpekte at grunnlaget for evalueringen de var satt til å gjøre var mangelfull, ettersom de ikke hadde tilgang til enkeltsaker.[29] Metodekontrollutvalget uttaler blant annet at dataavlesing vil kunne utgjøre et svært kraftig inngrep i enkeltmenneskers personvern, da politiet vil kunne få tilgang til informasjon som ikke har vært kommunisert til andre, og som tilhører brukerens innerste personlige sfære. Videre slo Metodekontrollutvalget fast at dets klare oppfatning var at innføring av dataavlesing som et nytt selvstendig tvangsmiddel må bygge på solid dokumentasjon av behovet, men fant ikke at dette behovet var tilstrekkelig dokumentert. Imidlertid vurderte utvalget at krypteringer kan vanskeliggjøre politiets informasjonstilgang etter de tradisjonelle tvangsmidlene. Det falt derfor ned på en mellomløsning, der dataavlesing ble foreslått for å muliggjøre kommunikasjonskontroll eller hemmelig ransaking av dataanlegget. [30]

Justis- og beredskapsdepartementet la etter dette frem forslag om lovendringer som vil gi politiet en utvidet adgang til å benytte skjulte tvangsmidler ved etterforskning, avverging og forebygging av alvorlige lovbrudd i Prop. 68 L (2015-2016). I lovproposisjonen kompromisser departementet ikke i tråd med forslaget fra Metodekontrollutvalget, og foreslo å fullt ut åpne for at dataavlesing kan benyttes som et selvstendig skjult tvangsmiddel. Dette lovforslaget ble så vedtatt, og trådte i kraft 9. september 2016.[31]

Dataavlesing som et selvstendig, straffeprosessuelt skjult tvangsmiddel er for politiets vedkommende nå regulert av straffeprosessloven § 216 o. Etterforskningsmetoden er forbeholdt de mest alvorlige lovbrudd, og krever at noen med skjellig grunn mistenkes for en handling eller forsøk på en handling som enten kan medføre straff av fengsel i ti år eller mer,

[27] NOU 2007: 2 s. 47.
[28] NOU 2009: 15 s. 21.
[29] NOU 2009: 15 s. 107.
[30] NOU 2009: 15 s. 244.
[31] Ved forskrift 9. september 2016 nr. 1046 om delvis ikraftsetting av lov 17. juni 2016 nr. 54 om endringer i straffeprosessloven mv. (skjulte tvangsmidler).

eller som er inkludert i den uttømmende oppregningen i § 216 o bokstav b.[32] Iverksettelse av dataavlesing krever etter bestemmelsens første ledd kjennelse fra retten.

2.1.2 Begrepet «dataavlesing»

Som nevnt tidligere, er ikke «dataavlesing» noe entydig juridisk eller teknologisk begrep, og refererer heller ikke til en klart avgrenset fremgangsmåte. Legaldefinisjonen av begrepet «dataavlesing» i straffeprosessloven § 216 o første ledd er «avlesing av ikke offentlig tilgjengelige opplysninger i et datasystem». Denne definisjonen ligner den som ble gitt av Metodekontrollutvalget, som definerte begrepet slik: «Avlesing av opplysninger i et ikke offentlig tilgjengelig informasjonssystem ved hjelp av programmer eller annet utstyr.»[33] Det ble i lovproposisjonen slått fast at begrepet kan være dekkende for en rekke ulike fremgangsmåter for å skaffe tilgang til informasjon som produseres, lagres eller kommuniseres i eller mellom elektroniske informasjonssystemer.[34]

Definisjonen favner svært bredt, og innbefatter en teknologi med meget bred funksjonalitet. I forlengelsen av dette må det kunne hevdes at mulighetsrommet for overvåking er stort, noe som igjen resulterer i at det må stilles særdeles høye krav til terskelen for bruk og kontroll av denne metoden. Lovgiver har, for å minimere overvåkingsrommet, innført en del skranker for når bruk av dataavlesing kan forekomme. Etter straffeprosessloven § 216 o tredje ledd kan «tillatelse etter første ledd (...) bare gis dersom det må antas at dataavlesing vil være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort.» Videre kan det etter bestemmelsens fjerde ledd «bare gis tillatelse til å avlese bestemte datasystemer eller brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester som den mistenkte besitter eller kan antas å ville bruke.»

Blant flere mulige varianter ved gjennomføring av dataavlesing, er bruk av «trojanere»[35] og anen tilsvarende programvare nevnt i lovproposisjonen. Politiet kan så plassere slik

[32] Eksempler på kriminelle handlinger inkluderer blant annet frihetsberøvelse etter straffeloven § 254, fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn etter straffeloven § 311, grov narkotikaovertredelse etter straffeloven § 232 og oppfordring, rekruttering og opplæring til terrorhandlinger etter straffeloven § 136.
[33] NOU 2009: 15 s. 17.
[34] Prop. 68 L (2015-2016) s. 224.
[35] Datavirus som mottaker ikke merker at han eller hun får installert i sitt datasystem.

programvare i den mistenktes datasystem for å gi politiet tilgang til den mistenktes kommunikasjon, lagrede informasjon og andre opplysninger om bruken av datasystemet.[36]

I lovproposisjonen er dataavlesing trukket frem som en særlig interessant fremgangsmåte i forbindelse med etterforskning, forebygging og avverging av kriminalitet i form av skjult innhenting av informasjon fra informasjonssystemer som benyttes av mistenkte. Hva gjelder *hvilken type informasjon* som kan avleses av politiet, vil dette variere fra sak til sak. Begrensningene for hva som kan avleses følger teknisk sett bare av hva slags informasjonssystem det er tale om, og funksjonaliteten til program- eller maskinvaren som benyttes. I prinsippet kan dataavlesing blant annet innebære avlesing av lydstrøm fra mikrofon eller høyttaler, videostrøm som sendes fra webkamera, tastetrykk, innholdet på harddisk eller minnepenn, data som hentes inn fra eller sendes ut på internett eller andre nettverk, IP-adresser, geografisk koordinatinformasjon og signalstrømmen mellom tilkoblet skjerm og datautstyret.[37]

I oppgavens del 4 vil jeg gå nærmere inn på fremgangsmåten ved dataavlesing.

[36] Prop. 68 L (2015-2016) s. 12.
[37] Prop. 68 L (2015-2016) s. 224.

3 Rettssikkerhetsgarantier ved gjennomføring av dataavlesing

3.1 Hva er rettssikkerhet?

For å kunne fastslå hvilke rettssikkerhetsgarantier som må være til stede ved bruk av dataavlesing som etterforskningsmetode, må det først avklares hva som ligger i og rundt begrepet «rettssikkerhet». *Rettssikkerhet* er et mye brukt og viktig begrep,[38] men som det kan være vanskelig å angi en presis og allment akseptert definisjon. Kjernen i begrepet ligger imidlertid i at det enkelte individ skal være beskyttet mot overgrep og vilkårlighet fra myndighetenes side, samtidig som vedkommende skal ha mulighet til å forutberegne sin rettsstilling og forsvare sine rettslige interesser.[39]

3.1.1 Rettssikkerhetskrav og –garantier

Innenfor rettssikkerhetssfæren kommer også begrepene «rettssikkerhetskrav» og «rettssikkerhetsgarantier». Det kan også være vanskelig å skille mellom disse begrepene, og de ofte blir brukt om hverandre og gitt samme meningsinnhold.[40] I det videre vil likevel forskjellen på begrepene forsøkes forklares.

Rettssikkerhetskrav kan brukes som en samlebetegnelse på de overordnede kravene enkeltindividet kan stille til myndighetenes handlinger og avgjørelser, så vel materielle som prosessuelle. Materielle rettssikkerhetskrav stiller overordnede krav til en avgjørelses innhold, mens prosessuelle rettssikkerhetskrav angir kravene til hvordan en avgjørelse blir truffet. *Rettssikkerhetsgarantier* kan på sin side sies å være enkeltelementer som hver for seg, og samlet, bidrar til å ivareta rettssikkerhetskravene på en best mulig måte.[41] Eksempler på rettssikkerhetsgarantier er blant annet prinsippet om offentlighet og kravene til utforming av rettens avgjørelser.

[38] Begrepet har også blitt omtalt som et «honnørbegrep» i NOU 2009: 15 s. 60.
[39] NOU 2009: 15 s. 60.
[40] Se eksempelvis Prop. 68 L (2015-2016) s. 21, hvor retten til kontradiksjon blir henvist til som både et rettssikkerhetskrav og en rettssikkerhetsgaranti.
[41] Prop. 68 L (2015-2016) s. 20.

I det materielle rettssikkerhetskravet er hjemmelskravet, altså legalitetsprinsippet, og forholdsmessighetskravet sentrale rettssikkerhetsgarantier. For at myndighetene kan gjøre inngrep mot borgerne, må inngrepet ha hjemmel i lov for å motvirke overgrep og vilkårlighet, og for å muliggjøre at borgerne kan forutberegne sin rettsstilling. Kjernen i forholdsmessighetsprinsippet henviser til en interesseavveining hvor nytten og nødvendigheten av å gjennomføre et inngrep må måles opp mot hvilken belastning dette vil innebære for borgeren.[42]

Den prosessuelle rettssikkerhet innbefatter blant annet kravene til saksbehandling, herunder saksbehandlingsreglene, for iverksetting og kontroll av etterforskningsmetoder. Dette inkluderer regler som har som formål å forhindre at det benyttes tvangsmidler uten materielt grunnlag, som eksempelvis regler om at kjennelse fra retten kreves for å kunne iverksette dataavlesing. Videre er kravene til myndighetenes uavhengighet, objektivitet og saklighet i denne sammenheng viktige rettssikkerhetsgarantier. Disse innebærer blant annet at den som treffer beslutninger må ha den tilstrekkelige distanse til saken, slik at avgjørelser tas uten at utenforliggende eller usaklige hensyn spiller inn. Retten til kontradiksjon, innsyn og underretning, og adgangen til bistand og representasjon er andre prosessuelle rettssikkerhetskrav. Videre er krav til begrunnelse av en avgjørelse, overprøving, kontroll og offentlighet sentrale elementer under den prosessuelle rettssikkerhet.[43]

Det er særlig den prosessuelle rettssikkerhetsgarantien om *kontroll* for å sikre de prosessuelle rettssikkerhetskravene som har relevans i relasjon til oppgavens tema.

3.1.2 Generelt om rettssikkerhetsgarantier ved bruk av skjulte tvangsmidler

I forbindelse med gjennomføring av dataavlesing må hensynet til den mistenktes rettssikkerhet og personvern stadig avveies mot hensynet til effektiv kriminalitetsbekjempelse, ettersom metoden representerer et myndighetsautorisert inngrep i den mistenktes rettigheter og private sfære.[44] Det er imidlertid grunnleggende å påpeke at det vernet mot overgrep og vilkårlighet som rettssikkerhetskravene utgjør, *ikke* er et vern mot inngrep i seg selv. Inngrep i enkeltpersoners rettssfære fra myndighetenes side kan ha legitime

[42] Prop. 68 L (2015-2016) s. 20.
[43] Prop. 68 L (2015-2016) s. 22.
[44] Prop. 68 L (2015-2016) s. 7.

begrunnelser, og er også nødvendige i demokratiske samfunn, som eksempelvis ved etterforskning av alvorlig kriminalitet.[45] Rettssikkerhetskravene og rettssikkerhetsgarantiene skal primært sørge for at inngrepet overfor borgeren skjer innenfor de rettslige rammene som er oppstilt gjennom demokratiske prosesser.[46]

Bruk av skjulte tvangsmidler under etterforskning står i denne sammenheng i en særstilling i norsk straffeprosess. En mistenkt som blir utsatt for skjult etterforskning – det være seg dataavlesing eller andre skjulte tvangsmidler – blir ikke underrettet om dette underveis i prosessen. Dette har klarligvis bakgrunn i at tvangsmiddelet ville mistet sin effektivitet dersom dette ble gjort. Det gjøres dermed et innhugg i den mistenktes grunnleggende rettigheter som følger av kontradiksjonsprinsippet, da han eller hun blant annet ikke får varsel om begjæringen, rettens behandling eller selve gjennomføringen av tvangsmiddelbruken. Den manglende underretningen medfører at den mistenkte mister muligheten til å ta til motmæle mot den mistanke som er kastet over han eller henne eller på ulike måter. Ettersom den straffeprosessuelt grunnleggende rettssikkerhetsgarantien kontradiksjon ikke kan gjøres gjeldende fullt ut for den mistenkte, medfører dette at de øvrige tradisjonelle rettssikkerhetsgarantiene blir enda viktigere på dette området. Videre er det også innført flere kompenserende tiltak – rettssikkerhetsgarantier som bare gjelder ved skjult tvangsmiddelbruk – for å på tilfredsstillende måte ivareta den mistenktes rettssikkerhet.[47]

En måte innhugget i den mistenktes kontradiksjon – og dermed rettssikkerhet – søkes kompensert, er gjennom en økt mulighet for kontroll av politiets skjulte tvangsmiddelbruk. Denne muligheten for kontroll er en helt sentral rettssikkerhetsgaranti hva gjelder skjulte tvangsmidler, og manifesterer seg på flere ulike måter i regelverkene rundt metodene.[48] Blant ulike kontrollformer som finnes, er at tvangsmiddelbruk først kan settes i verk etter tillatelse fra retten, etterkontroll fra retten i de tilfeller hvor påtalemyndigheten har hastekompetanse og overprøving av kjennelser om skjult tvangsmiddelbruk gjennom anke, jf. straffeprosessloven § 377. Videre er skjult tvangsmiddelbruk også gjenstand for løpende kontroll og etterkontroll både internt i påtalemyndigheten og eksternt gjennom Kontrollutvalget for kommunikasjonskontroll og EOS-utvalget.[49]

[45] Ingvild Bruce og Geir Sunde Haugland, *Skjulte tvangsmidler*, Oslo 2014, s. 27
[46] Se blant annet Prop. 68 L (2015-2016) s. 21 og Bruce/Haugland (2014) s. 27.
[47] Bruce/Haugland (2014) s. 28.
[48] Se nærmere NOU 2009: 15 kapittel 11 og Prop. 68 L (2015-2016) punkt 14.7.4.1.
[49] Bruce/Haugland (2014) s. 48-49.

Hvorvidt disse kontrollformene på tilfredsstillende måte ivaretar den mistenktes rettssikkerhet når det gjelder gjennomføring av dataavlesing og risikoen for uberettiget tilgang til informasjon fra tredjepersoner, blir vurdert i oppgavens punkt 4.2 og utover.

3.2 Betydningen av internasjonale forpliktelser

Norge har, gjennom medlemskap i internasjonale organisasjoner og tiltredelse av ulike konvensjoner, påtatt seg en rekke forpliktelser knyttet til bekjempelse av kriminalitet og ivaretakelse av personvern og rettssikkerhet. Disse forpliktelsene har betydning for adgangen til å anvende skjulte tvangsmidler, da straffeprosessloven bare gjelder «med de begrensninger som er anerkjent i folkeretten eller følger av overenskomst med fremmed stat», jf. straffeprosessloven § 4. Dette medfører at både folkerettslige regler og konvensjonsforpliktelser vil supplere, og ved motstrid gå foran, reglene i straffeprosessloven. For de konvensjonene som er inntatt i menneskerettsloven av 1999, følger dette av menneskerettsloven § 3, jf. § 2.[50]

Blant konvensjonene som er inntatt i menneskerettsloven § 2, er Den europeiske menneskerettskonvensjon av 1950 (EMK). Denne konvensjonen har hatt stor betydning for norsk straffeprosess,[51] også – og i nyere tid kanskje spesielt – med hensyn til politiets bruk av skjulte tvangsmidler og kontroll rundt dette. Etter EMK artikkel 1 er statene pålagt å respektere og sikre konvensjonens rettigheter. I dette ligger både en negativ forpliktelse for staten til å avstå fra ulovlige inngrep i rettighetene, og en positiv forpliktelse til å sikre at konvensjonsrettighetene gis en effektiv beskyttelse.[52]

3.2.1 EMK artikkel 8

EMK artikkel 8 er en sentral bestemmelse når det kommer til bruk av skjulte tvangsmidler, herunder dataavlesing. Av artikkel 8 nr. 1 følger det at «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.» Det er åpenbart at dataavlesing innebærer betydelige inngrep i de rettigheter som er vernet etter denne artikkelen. Dataavlesing berører retten til privatliv så vel som korrespondanse, og griper inn i den

[50] At staten skal respektere menneskerettigheter følger for øvrig også av Grunnloven § 110 c, som fastslår at «Det paaligger Statens Myndigheder at respektere og sikre Menneskerettighederne.»
[51] Se Bruce/Haugland (2014) s. 35 med videre henvisninger.
[52] Bruce/Haugland (2014) s. 35.

mistenktes fysiske og psykiske integritet. Videre kan metoden også tenkes rettet mot det private hjem, hvor vernet etter artikkel 8 nr. 1 står særlig sterkt.[5354]

Retten til respekt for privatlivet er likevel ikke absolutt, og innebærer ingen udelt rett for den enkelte til å ha sitt privatliv i fred. I artikkel 8 nr. 2 heter det at «Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.» For å kunne gjøre et lovlig inngrep i de beskyttede rettigheter stilles det således opp tre hovedvilkår; inngrepet må være foreskrevet i lov, det må ivareta anerkjennelsesverdige formål og det må være nødvendig i et demokratisk samfunn. Det siste vilkåret manifesterer seg som både et formåls- og forholdsmessighetskrav. Disse vilkårene er viktige rettssikkerhetsgarantier som bidrar til å verne borgerne mot vilkårlighet og maktmisbruk fra statens side, og både lovgivningen om skjulte tvangsmidler generelt og anvendelsen av den i hvert enkelt tilfelle må tilfredsstille disse vilkårene.[55]

I lovproposisjonen legger departementet til grunn at vilkårene for inngrep i den mistenktes privatliv etter artikkel 8 nr. 2 er oppfylt når det kommer til dataavlesing. Det påpekes at Den europeiske menneskerettsdomstol (EMD) ikke i noe tilfelle har vurdert konkret om vilkårene for å gjøre inngrep ved å benytte dataavlesing som egen metode har vært oppfylt, men at tilnærmingen må være omtrent den samme som ved inngrep gjennom kommunikasjonsavlytting og romavlytting – skjulte overvåkingsmetoder som jo er anerkjente.[56] EMD har også akseptert at lovgivning som åpner for skjult overvåking av kommunikasjon kan være nødvendig i et demokratisk samfunn for å beskytte nasjonal sikkerhet og forebygge uorden og kriminalitet.[57] I forlengelsen av dette kan slik lovgivning, etter omstendighetene, også være egnet til å beskytte andre konvensjonsrettigheter, som også er et anerkjent formål etter artikkel 8 nr. 2.[58]

[53] Prop. 68 L (2015-2016) s. 238.
[54] Grunnloven § 102, hvoretter «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon.» gir i likhet med EMK art. 8 nr. 1 også et generelt vern av privatlivets fred.
[55] Bruce/Haugland (2014) s. 39.
[56] Prop. 68 L (2015-2016) s. 238.
[57] Dom 6. september 1978 *Klass m.fl. mot Tyskland* avsnitt 48.
[58] Bruce/Haugland (2014) s. 41.

Hvorvidt lovgiver har riktig i at dataavlesing som selvstendig tvangsmiddel er egnet til å oppfylle vilkårene i artikkel 8 nr. 2, og dermed representerer et lovlig inngrep i den mistenktes private sfære i det hele tatt, er en interessant problemstilling.[59] Det er imidlertid ikke denne problemstillingen som ligger til grunn for oppgaven, og den vil derfor ikke bli behandlet nærmere. I det videre vil det derimot fokuseres på hvilken rettssikkerhetsstandard og hvilke rettssikkerhetsgarantier som springer ut av EMK artikkel 8 og tilhørende EMD-praksis når det gjelder skjult overvåking, og som har overføringsverdi til dataavlesing.

3.2.2 Rettssikkerhetsgarantier oppstilt av EMD ved bruk av skjulte tvangsmidler

EMD har ikke uttalt seg direkte om dataavlesing. Domstolen har imidlertid i flere saker lagt føringer for hvordan myndighetene kan anvende skjulte tvangsmidler, og hvilke kontrollmekanismer som må være på plass for å ivareta rettssikkerheten til den som blir utsatt for overvåkingen. Det må derfor kunne legges til grunn at de samme rettssikkerhetsgarantiene må gjelde for dataavlesing, spesielt på bakgrunn av at metoden fremstår som noe mer inngripende enn kommunikasjonsavlytting og hemmelig ransaking.[60]

Dommen *Klass m.fl. mot Tyskland* av 1978 var en av de første sakene hvor EMD anerkjente at trekk ved kriminalitetsbildet, og da særlig utviklingen innenfor spionasje og terrorisme, gjorde at myndighetene kunne ta i bruk inngripende midler som hemmelig overvåking av kommunikasjon. Saken omhandlet fem tyske advokater som klaget på tysk lovgivning som ga myndighetene kompetanse til å overvåke deres post- og telefonkorrespondanse, uten plikt til å informere om overvåkningen etterpå. Domstolen understreket at myndighetenes skjulte overvåking av borgerne kun kan aksepteres i eksepsjonelle tilfeller, og at «powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions».[61] Etter dette kan metoder for skjult overvåking bare tillates når det er strengt nødvendig.

Til tross for det strenge nødvendighetskravet EMD har oppstilt for skjult overvåking, har domstolen likevel flere ganger vist tilbakeholdenhet med overprøving av nasjonale myndigheters vurderinger av om slike tiltak er forholdsmessige. I stedet gjør EMD en

[59] Se blant annet International Commission of Jurists' høringsuttalelse til forslag om utvidet overvåking av 6. april 2016 punkt 1 og 5.6 for problematisering rundt dette.
[60] Prop. 68 L (2015-2016) s. 268.
[61] Dommens avsnitt 48.

inngående vurdering av om det i lovgivningen finnes egnede og effektive rettssikkerhetsgarantier mot vilkårlige inngrep og maktmisbruk.[62] Videre har domstolen også understreket at kravene til prosessuell rettssikkerhet er særlig strenge i denne sammenheng, da bruken av hemmelig overvåking ikke er underlagt offentliges undersøkelser.[63] I *Klass*-saken ble vurderingstemaet beskrevet på denne måten:

> «The Court must be satisfied that, *whatever system of surveillance is adopted*, there exists adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by national law.»[64] (min utheving).

Denne uttalelsen står på mange måter som en grunnpilar når det kommer til myndighetsautoriserte inngrep i borgernes private sfære ved skjult overvåking, og gjør seg også klart gjeldende ved dataavlesing, jf. uthevingen. Uttalelsen viser at rettssikkerhetsgarantiene rundt skjult overvåking er strenge, men at det vil bero på en helhetsvurdering i det aktuelle tilfellet om de er oppfylt, basert på hvor inngripende tiltaket er, omfanget og varigheten.[65]

Videre har domstolen flere ganger presisert viktigheten av å ha klare regler i lovgivningen og i kontrollen rundt utføringen av skjult overvåking. I dommen *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* fra 2008, som omhandlet telefonavlytting, fastslo domstolen at det bulgarske politiet ikke var underlagt noen form for ekstern kontroll, verken når begjæring om metodebruk ble fremmet, under gjennomføringen eller i ettertid, og at dette medførte et ikke lovlig inngrep i den private sfære. Det ble videre slått fast at det er:

[62] Se eksempelvis *Klass mfl. mot Tyskland*, dom av 25. februar 1993 *Funke mot Frankrike* og dom av 1. juli 2008 *Liberty m.fl. mot Storbritannia*.
[63] Bruce/Haugland (2014) s. 43.
[64] Dommens avsnitt 50.
[65] Et slikt synspunkt er også fulgt opp i blant annet dom av 2. september 2010 *Uzun mot Tyskland* og dom av 25. september 2001 *P.G og J.H. mot Storbritannia*.

> «essential to have clear detailed rules on the subject, especially as the technology for use is continually becoming more sophisticated.»[66]

Uttalelsen har sin bakgrunn i at hemmelig overvåking er vanskelig å kontrollere – fordi den er hemmelig – og derfor utgjør en trussel mot rettsikkerheten.[67] Videre underbygger uttalelsen også at det er god grunn til å kontrollere bruk av skjult overvåking i størst mulig grad, spesielt i lys av at teknologien stadig utvikles. Uttalelsen forespeiler også, etter min mening, viktigheten av å lage solide rammeverk for kontroll som også hensyntar fremtidig teknologisk utvikling, herunder dataavlesing som skjult tvangsmiddel. Dette underbygges videre av EMDs dynamiske tolkningsstil. Domstolen har selv uttalt at EMK er et «living instrument which (...) must be interpreted in the light of present-day conditions»,[68] hvori dataavlesing klart nok representerer et dagsaktuelt tiltak som omfattes av dette.

Når det gjelder skjult overvåking, krever EMD videre at det i formell lov angis «minimum safeguards» for å forhindre vilkårlige inngrep. Loven må angi hvilke typer kriminelle handlinger som kan danne grunnlag for overvåkingen, den må definere hvilke kategorier mennesker som kan overvåkes, den må oppstille en grense for hvor lenge overvåkingen kan vare, samt oppstille prosedyrer for gjennomgangen, bruken og oppbevaringen av de innsamlede opplysningene.[69] Disse vilkårene synes ivaretatt i den nye lovgivningen,[70] og vil ikke behandles nærmere her.

I forlengelsen av disse «minimum safeguards» som kreves i formell lov, kreves det i tillegg at loven utformer nødvendige kontrollmekanismer for å hindre misbruk og skape tillit til myndighetenes praktisering av inngrepsadgangen.[71] EMD uttalte i *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* at domstolen må kunne si seg:

> «satisfied that there *exists adequate and effective guarantees against abuse*. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the

[66] Dommens avsnitt 75. Dette er også uttalt i dom av 24. april 1990 *Kruslin mot Frankrike,* og gjentatt i flere andre overvåkningssaker.
[67] Dommen samme sted med videre henvisninger.
[68] Dom av 25. april 1978 *Tyrer v. Storbritannia,* avsnitt 31.
[69] Dom av 28. juni 2007 *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,* avsnitt 76.
[70] Straffeprosessloven § 216 o og p.
[71] Inger Marie Sunde, «Dataavlesing som etterforskningsmetode», tidsskriftet *Retfærd* (2012) årgang 35, nr. 1/136 s. 20.

authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.»[72] (min kursivering).

I dette ligger at domstolen krever dokumentasjon for at lovens kontrollmekanismer i det hele tatt eksisterer og er tatt i bruk, slik at retten kan føle seg overbevist om at metoden praktiseres på en betryggende måte. Videre peker denne uttalelsen, etter min mening, i retning av at alle tenkelige risikoer rundt bruken av et skjult tvangsmiddel må kartlegges og evalueres, slik at det er mulig å iverksette et effektivt kontrollsystem rundt det. Dette er et naturlig synspunkt, både i lys av EMDs dynamiske tolkningsprinsipp og videre med hensyn til den teknologiske utviklingen og overvåkingsmulighetene denne fører med seg.

3.3 Rettssikkerhetsgarantier oppsummert

Basert på det foregående i punkt 3.2.1 og 3.2.1, har EMD gitt statene et stort spillerom til selv å bestemme hvilke skjulte metoder de ønsker å tillate. Til gjengjeld har domstolen stilt strenge krav når det gjelder rettssikkerhetsgarantier rundt bruken av skjulte tvangsmidler for å verne borgerne mot misbruk, og for å ivareta deres rettssikkerhet. Disse rettssikkerhetsgarantiene manifesterer seg ofte i krav om omfattende kontroll på alle stadier av overvåkingsprosessen. Kontrollmekanismene må eksistere og i tillegg fungere effektivt for å sikre at den skjulte overvåkingsmetoden i så høy grad som mulig er sikker å bruke. Dette er viktig for å minimere – om ikke eliminere – risikoen for misbruk og vilkårlig bruk.

Som også poengtert i punkt 3.1.2, står skjulte tvangsmidler i en særstilling når det kommer til rettssikkerhetsgarantier, da innhugget i retten til kontradiksjon tilsier et behov for økt og omfattende kontroll. Disse rettssikkerhetsgarantiene danner et grunnleggende bakteppe for all bruk av skjulte tvangsmidler. Etter dette er det rimelig å legge til grunn at dataavlesing, som jo representerer et kanskje mer integritetskrenkende inngrep enn andre tvangsmidler, må være gjenstand for utførlig kontroll som effektivt kan motvirke alle kjente risikoer. I tillegg til integritetskrenkelsen i den innerste sfære som dataavlesing utgjør, reiser metoden også kompliserte, tekniske problemstillinger som igjen kan aktivere risikoer for rettssikkerheten til den mistenkte. Dette taler for at kontrollen med dataavlesing må være spesielt stor for å kunne oppnå de høye rettssikkerhetskravene og –garantiene som EMD har lagt grunn i sin praksis.

[72] Dommens avsnitt 77.

Med dette som utgangspunkt, er spørsmålet som søkes besvart i det videre hvorvidt lovgiver har evaluert alle tenkelige rettssikkerhetsrisikoer i forbindelse med bruk av dataavlesing, og innført dertil egnede kontrollsystemer. Det vil først presenteres en generell oversikt over kontrollmekanismene som er innført.

4 Gjennomføring av dataavlesing

4.1 Innledning

Metodekontrollutvalget har uttalt at det neppe er hensiktsmessig å beskrive mulige gjennomføringsmåter av dataavlesing i detalj. Dette er på bakgrunn av at de tekniske mulighetene er «mange- og forskjelligartede», og at den teknologiske utviklingen «formodentlig vil innebære at en slik beskrivelse raskt blir utdatert».[73] På et overordnet og generelt plan, kan prosessen politiet gjennomgår for å gjennomføre dataavlesing likevel deles inn i tre faser: en *innledende fase* der det teknologiske virkemiddelet som skal forestå avlesingen installeres eller monteres, en *avlesingsfase* kombinert med en fase der opplysningene tilgjengeliggjøres for politiet, samt en *avslutningsfase* der avlesingsmiddelet avinstalleres eller fjernes.[74]

Det er videre slått fast at det finnes to hovedgjennomføringsmåter for hvordan politiet gjennomfører dataavlesing; en software-basert løsning og en hardware-basert løsning.[75] Hvilken gjennomføringsmåte som blir benyttet, vil avhenge av politiets informasjonsbehov og de faktiske forhold i den enkelte sak.

Med en *software-basert* løsning får politiet installert et program, typisk i den mistenktes datamaskin, som gjør politiet i stand til å hente ut informasjon fra datasystemet. Dette kan eksempelvis gjøres ved at politiet utnytter et sikkerhetshull i datasystemet for å installere programmet, ved å sende en e-post som inneholder et skjult vedlegg med det aktuelle programmet, ved å installere programmet i forbindelse med en hemmelig ransaking eller etter å ha utført innbrudd i datasystemet.[76] For at politiet skal få tilgang til informasjonen som avleses på datasystemet, må programvaren enten lagre den, eller sende den via internett eller annet tilknyttet nettverks- eller radioutstyr.[77] Det er i lovproposisjonen imidlertid ikke nevnt *hvor og på hvilken måte* politiet får tilgang til slik programvare fra.

En *hardware-basert* løsning går ut på at det installeres komponenter på for eksempel mistenktes datamaskin, som gjør politiet i stand til å skaffe seg tilgang til informasjon. Dette

[73] NOU 2009: 15 s. 247.
[74] Se nærmere Sunde (2012) s. 14 flg.
[75] NOU 2009: 15 s. 247-248.
[76] Bruce/Haugland (2014) s. 254.
[77] Prop. 68 L (2015-2016) s. 224.

kan blant annet være utstyr som monteres i tastaturet og leser av tastetrykkene («key-logging»), montert utstyr i overgangen mellom tastaturet og selve datamaskinen, for eksempel i en USB-port, som leser av informasjonen som går fra tastaturet til maskinen, eller montert utstyr i en mikrofon som gjør det mulig å fange opp lydsignalene ved kommunikasjon over Internett. Også en rekke andre gjennomføringsmetoder er tenkelige. Imidlertid vil en slik fremgangsmåte, fordi hardware-baserte løsninger forutsetter fysisk tilstedeværelse ved datautstyret, by på større operative vanskeligheter enn de software-baserte løsningene.[78] Ved denne løsningen, får politiet tilgang til informasjonen som avleses ved fysisk tilstedeværelse.

4.2 Kontrollmekanismer rundt gjennomføringen

I forbindelse med innføring av dataavlesing som et selvstendig skjult tvangsmiddel, har behovet for forsvarlig kontroll rundt metoden blitt fremhevet og viet mye plass – helt i tråd med det sterke fokuset EMD har hatt på adekvate og effektive rettssikkerhetsgarantier. Metodekontrollutvalget uttalte blant annet at dataavlesing «bare kan aksepteres dersom kontrollen med inngrepet er forsvarlig.» Utvalget fremhevet også at det kreves «skjerpet kontroll med og dokumentasjon av bruken av et slikt tvangsmiddel»,[79] på bakgrunn av at dataavlesing kan etterlate seg sikkerhetshull, og fordi det gjør seg gjeldende en misbruksrisiko ved at dataavlesingen kan gi tilgang til informasjon som politiet ikke har hjemmel til å innhente.[80]

Flere høringsinstanser har også trukket frem viktigheten av å etablere robuste og tilfredsstillende kontrollsystemer rundt bruken av dataavlesing.[81] Blant annet uttalte Oslo statsadvokatembeter at dataavlesing som gjennomføringsmåte bør forutsette at man kan «etablere tilfredsstillende kontrollsystemer som sikrer mot misbruk eller påstander mot misbruk», og at det kan være av avgjørende betydning for å gi «legitimitet for de regler som innføres».[82] Videre har også departementet stresset betydningen av at dataavlesing skal gjennomføres på en så kontrollert og sikker måte som mulig, og har blant annet uttalt at «inngrepshjemlene må ledsages av objektive kontrollmekanismer for å hindre at noen utsettes

[78] Bruce/Haugland (2014), s. 254.
[79] Begge sitater er hentet fra NOU 2009: 15 s. 249.
[80] Prop. 68 L (2015-2016) s. 248.
[81] Prop. 68 L (2015-2016) s. 258.
[82] Oslo statsadvokatembeters høringsuttalelse av 4. mai 2010.

for uforholdsmessig eller unødvendig belastning som følge av tvangsmiddelbruken og for å hindre misbruk av tvangsmiddeladgangen.»[83]

Det rettssikkerhetsmessige behovet for adekvate og effektive kontrollmekanismer rundt bruken, har manifestert seg på ulike måter i lovverket, og spiller inn i alle faser av gjennomføringsprosessen. Disse blir presentert nedenfor.

Vilkårene som må være oppfylt for at politiet kan iverksette dataavlesing er presentert i straffeprosessloven § 216 o. Flere rettssikkerhetsgarantier i form av kontrollmekanismer presenteres i denne bestemmelsen. Disse er nevnt før, og vil kort bli oppsummert her. For det første ligger kompetansen for å tillate dataavlesing i hver enkelt sak hos retten,[84] jf. første ledd. Påtalemyndigheten er etter Kommunikasjonskontrollforskriften § 3 pliktet til å sende riksadvokaten kopi av enhver begjæring om dataavlesing. Dette er viktig for å sikre rettslig kontroll med påtalemyndigheten, og skape tillit til metodens uavhengighet. Videre er det etter tredje ledd et krav om at dataavlesing må være av «vesentlig betydning» for å oppklare den aktuelle sak, og at oppklaring ellers ville blitt vanskeliggjort i vesentlig grad. Dette er en kontrollmekanisme for å forhindre at en så inngripende etterforskningsmetode blir benyttet i saker hvor dette ikke er absolutt nødvendig. Tillatelsen for gjennomføring av dataavlesing må videre kun rettes inn mot «bestemte datasystemer eller brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester som den mistenkte besitter eller kan antas å ville bruke», jf. fjerde ledd. Denne kontrollmekanismer skal forhindre at overvåkingens omfang blir for stort, og dermed mer inngripende og integritetskrenkende for den mistenkte enn hva som er tiltrengt for å samle den nødvendige informasjon i den enkelte sak. Endelig ligger det etter bestemmelsens femte ledd også en kontrollmekanisme i at tillatelse «ikke kan gis for mer enn to uker om gangen»[85], og at «eventuelt utstyr som er benyttet for å gjennomføre dataavlesingen skal fjernes snarest mulig etter avlesingsperiodens utløp».

Videre angir straffeprosessloven § 216 p rammene for hvordan politiet kan gå frem ved gjennomføring av dataavlesing etter § 216 o. Bestemmelsen gjengis i sin helhet:

[83] Prop. 68 L (2015-2016) s. 259.
[84] Påtalemyndigheten har dog kompetanse til å ta avgjørelsen selv i hastesaker, jf. Forskrift om kommunikasjonskontroll, romavlytting og dataavlesing § 1 annet ledd. Beslutningen med begrunnelse må imidlertid forelegges retten for godkjennelse senest 24 timer etter kontrollen ble påbegynt.
[85] Dette er mindre tid enn ved for eksempel kommunikasjonskontroll, hvor hovedregelen er at tillatelse ikke kan gis for mer enn fire uker av gangen, jf. straffeprosessloven § 216 f første ledd annet punktum.

> «Dataavlesing etter § 216 o kan bare utføres av personell som er særlig skikket til det og som utpekes av politimesteren, sjef PST eller den som bemyndiges. Avlesingen kan foretas ved hjelp av tekniske innretninger, dataprogram eller på annen måte. § 199 a gjelder tilsvarende. Politiet kan bryte eller omgå beskyttelse i datasystemet dersom det er nødvendig for å kunne gjennomføre avlesingen. Tekniske innretninger og dataprogram kan installeres i datasystemet og i annen maskinvare som kan knyttes til datasystemet. Når retten ikke bestemmer noe annet, kan politiet også foreta innbrudd for å plassere eller fjerne tekniske innretninger eller dataprogram som er nødvendig for å gjennomføre dataavlesingen.
>
> Dataavlesingen skal innrettes slik at det ikke unødig fanges opp opplysninger om andre enn mistenktes bruk av datasystemet. Avlesingen skal utføres slik at det ikke unødig voldes fare for driftshindring eller for skade på utrustning eller data. Politiet skal så vidt mulig avverge fare for at noen som følge av gjennomføringen settes i stand til å skaffe seg uberettiget tilgang til datasystemet eller vernet informasjon eller til å begå andre straffbare handlinger.»

I denne bestemmelsen ligger særlige kontrollmekanismer i at personene som utfører dataavlesing må inneha en særskilt kompetanse, og at utenforstående tredjepersoner så godt det lar seg gjøre ikke skal bli rammet av overvåkingen. Videre stilles det krav til at datasystemet til den mistenkte i minst mulig grad skal ta skade av dataavlesingsgjennomføringen, og at politiet «så vidt mulig» skal avverge faren for at tredjepersoner kan få en ikke tiltenkt tilgang til selve datasystemet som er gjenstand for overvåking, og informasjonen som springer ut av det.

For øvrig nevnes også at politiets og påtalemyndighetens behandling av saker med bruk av dataavlesing er gjenstand for ekstern kontroll av Kontrollutvalget for kommunikasjonskontroll i tråd med straffeprosessloven § 216 h første ledd. I tillegg må politiet protokollføre vidstrakt om alle aspekter rundt gjennomføringen, slik Kommunikasjonskontrollforskriften § 7 første og andre ledd krever.

Etter dette kan det synes som om lovgiver i stor grad har tatt høyde for misbruksfarer ved gjennomføring av dataavlesing. Metoden er underlagt omfattende kontroll, på en måte som gjør at borgerne – i den grad det i det hele tatt er mulig å ha tillit til et så inngripende overvåkingstiltak – skal kunne føle seg trygge på at kontrollsystemene vil fange opp misbruk

eller forsøk på misbruk. Det som imidlertid mangler, er et kontrollsystem som innretter seg mot *selve* programvaren som benyttes i dataavlesingen. I det videre diskuteres det om risikoer forbundet med bruk av programvare til dataavlesing tilsier at slik programvare skulle vært underlagt et kontrollsystem for at metoden skal være rettssikker. Dette gjøres særlig i lys av det lovfestede kravet om at politiet «så vidt mulig [skal] avverge fare for at noen som følge av gjennomføringen settes i stand til å skaffe seg uberettiget tilgang til datasystemet eller vernet informasjon eller til å begå andre straffbare handlinger»[86], og på bakgrunn av de strenge rettssikkerhetsgarantiene i form av kontroll EMD har trukket opp.

[86] Jf. straffeprosessloven § 216 p andre ledd, tredje punktum.

5 Risikoen for uberettiget tilgang fra tredjepersoner

5.1 Generelt om risikoer ved bruk av programvare til å gjennomføre dataavlesing

Når det kommer til programvaren politiet benytter i forbindelse med dataavlesing, vet ikke vi som jevne borgere mye. Det vi vet, er at blant flere tenkelige varianter, er bruk av «trojanere og annen tilsvarende programvare» trukket frem som aktuelle.[87] Trojanere er kort fortalt et datavirus som politiet – ved å utnytte svakheter i den mistenktes datasystem – installerer for å kunne gjennomføre dataavlesing. På bakgrunn av at trojanere i utgangspunktet blir brukt av kriminelle og/eller hackere for å infiltrere datasystemer, synes det naturlig å sette spørsmålstegn ved hvor politiet får tilgang til slik programvare fra, og om og eventuelt hvordan de sikrer at denne er trygg å bruke. Ved bruk av programvarer, eksempelvis trojanere, løper en alltid en risiko, da all programvare inneholder feil eller mangler som i større eller mindre grad kan utgjøre en sårbarhet for det aktuelle datasystemet.[88] Spesielt i lys av at informasjonen som fremkommer under etterforskningen i utgangspunktet ikke er ment delt til omverdenen, og kan være av sensitiv karakter, synes det nærliggende å etterstrebe at programvaren som benyttes må være gjenstand for kontrollmekanismer for å forhindre at informasjonen kommer på avveie til uberettigede.

Som det vil bli vist og eksemplifisert for nedenfor, står dataavlesing kanskje i en særstilling av de skjulte tvangsmidlene hva gjelder risiko for misbruk. Dette har blant annet sin bakgrunn i at trojanerne som benyttes av politiet kan være mulige for andre å avdekke, samt at det ikke er utarbeidet formelle krav om at programvaren som benyttes må gjennomgå en sikkerhetstest eller andre kontrollformer i *forkant* av bruken.

[87] Prop. 68 L (2015-2016) s. 12.
[88] Prop. 68 L (2015-2016) s. 266-267.

5.2 Vurderinger av risikoene i forarbeidene og tiltak i lov

Selv om det ikke finnes et eget lovregulert kontrollsystem eller en sikkerhetstest som innretter seg mot selve programvaren, har problemstillingen til en viss grad blitt berørt i forarbeidene. Metodekontrollutvalget pekte i sin utredning på at politiet, overfor kontrollmyndigheten:

> «må være i stand til å dokumentere hva slags programvare eller maskinvare som er benyttet, herunder angivelse av leverandør, leverandørens programnavn og/eller produktnavn, versjonsangivelse, og påtegningen av hvilke modifikasjoner eller tilpasninger som er gjort med programvaren eller hardwaren dersom man ikke benytter programvaren eller hardwaren slik den leveres av leverandøren.»[89]

Denne oppfordringen ser imidlertid ikke ut til å ha manifestert seg tilstrekkelig i Kommunikasjonskontrollforskriften. I forskriftens § 7 første og annet ledd oppstilles 17 aspekter som må protokollføres ved gjennomføringen av dataavlesingen, men ingen av dem innretter seg direkte på dokumentasjon av programvaren, dens produktnavn, versjonsangivelse eller lignende. Det nærmeste synes å være § 7 annet ledd nr. 3, hvoretter det skal protokollføres «hvorvidt det er benyttet tekniske innretninger, maskinvare eller programvare ved dataavlesingen.» Dette protokollkravet er dog noe overfladisk og generelt, og går ikke i dybden på programvarens kvaliteter, som Metodekontrollutvalget anbefalte og etterspurte kontroll med.

Videre er protokollføringen som stilles opp i Kommunikasjonskontrollforskriften § 7 ment å sikre etterfølgende kontroll og notoritet rundt bruken av dataavlesing. På grunn av dette er protokollføringen nettopp *etterfølgende*, og dermed ikke egnet til å fange opp rettssikkerhetsrisikoer før en eventuell skade har skjedd.

I lovproposisjonen anerkjenner departementet at dataavlesing:

> «innebærer (...) en viss risiko for at det utilsiktet voldes skade på datasystemet og for at andre enn politiet settes i stand til å skaffe seg uberettiget tilgang til datasystemet eller opplysninger som behandles i systemet. For eksempel kan det tenktes at det ved

[89] NOU 2009: 15 s. 248.

gjennomføringen skapes sikkerhetshull eller oppstår fare for at andre kan «overta» eller utnytte programvaren som politiet benytter.»[90]

Metodekontrollutvalget uttalte i forbindelse med disse problemstillingene i sin utredning at:

> «Utvalget har vært opptatt av at dataavlesingen må innebære så liten sikkerhetsrisiko for mistenktes datasystem som mulig. (...) Utvalget er videre opptatt av at eventuelle sikkerhetshull må tettes så snart som mulig etter at de er oppstått. All programvare inneholder feil eller mangler som i større eller mindre grad kan utgjøre en sårbarhet for det aktuelle datasystemet. Ved politiets installasjon av programvare for å muliggjøre dataavlesing kan slike svakheter utnyttes. Det innebærer at også andre kan utnytte de samme svakhetene. I tillegg vil politiets programvare kunne inneholde svakheter som kan utnyttes av andre. Ved installasjon av hardware- eller software-baserte avlyttingsløsninger som skal kommunisere data tilbake til politiet over en eller annen form for kommunikasjonsnettverk, som for eksempel kan være radio, Internettet eller GSM-nettet, vil det være nødvendig å sette inn tiltak for å hindre uvedkommende i å fange opp disse dataene, eller overta og kontrollere avlyttingsløsningen. Det er for utvalget opplyst at selv kriminelle som foretar innbrudd i datasystem regelmessig tetter de sikkerhetshull som er utnyttet for å verne om det datasystemet de har skaffet seg kontroll over. Det samme vil selvsagt også politiet kunne gjøre.»[91]

Det synes som om noen av disse problemstillingene er søkt løst i straffeprosessloven § 216 p annet ledd siste punktum, hvor det heter at politiet «så vidt mulig [skal] avverge fare for at noen som følge av gjennomføringen settes i stand til å skaffe seg uberettiget tilgang til datasystemet eller vernet informasjon eller til å begå andre straffbare handlinger». Etter Kommunikasjonskontrollforskriften § 7 annet ledd nr. 6 er politiet også pålagt å føre protokoll for «hvilke risikoer datasystemet har vært utsatt for ved dataavlesingen, og informasjon om hva som har vært foretatt for å avverge fare for driftshindring eller for skade på utrustning eller data, samt fare for at noen som følge av gjennomføringen settes i stand til å skaffe seg uberettiget tilgang til datasystemet eller vernet informasjon.»

Hva som ligger i vilkåret om at politiet «så vidt mulig» skal avverge fare for at noen, på bakgrunn av gjennomføringen av dataavlesing, settes i stand til å skaffe seg en uberettiget

[90] Prop. 68 L (2015-2016) s. 266.
[91] NOU 2009: 15 s. 248.

tilgang, kan virke noe generelt og uklart. Forarbeidene har heller ikke presisert hva som ligger i dette vilkåret. En naturlig, språklig forståelse tilsier imidlertid at politiet skal strekke seg så langt som mulig innenfor de tids- og ressursrammene de har blitt gitt for å forhindre at uberettigede tredjepersoner får en ikke tiltenkt tilgang til informasjonen. Sannsynligvis vil dette vilkåret oppfylles ved at eventuelle «sikkerhetshull» i datasystemet må bli tettet så fort som mulig, slik at andre enn politiet ikke får utnytte samme «sikkerhetshull» og tilegne seg informasjon på lik linje med politiet.[92] Det må dog sies å være et tankekors at politiet blir pålagt å «så vidt mulig» avverge fare for at uberettigede tredjepersoner får tilgang til informasjon, samtidig som programvaren de anvender ikke er gjenstand for et selvstendig kontrollsystem.

Etter min mening er et selvstendig kontrollsystem – som godkjenner eller underkjenner programvaren som benyttes før den blir tatt i bruk – i tillegg til politiets etterfølgende avvergelse av fare for at noen får en uberettiget tilgang til risikoen, i mye større grad egnet til å effektivt minimere denne risikoen. Som Inger Marie Sunde påpeker i sin artikkel «Dataavlesing som etterforskningsmetode», har Metodekontrollutvalget kanskje ikke klart å skille mellom sårbarhet og sikkerhetsrisikoer som politiet *selv* skaper ved gjennomføringen og må ta ansvar for, og sårbarhet som allerede eksisterer på programvaresystemet.[93]

Videre har Metodekontrollutvalget, med tanke på risiko for uberettiget tilgang fra tredjepersoner, uttalt at:

> «Med hensyn til eventuelle «sikkerhetshull», gjør utvalget (...) gjeldende at disse må tettes «så snart som mulig etter at de er oppstått».[94] Det pekes på at politiet må iverksette nødvendige tiltak for å hindre at uvedkommende utnytter svakheter i den programvaren politiet benytter, og at overføring av informasjon tilbake til politiet ikke avlyttes av andre. Utvalget vurderer sikkerhetsrisikoen, herunder *faren for at andre utnytter svakheter eller sikkerhetshull som oppstår ved dataavlesingen, som «liten, og uansett innenfor et akseptabelt nivå»*. Faren for misbruk må etter utvalgets oppfatning inngå som et element i forholdsmessighetsvurderingen i hvert enkelt tilfelle.»[95] (min kursivering).

[92] Prop. 68 L (2015-2016) s. 248.
[93] Sunde (2012), s. 23.
[94] NOU 2009: 15 s. 248.
[95] Prop. 68 L (2015-2016) s. 248.

Men, er virkelig risikoen for at andre utnytter svakheter eller sikkerhetshull som oppstår ved dataavlesingen så liten at det er akseptabelt å ikke adressere den nærmere og innføre strengere kontrollsystemer? Dette er tema i det videre.

5.3 Uadresserte risikoer ved gjennomføring av dataavlesing

5.3.1 Hvor får politiet tak i programvaren fra?

Et viktig spørsmål som ikke blir besvart i hverken forarbeider eller lov, er *hvor* politiet får tilgang til dataavlesingsprogramvare fra. Spørsmålet er viktig fordi svaret kan angi i hvor stor grad behovet for kontrollmekanismer rundt programvaren gjør seg gjeldende. Det er god grunn til å anta at politiet kjøper dataavlesingsprogramvare av eksterne, ofte utenlandske kommersielle tilbydere, ettersom norske myndigheter ikke har utviklet en egen, statlig programvare for dataavlesing.[96]

Det er også grunn til å poengtere – selv om det mulig faller noe utenfor oppgavens rammer – at dersom politiet kjøper slik programvare av kommersielle tilbydere, står det i fare for å bli en betalende aktør i et omstridt gråmarked. Dette har bakgrunn i at sikkerhetshull på datasystemer blir utnyttet for å gi betalende aktører tilgang til andres maskiner, i stedet for at de blir rapporterte inn til programvareprodusenten. Dette dreier seg, som Teknologirådet påpeker i sitt innspill, om handel i digitale sårbarheter i et gråmarked.[97] Ulike menneskerettighetsorganisasjoner har også pekt på at flere selskaper som tilbyr slik programvare, også har solgt sine tjenester til regimer som bruker teknologien for å spionere på politiske motstandere og mot aktivister.[98] I forlengelsen av dette, vil politiet da paradoksalt nok undergrave arbeidet for styrket samfunnssikkerhet samtidig som det forsøker å jobbe for det.

En annet mulighet, er at politiet benytter seg av programvarer som i andre land er spesielt utviklet med tanke på politiets behov for slik overvåking. Slike programvarer finnes det et internasjonalt teknologimarked for politiet for, og disse kan utvikles innenfor en myndighets

[96] Se blant annet Teknologirådets innspill til Prop. 68 L (2015-2016) s. 2 og Sunde (2012) s. 22.
[97] Teknologirådets innspill til Prop. 68 L (2015-2016) s. 2.
[98] SurPRISE – surveillance, privacy and security, D 3.1 Report on surveillance technology and privacy enhancing design, s. 33-44.

egne organisasjoner, innad i politiet eller andre sikkerhetsetater. Et eksempel er National Security Agency i USA, samt enkelte kommersielle bedrifter som har avtale med myndighetene. Programvarer som er utviklet innenfor en organisasjon deles ofte med tilsvarende organisasjoner på tvers av landegrenser, med forbehold om at teknologien ikke skal gjøres alminnelig kjent. Resultatet vil uansett være at politi- og sikkerhetsetater verden over kan kjenne til hverandres teknologi.[99] Dette kan være både positivt og negativt. Positivt i den forstand at etatene kan utveksle erfaringer og lettere samarbeide i saker som krysser landegrenser, negativt i den forstand at risikoen for misbruk øker dersom alle benytter seg av samme programvare.

Felles for de to måtene å få tak i dataavlesingsprogramvare på, er imidlertid at de begge potensielt kan øke risikoen for jurisdiksjonsproblemer. Når programvaren kjøpes fra utlandet, er det stor sannsynlighet for at informasjonen vil gå via servere i andre lands jurisdiksjon, og informasjonen kan dermed risikere å bli plukket opp av andre enn bare norsk politi.

5.3.2 Skjulte funksjonaliteter i programvare for dataavlesing

Et annet moment som ikke er problematisert i forarbeidene, er risikoen for at eksterne tilbydere av dataavlesingsprogramvare kan legge inn skjult funksjonalitet som innhenter informasjon til andre interessenter enn norsk politi.[100] Dette momentet har også Gisle Hannemyr, universitetslektoren som blant annet var med å kvalitetssikre de teknologiske aspektene i Metodekontrollutvalgets utredning, påpekt i intervju. Han har uttalt at norske myndigheter ikke har full kontroll over programvaren som benyttes, og at dette i det minste innebærer en risiko for at programvaren kan «ringe hjem» og levere data til produsenten eller aktører som produsenten samarbeider med – at det kan finnes en «trojaner i trojaneren». Han påpeker videre at det finnes metoder å skjule en slik trojaner på, som selv ikke kan oppdages selv om man har tilgang til kretsdiagrammer eller kildekoden.[101]

Ut ifra disse synspunktene, synes et rimelig alternativ å være at norske myndigheter selv må utarbeide en egen programvare som benyttes i forbindelse med dataavlesing for å sikre best mulig kontroll. Med tanke på at slike skjulte funksjonaliteter nettopp er skjulte, kan det være vanskelig – selv for et kontrollerende sikkerhetssystem – å avdekke risikoen for at skjulte

[99] Sunde (2012), s. 22.
[100] Teknologirådets innspill til Prop. 68 L s. 2.
[101] Wærstad, Lars, «– Det er ikke forbudt å tenke onde tanker. Så galt kan det gå om politiet får retten til å dataavlese Norges innbyggere», *Nettavisens Side3*, (25. mai 2016), sist lastet ned 12. april 2017.

funksjonaliteter finnes i programvaren. Dette er også anbefalingen fra Teknologirådet, idet en slik løsning i større grad vil gi forsikring om at informasjon ikke kommer på avveie til tredjeparter, og kanskje også forenkle politiets og tilsynsmyndigheters tilgang til kildekode.[102] At denne risikoen ikke engang er problematisert i forarbeidene, eller forsøkt kontrollert i lov, kan vitne om en enten manglende teknologisk innsikt i de programvarer som benyttes, eller en utilstrekkelig og mangelfull evaluering av risikoer knyttet til dataavlesing. Uansett tilsier det faktum at det i det hele tatt finnes en mulighet for at skjulte funksjonaliteter kan forekomme i programvaren som benyttes til dataavlesing, at dette er et område som både krever og fortjener tilfredsstillende kontrollmekanismer, som per i dag ikke eksisterer.

5.3.3 Risikoen for at andre kan avdekke bruk av trojaner

Som Inger Marie Sunde fremhever i sin artikkel, kan Bakdørsaken i Rt. 2004 s. 1619 illustrere på hvilken måte dataavlesing ved bruk av trojaner kan synes å stå i en særstilling med tanke på risiko for misbruk. I denne saken ble to menn domfelt for datainnbrudd og dataskadeverk mot flere hundre datamaskiner verden over. Måten de gikk frem på for å bryte seg inn i servere, var at de brukte et skanneprogram som – etter fullført skanning – opprettet en logg som blant annet viste hvilke datamaskiner som har den type program og programdetaljer de søkte etter. Grunnen til at det ble søkt etter bestemte versjoner av programmer var at de tiltalte hadde funnet ut at enkelte programversjoner inneholdt svakheter som de kunne utnytte. Slike svakheter i programmer kan i tillegg være offentlig kjent og publisert på offentlig tilgjengelige internettsider, og kan dermed være gjenstand for utnytting. Det finnes videre en rekke svakheter utviklet i slike «exploit-programmer» - dataprogrammer som har som formål å utnytte svakheten, slik at man får tilgang til datamaskinen som kjører det aktuelle dataprogram.[103]

Etter dette kan kjente trojanere (exploit-programmer) avdekkes ved automatiske søk på Internett. Dette gjelder også polititrojanere dersom politiet tilegner seg programvaren fra alminnelige, kommersielle aktører. I forlengelsen av dette, og på bakgrunn av at disse individenes kommunikasjonsutstyr også kan være tilgjengelige for andre politi- og sikkerhetsetater i verden, betyr dette at politiet ved installering av trojaneren kan skape en allment tilgjengelig sårbarhet på den mistenktes datamaskin som også kan avdekkes og

[102] Teknologirådet innspill til Prop. 68 L, s. 3.
[103] Sunde (2012), s. 12.

utnyttes av andre.[104] Dette må sies å representere en alvorlig risiko ved fremgangsmåten, som ikke har vært problematisert eller blitt viet oppmerksomhet av lovgiver.

5.3.4 Erfaringer fra Tyskland

Alternativet til å kjøpe programvare til dataavlesing fra kommersielle aktører eller av andre politi- eller sikkerhetsetater, er som nevnt at Norge kan utvikle en slik programvare i nasjonal regi. Skal dette gjøres, kan det være nyttig å se hen til Tyskland og hvordan problemstillingen har blitt behandlet der. I forbindelse med overvåking av internettelefoni før kryptering, avdekket den tyske hackergruppen Chaos Computer Club flere svakheter ved en trojaner som var utviklet og brukt av tysk politi.[105]

Svakhetene gjaldt blant annet at svak sikkerhet og kontroll i form av dårlig kryptering og autentisering av trojaneren. Dette gjorde det mulig for hackergruppen å skaffe seg tilgang til alle maskiner som var infisert av trojaneren og ta kontroll over disse. Denne dårlig sikrede programvaren gjorde dermed at både datasystemene til de som ble overvåket og politiet var sårbare for misbruk av tredjeparter. Videre gjorde svakhetene i programvaren seg gjeldende i form av jurisdiksjonsproblemer. Kommunikasjonen mellom trojaneren og tysk politi gikk via servere i USA, der de innhentede dataen fra etterforskningen løp en risiko for å bli eksponert for overvåking fra amerikanske sikkerhetsmyndigheter. I tillegg hadde hackergruppen mulighet til å installere og kjøre hvilket som helst program på den infiserte maskinen, til og med funksjonaliteter som gikk utover skrankene i tysk lov, som eksempelvis mulighet til å aktivere webkameraet til den infiserte maskinen eller å plante bevis på den.[106]

Disse erfaringene fra Tyskland viser hvor kompliserte de tekniske problemstillingene rundt metoden som muliggjør dataavlesing er, og hvilke utfordringer kontroll- og tilsynsmyndighetene står overfor. Som poengtert av Teknologirådet, var det tross alt et hackermiljø, og ikke et tysk tilsynsorgan som varslet om svakhetene som fantes i programvaren. Dette kan tilsi at politiet kanskje har fått rettslige rammer til å bedrive dataavlesing som potensielt går langt på vei overgår den reelle muligheten og kompetansen de har til å kontrollere det. Dette er komplisert og avansert teknologi, som i aller høyeste grad

[104] Sunde (2012), s. 23.
[105] Teknologirådets innspill til Prop. 68 L, s. 2 med videre henvisninger.
[106] Teknologirådets innspill til Prop. 68 L, s. 3 med videre henvisninger.

tilsier at skranker for selve teknologien og programvaren som muliggjør dataavlesing må inkluderes i den tekniske utformingen av verktøyet.[107]

5.4 Er gjeldende kontrollmekanismer tilfredsstillende rettssikkerhetsgarantier i lys av risikoene?

De gjeldende kontrollmekanismene som i dagens lovgivning sikter seg inn på dataavlesing og risikoen mot uberettiget tilgang til informasjonen som fremkommer under etterforskning, blir som nevnt bare lovregulert i straffeprosessloven § 216 p siste ledd. Etter denne bestemmelsen skal politiet «så vidt mulig» avverge fare for at noen som følge av gjennomføringen settes i stand til å skaffe seg uberettiget tilgang til datasystemet som blir overvåket. I lys av de presenterte risikoene, som ikke engang har blitt tilstrekkelig problematisert og trukket frem i lovforarbeidene, synes dette som en mager kontrollmekanisme i et hav av uadresserte risikoer. Politiets kompetanse og reelle mulighet til å føre effektiv kontroll er liten, og kommer inn for sent i prosessen til å kunne imøtegå disse risikoene på en formålstjenlig måte.

På bakgrunn av de strenge føringene EMD har lagt når det kommer til å sette inn effektive rettssikkerhetsgarantier i form av kontroll, synes ikke dagens ordning å kunne oppfylle kravet til at kontrollmekanismer skal eksistere og være effektive. Det er høyst problematisk at programvaren som benyttes i gjennomføringen av dataavlesing ikke er gjenstand for krav eller kontroll hva gjelder dens tekniske utforming og opphav. Den etterfølgende protokollføringen som fremgår av Kommunikasjonskontrollforskriften § 7 kommer også inn for sent i prosessen, og er ikke egnet til å redusere de presenterte risikoene på noen måte.

Videre kan det tilsynelatende virke som om de risikoer som er nevnt i forarbeidene går på sårbarhet og sikkerhetsrisikoer som politiet selv skaper ved gjennomføringen av dataavlesing, i stedet for på selve programvaren som benyttes. At programvaren politiet benytter ikke er underlagt noen form for lovregulert kontroll, er helt klart problematisk i lys av de presenterte risikoene som finnes. Den manglende kontrollen må også gjøre seg gjeldende i form av at metoden ikke er egnet til å ivareta rettssikkerhetsgarantiene som den er ment å ha. EMDs praksis har utpenslet krav om at kontrollsystemer må *eksistere*, og den ikke-eksisterende kontrollen på dette området må følgelig føre til at metoden dermed ikke oppnår dette kravet. Dette vil igjen kunne føre til at man potensielt står overfor et inngrep i en mistenkts innerste,

[107] Teknologirådets innspill til Prop. 68 L, s. 3.

personlige sfære som ikke er legitimt i tråd med EMK artikkel 8 nr. 2. Hvorvidt domstolen vil ta stilling til denne type problemstilling i fremtiden vil bli spennende å se.

Uansett hvor liten risikoen for at uberettigede personer får tilgang til informasjon som fremkommer ved politiets dataavlesing måtte være, så *er den der*. På det datateknologiske feltet, som stadig utvikles og kompliseres, og hvor eventuell realisering av de nevnte risikoer kan ha meget store konsekvenser for både den mistenkte og politiet, er det uklokt å ikke ha et robust og vidstrakt kontrollsystem i bunn. Dataavlesing er et felt som reiser mange og kompliserte tekniske utfordringer. Det er etter min mening et felt hvor man bør lytte til datafaglige ekspertorganer, og det kan potensielt koste dyrt å ikke innføre et kontrollsystem for mye enn for lite.

6 Oppsummering og veien videre

Som vist i det foregående, er risikoen for at tredjepersoner kan få tilgang til sensitiv informasjon som politiet har hentet ut fra en mistenkts datasystem ved dataavlesing, absolutt til stede. I forarbeidene er det ikke blitt tatt tilstrekkelig høyde for denne risikoen, og de kontrollmekanismer som er iverksatt for å motvirke risikoen er som vist utilstrekkelige for å imøtegå risikoene effektivt. Kontrollen som eksisterer i lovverket i dag, er ikke egnet til å oppfylle gjeldende rettssikkerhetsgarantier på en tilfredsstillende måte.

Å ikke innføre et kontrollsystem for programvaren som benyttes, vitner etter min mening om manglende forståelse for datakriminalitet, hackervirksomhet og teknologiutvikling. Teknologien, herunder teknologien som benyttes av kriminelle for å utnytte «bakdører» med det formål å tilegne seg uberettiget informasjon, er mer avansert og kan utvikle seg raskere enn lovgiver etter gjeldende rett har tatt høyde for. At noe ikke ansett som en nevneverdig risiko av lovgiver betyr ikke at risikoen ikke eksisterer, og med lovbestemmelser som har en side til datakriminalitet bør lovgiver være særlig aktsom på sikkerhets- og kontrollmekanismene. Det er spesielt viktig at lovgiver tar høyde til samtlige risikoer ved en så inngripende og integritetskrenkende metode som dataavlesing representerer.

Hvis lovgiver ikke fullt og helt kan garantere at tredjepersoner ikke har mulighet til å tilegne seg sensitiv informasjon hentet fra dataavlesingsoperasjoner, er ikke metoden tilfredsstillende kontrollerbar, og borgernes rettssikkerhet står da i fare.

Jeg synes Teknologirådet kom med flere fornuftige forslag i sitt innspill til lovproposisjonen for å fremme sikkerhet, kontroll og tilsyn. For det første bør dataavlesingsverktøy og –programvare utvikles i Norge. Politiet har etter dagens lov stor frihet til selv å velge hvilken fremgangsmåte de vil for å gjennomføre dataavlesingen, også hva gjelder tekniske hjelpemidler og dataprogramvare. For at borgerne skal ha tillit til politiets overvåkingsvirksomhet, krever dette innsikt i hva programvaren faktisk gjør, og hvilken kontroll som føres med bruken. Det kan være formålstjenlig at norske myndigheter utvikler dataavlesingsverktøy for å gi norsk politi og tilsyn tilstrekkelig kontroll. Dette kan videre i større grad forsikre om at informasjon ikke kommer på avveie til uberettigede tredjepersoner, og kanskje også forenkle politiets og tilsynsmyndigheters tilgang til kildekode.

Videre kan det være hensiktsmessig å kreve at verktøyene som benyttes i forbindelse med dataavlesing må bestå en sikkerhetstest for å kunne benyttes i gjennomføring av dataavlesing. De nevnte erfaringene fra Tyskland viser at dataavlesing både kan medføre en sikkerhetsrisiko for den som overvåkes og for politiet. En måte å bedrive effektiv sikkerhetstesting på, er å innføre strenge sertifiseringskontroller av en egnet sikkerhetsmyndighet for å motvirke at både politiets og den overvåkedes datasystemer gjøres sårbare for angrep fra tredjeparter, og at kommunikasjonen mellom den overvåkedes datasystem og politiet gjøres tilgjengelig for andre.

I tillegg er det et poeng at data, i form av informasjon som springer ut av dataavlesingen, bør holdes innenfor norsk jurisdiksjon. Som vist i saken fra Tyskland, kan kommunikasjonen mellom datasystemet til den overvåkede og politiet være sårbar for overvåkning fra tredjeparter i andre land, som eksempelvis fremmede politi- og sikkerhetstjenester. Dette er uheldig, og så vidt mulig bør derfor ikke dataavlesingen benytte seg av teknisk infrastruktur i andre jurisdiksjoner.[108]

Oppsummert viser dette at det, i lys av de presenterte risikoer, i stor grad er rom for innføring av nye kontrollsystemer når det gjelder dataavlesing og verktøyene og programvaren som blir benyttet i denne sammenheng. For å i det hele tatt kunne ha effektive kontrollmekanismer, er det en forutsetning at en må evaluere samtlige risikoer, og lage tilpassede kontrollsystemer deretter. Dette er nødvendig for å sikre at metoden tilfredsstiller kravene og garantiene til rettssikkerhet som er utpenslet i EMD og norsk straffeprosess for øvrig.

[108] Teknologirådets innspill til Prop. 68 L, s. 3-4.

Kilderegister

Lover, forskrifter, konvensjoner mv.

Lover

Kongeriket Norges Grunnlov, gitt i riksforsamlingen på Eidsvoll den 17. mai 1814, sist endret ved stortingsvedtak 24. mai 2016.

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 lov om straff

Lov 17. Juni 2005 nr. 87 om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)

Lov 17. juni 2016 nr. 54 om endringer i straffeprosessloven mv. (skjulte tvangsmidler)

Forskrifter

Forskrift 9. september 2016 nr. 1046 om delvis ikraftsetting av lov 17. juni 2016 nr. 54 om endringer i straffeprosessloven mv. (skjulte tvangsmidler)

Forskrift 9. september 2016 nr. 1047 om kommunikasjonskontroll, romavlytting og dataavlesing (kommunikasjonskontrollforskriften)

Konvensjoner

Convention for the Protection of Human Rights and Fundamental Freedoms. Vedtatt 4. november 1950, Roma, trådte i kraft 3. september 1953.

Forarbeider og andre offentlige dokumenter

Forarbeider

NOU 2003: 19 Makt og demokrati

NOU 2004: 6 Mellom effektivitet og personvern. Politimetoder i forebyggende øyemed

NOU 2007: 2 Lovtiltak mot datakriminalitet

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

Prop. 68 L (2015-2016) Endringer i straffeprosessloven mv. (skjulte tvangsmidler)

Andre offentlige dokumenter

Teknologirådets innspill til Prop. 68 L (2015-2016) – skjulte tvangsmidler, datert 25. mai 2016

International Commission of Jurists' høringsuttalelse til justiskomiteen – Prop. 68 L – skjulte tvangsmidler, datert 7. april 2016

Rettsavgjørelser

Høyesterett

Rt. 2004 s. 1619, Kjennelse (Bakdørsaken)

Internasjonale domstoler

Den europeiske menneskerettighetsdomstol

Association for European Integration and Human Rights (AEIHR) og Ekimdzhiev mot Bulgaria 28. Juni 2007 (saksnummer 625400/00)

Funke mot Frankrike 25. februar 1993 (saksnummer 10828/84)

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

Kruslin mot Frankrike 24. April 1990 (saksnummer 11801/85

Liberty mfl. Mot Storbritannia 1. juli 2008 (saksnummer 58243/00)

P.G. og J.H. mot Storbritannia 25. september 2001 (saksnummer 44787/98)

Tyrer mot Storbritannia 25. april 1978 (saksnummer 5856/72)

Uzun mot Tyskland 2. september 2010 (saksnummer 35623/05)

Litteratur

Bøker

Torstein Eckhoff, *Rettskildelære*, 5. utgave ved Jan E. Helgesen, Oslo 2001.

Mads Henry Andenæs, *Rettskildelære*, 2. utgave, Oslo 2009

Bruce/Haugland (2014): Ingvild Bruce og Geir Sunde Haugland, *Skjulte tvangsmidler,* Oslo 2014.

Juridiske artikler

Inger Marie Sunde, «Dataavlesing som etterforskningsmetode», tidsskriftet *Retfærd* (2012) årgang 35, nr. 1/136

Avisartikler

Nærø, Amalie Frøystad, Newth, Magnus og Hvistendahl, Nora Evensmo, «Hackerangrep rammet nærmere 100 land», *VGs nettutgave:* http://www.vg.no/nyheter/utenriks/hackerangrep-rammet-naermere-100-land/a/23997276/ (12. mai 2017), sist lastet ned 12. mai 2017.

Wærstad, Lars, «– Det er ikke forbudt å tenke onde tanker. Så galt kan det gå om politiet får retten til å dataavlese Norges innbyggere», *Nettavisens Side3:* http://www.side3.no/teknologi/--det-er-ikke-forbudt-a-tenke-onde-tanker/3423227590.html, (25. mai 2016), sist lastet ned 12. april 2017.