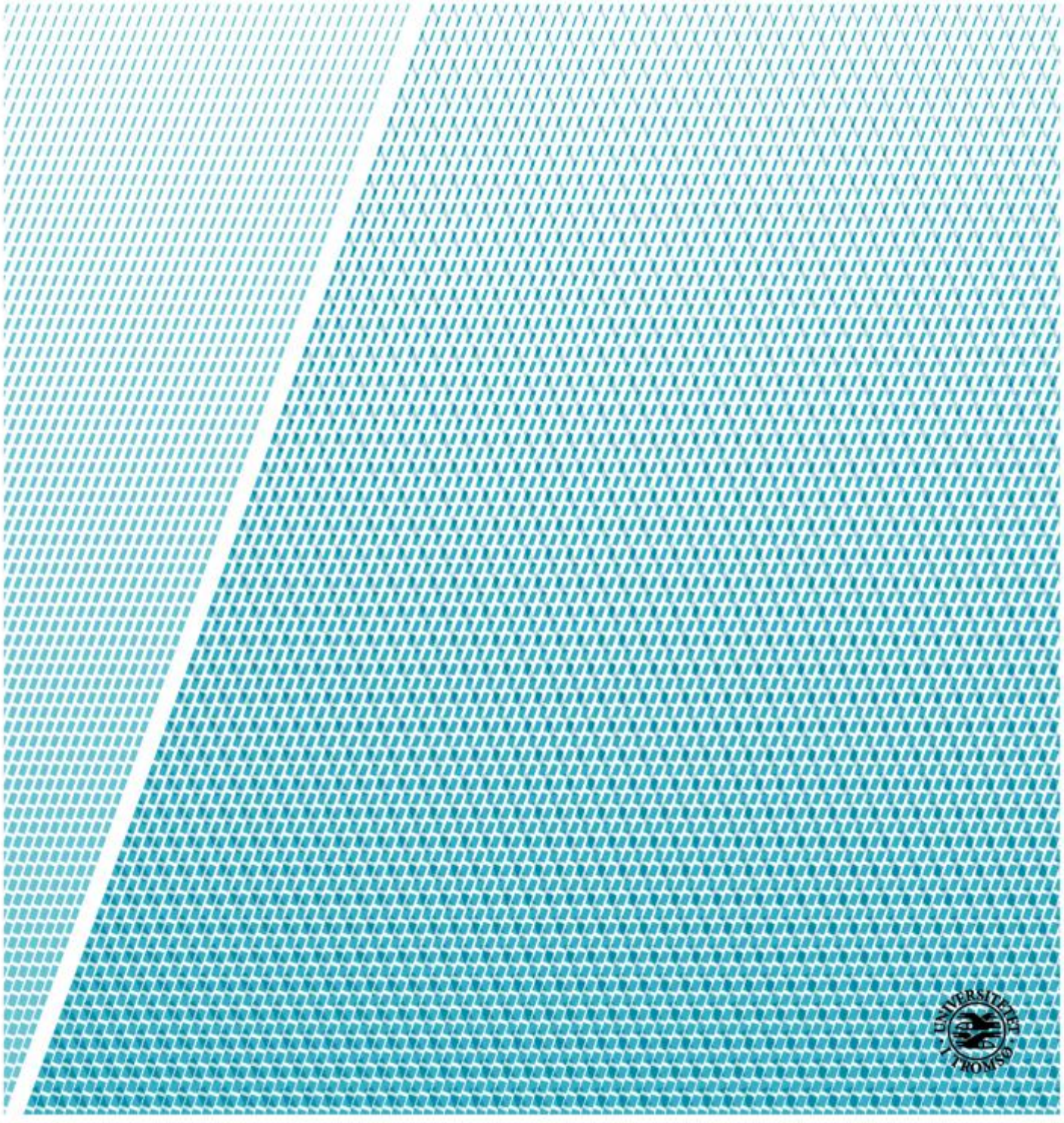
UiT
NORGES
ARKTISKE
UNIVERSITET

Det juridiske fakultet

Dataavlesning- med særlig fokus på inngrep i den private sfære

Av Terese Ytterstad

Liten masteroppgave i rettsvitenskap vår 2017



Innholdsfortegnelse

Forord

Det tas utgangspunkt i det endrede kriminalitets og trusselbildet som kan tilsi at behovet for skjulte politimetoder øker. Her fremkommer balansepunktet mellom kriminalitetsbekjempelse, personvern og rettssikkerhet. Ettersom samfunnet er i konstant utvikling og kriminalitet oppstår på nye arenaer, forutsetter dette at politiet har tilstrekkelige metoder for å ivareta samfunnssikkerheten. Mot denne oppgaven står tanken om å kunne sikre menneskets frihet. Ethvert individ skal være beskyttet mot overgrep og vilkårlighet fra myndighetene, kunne beholde en personlig sfære og samtidig skal de ha grunnlag for å forutse sin rettsstilling. Friheten er en viktig del av demokratiet. Samtidig må demokratiet beskyttes mot makter som vil ødelegge det. Politimetodene griper på ulike måter inn i de vernede interesser. Det oppstilles grense for politiets bruk av inngrep, både konstitusjonelle, menneskerettslige og etiske grenser. Dette reiser spørsmål om i hvilken grad det kan gripes inn i de vernede interesser. På dette grunnlag skal det ses på personvernets stilling vurdert opp mot dataavlesning, som politimetode og i hvilken grad det kan sammenlignes med kommunikasjonskontroll og ransaking.

1 Innledning

1.1 Tema og problemstilling

Utgangspunktet for avhandlingen er dataavlesning som politimetode for å bekjempe kriminalitet og på hvilken måte dataavlesning kommer i konflikt med retten til privatliv. Hovedfokus vil ligge på vernet mot inngrep fra offentlige myndigheter i dette perspektivet. Det vil bli foretatt en drøftelse av personvernets rekkevidde. Med dette menes hvilke typer rettigheter som er vernet og graden av vern ved politiets bruk av skjulte tvangsmidler. Dette belyses i hovedsak ved dataavlesning og med kommunikasjonskontroll og ransakelse som grunnlag for sammenligning. Avhandlingen vil derfor omhandle hvordan retten til privatliv materielt og prosessuelt begrenses ved dataavlesning. Det skal undersøkes i hvilken grad straffeprosessloven[1]§ 216 o balanserer vernet av personopplysninger mot de motstående interesser som gjør seg gjeldende for inngrepet. Dette vil sammenlignes med de "opprinnelige" skjulte tvangsmidlene, herunder kommunikasjonskontroll og hemmelig ransakelse. Med opprinnelige tvangsmidler sikter jeg til tvangsmidlene som var innført før dataavlesning ble vedtatt, og blant disse er det kommunikasjonsavlytting og hemmelig ransakelse som er mest relevant for sammenligningsgrunnlag.

1.2 Dataavlesningens og personvernets rettslige forankring

Dataavlesning er forankret nasjonalt i strpl. § 216 o. De nærmere vilkårene for bruk følger av bestemmelsen. Det følger av strpl. § 4 at lovens regler gjelder med de begrensninger som følger av folkeretten. Drøftelsen av vilkårene for inngrep følger i oppgavens punkt 2.2.

Personvernet er ved formuleringen "respekt for sitt privatliv" forankret i Grunnloven[2] § 102. Retten til privatlivets fred kommer til uttrykk blant annet i EMK[3] art. 8 og er også vernet i

[1] Lov av 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker *straffeprosessloven*, heretter forkortet strpl.

[2] Lov av 17. Mai 1814 Kongeriket Norges Grunnlov, heretter forkortet Grl.

[3] Europarådets konvensjon av 4. november 1950 om *beskyttelse av menneskerettighetene og de grunnleggende friheter* (Den europeiske menneskerettighetskonvensjon, heretter EMK).

andre internasjonale menneskerettskonvensjoner som Norge er bundet av.[4] Vernet om personopplysninger inngår i retten til respekt for sitt privatliv, jf. Grl § 102. Retten til respekt for privatliv, personvern og personopplysningsvern drøftes mer inngåendeunder punkt 3.6.

Med personopplysningsvern menes "*regler og standarder for behandling av personopplysninger som har ivaretakelse av personvern som hovedformål*".[5] Personopplysningsvernet er å regne som en del av personvernet, jf. personopplysningsloven[6] §1. Dette innebærer en nær tilknytning mellom personopplysningsvern og retten til privatliv. Retten til vern om personopplysninger regnes som en side av retten til privatliv[7] og omfatter alle personopplysninger. Retten til privatliv omfatter opplysninger relatert til individets privatliv. Men det er klart at selv om retten til privatliv og retten til beskyttelse av personopplysninger har mange fellestrekk, anses de ikke som en og samme rettighet.

Det følger av Politiloven[8] §1 jf. §2 at nasjonale myndigheter har det overordnede ansvar for å beskytte befolkningen mot kriminelle handlinger, sørge for rettssikkerhet og sikre rettigheter. Bruk av straffeprosessuelle tvangsmidler forekommer i forebyggende og, avvergende øyemed og under etterforsking. Reglene bygger blant annet på hensynet til effektiv kriminalitetsbekjempelse og må vurderes mot hensynet til personvern og rettssikkerhet. Dataavlesning kan gjennomføres ved etterforskning av straffbare handlinger som nevnt i strpl. § 216 o første ledd, eller som politimetode ved forebygging av alvorlig kriminalitet etter politiloven §17 d. Bruken av metoden på ulike stadier i prosessen taler for at den på ulik måte griper inn i de vernede interesser etter EMK art. 8. Vernet etter EMK art.8 er ikke absolutt og offentlige myndigheter kan gjøre inngrep i rettighetene på betingelsene som er gitt i EMK art. 8 nr.2.

---

[4] Herunder de forente nasjoners internasjonale konvensjon om sivile og politiske rettigheter av 16. Desember 1966 artikkel 17. Verdenserklæringen artikkel 12. (FNs erklæring) om menneskerettigheter av 10. Desember 1948. Personverndirektivet (95/46 EF).

[5] NOU 2009:1 s.17

[6] Lov av 14. April 2000 nr. 31 om behandling av personopplysninger.

[7] Personverndirektivet art.1 nr.1 hvor det fremgår at medlemsstater skal beskytte enkeltindividets fundamentale rettigheter, særlig retten til privatliv knyttet til beskyttelsen av personopplysninger.

[8] Lov av 4. August 1995 nr. 53 Politiloven

Dataavlesning utgjør et inngrep i retten til privatliv, det skal derfor undersøkes hvordan personvernet stiller seg i forhold til dataavlesning.

1.3 Bakgrunn og aktualitet

Innføringen av dataavlesning som straffeprosessuelt tvangsmiddel var en lang prosess i norsk rett. Begrepet "tvangsmiddel" er gitt i overskriften i straffeprosesslovens fjerde del. Loven gir ingen definisjon av begrepet. Ordlyden tilsier at virkemidlet anvendes under tvang, hvilket betyr at metoden kan brukes uten samtykke fra den tvangsmidlet brukes mot.[9]

Politimetodeutvalget uttrykker om begrepet tvangsmiddel at "*Uttrykket tvangsmiddel karakteriserer politimetoder som er så integritetskrenkende at politiet utvilsomt trenger hjemmel i lov for å ta metoden i bruk*".[10] Dette taler for at det er metoder som medfører krenkelse av den personlige integritet ved at borgere må tåle eller gjøre noe overfor myndighetene. Det følger av legalitetsprinsippet at myndighetens maktutøvelse overfor borgerne krever hjemmel i lov. Tvangsmidler kan anvendes av påtalemyndigheten og politiet med formål som kan være å sikre sakens gjennomføring og fullbyrdelse, å sikre bevis, eller forhindre at mistenkte begår nye lovovertredelser.[11] Hvorvidt et tvangsmiddel er så inngripende at det trenger hjemmel i særskilt lov, markerer skillet mellom handlinger politiet kan foreta seg med alminnelig handlefrihet, mot yttergrensene som krever særlig lovhjemmel. Felles for tvangsmidlene er at det skjer et inngrep i menneskets selvbestemmelsesrett. Dette er et inngrep som dermed krever klar lovhjemmel for å være rettmessig. [12].

En annen kategori tvangsmidler er skjulte tvangsmidler. Ved bruk av skjulte tvangsmidler foregår anvendelsen uten at den eller de bruken rettes mot underrettes og det kan besluttes utsatt eller unnlatt underetning. Dette medfører ytterligere interessespørsmål som blant annet personvern, personopplysningsvern og retten til privatliv. Spørsmålene om adgangen til bruk av skjult tvangsmiddel er fremdeles et dagsaktuelt og omstridt tema.

---

[9] NOU 1997: 15 s 72-75 Et samtykke danner ikke grunnlag for tvangsmiddelbruk. Bruken krever lovhjemmel og at vilkårene for tvangsmiddelbruk er oppfylte.

[10] NOU 2004: 6 pkt. 7.1.2.2 Tvangsmidlene (s.55)

[11] Norsk straffeprosess 4. Utgave kap.34.

[12] NOU 2004: 6 s 45

Lundutvalget berørte i NOU 2003:18 spørsmål om dataavlesning som politimetode. I samråd med justisdepartementet ble det ikke utredet nærmere. Politimetodeutvalget foreslo i NOU 2004:6 *Mellom effektivitet og personvern,* en innføring av regler om dataavlesning.[13] På den tiden var tanken om behovet for dataavlesning oppstått. Høringen av forslaget resulterte ikke i innføring av dataavlesning, men fastslo et behov for en nærmere vurdering av metoden og de tekniske spørsmål før innføring.[14] Etter dette kom spørsmålet opp for metodekontrollutvalget som blant annet skulle utrede og foreslå regler som tillater dataavlesning. Etter metodekontrollutvalgets syn må nye tvangsmidler eller utvidelser av eksisterende tvangsmidler, bygge på et bevist behov.[15] Deres forslag gikk ut på å innføre dataavlesning som ledd i gjennomføringen av de eksisterende metoder og ikke som et nytt selvstendig tvangsmiddel.

I Prop. L 68(2015-2016) om endringer i straffeprosessloven, la Justis- og beredskapsdepartementet frem forslag om lovendring som ga utvidet adgang til bruk av skjulte tvangsmidler ved etterforskning, avverging og forebygging av alvorlige lovbrudd. Proposisjon følger opp deler av utredningen i NOU 2009:15, men departementet fremmet forslag om dataavlesning som selvstendig tvangsmiddel hvor det kan foretas forløpende overvåking av datasystemet i sanntid. Kriminalitetsbildet som her ble lagt til grunn var Justiskomiteen[16] enig i, men det var ikke mulig å tallfeste noe konkret behov. Likevel mente departementet at behovet for dataavlesning var sterkere enn ved metodekontrollutvalgets vurderinger.[17] Behovet ble begrunnet i den teknologiske utviklingen som medførte at kommunikasjonsavlytting og hemmelig ransaking ikke var egnet til å gi politiet de samme opplysninger som før.[18]

Tendenser viser en kontinuerlig utvikling i bruk av datasystemer og det kan sies at det har utviklet seg en ny sosial norm for hvordan kommunikasjon foregår. Dette og tilgjengeliggjøring av informasjon, kan bidra til at kontrollen med personopplysninger

---

[13] NOU 2004:6 s. 207-208

[14] NOU 2007: 2 s.47

[15] Prop L68(2015-2016) s 249 jf. NOU 2009:15 s.240

[16] Innst.343 L(2015-2016)

[17] Prop. 68L(2015-2016) s. 261

[18] NOU 2009:15 s 237

svekkes. Bevisstheten om tilgjengelighet av privat informasjon har resultert i en utvikling i retning av økt informasjonsbeskyttelse. Økt bruk av beskyttelse, herunder kryptering, har resultert i en utfordring for politiets arbeid og anvendelse av opprinnelige tvangsmidler. Økt bevissthet om informasjonstilgjengelighet og behovet for informasjonsbeskyttelse vil også kunne påvirke kriminelle da de har en interesse i å følge med på politiets arbeidsmetode, særlig med tanke på sikre seg mot kontroll. Ved å anvende krypteringsprogrammer kan innhold i kommunikasjonen skjules, med dette menes å gjøre informasjon uleselig eller uforståelig for utenforstående.[19] Med opprinnelige tvangsmidler var adgangen til informasjon uendret rettslig sett, mens samme informasjon reelt sett var blitt vanskeligere tilgjengelig. Tilgang til informasjon krever dermed at politiet kommer over barrieren med krypteringene, noe som er en ressurskrevende prosess. På denne bakgrunn har et sentralt spørsmål vært hvorvidt politiets metoder skal følge den teknologiske utviklingen og gi adgang til nye metoder. Dataavlesning som tvangsmiddel ble innført ved lov 9. september 2016.[20] Hjemmelen for dataavlesning som ledd i etterforskning fremgår av straffeprosessloven[21] §216 o og som forebyggende tiltak i politiloven §17d.

1.4 Metode

Avhandlingen vil være av rettsdogmatisk art da problemstillingen besvares ved å klarlegge og å drøfte gjeldende rett på området. Både nasjonale og internasjonale rettskilder vil være av betydning for avhandlingen. Hovedproblemstillingen dreier seg om nasjonal straffeprosess, men må ses i lys av det mer internasjonale vern av privatliv og personvernet.

For avhandlingen er det to overordnede regler som er relevante ved vurderingen av den private sfære. Grunnloven §102 og EMK art. 8 som er inkorporert i norsk lov, jf. Menneskerettsloven[22] § 3. Grunnloven er lex superior og dermed av øverste rang. Konvensjoner og protokoller som er inkorporert i norsk rett, er i utgangspunktet på lovs nivå. Det følger derimot av mrl. § 3 at konvensjoner og protokoller omfattet av lov, har forrang før norsk lov. Da dette er en sammenligningsoppgave vil fokus ligge på norsk rett, de lege lata.

---

[19] https://www.datatilsynet.no/Sikkerhet-internkontroll/Kryptering/ sist besøkt 01.02.17

[20] Innført ved forskrift 9. september 2016 nr. 1046 om delvis ikraftsetting av lov 17. juni 2016 nr. 54 vedrørende endringer i straffeprosessloven (skjulte tvangsmidler).

[21] Lov av 22. Mai 1981 nr. 25 om rettergangsmåter i straffesaker

[22] Lov av 21. Mai 1999 nr. 30 om styrking av menneskerettighetene i norsk rett.

Det finnes lite tilgjengelig rettspraksis om forståelsen av vilkårene i strpl. §216 o. Analyser av regler og kritisk vurdering av politiets skjulte tvangsmidler vil derfor bero på ordlyd, forarbeider og juridisk litteratur, i tillegg til reelle hensyn som vil være av vesentlig betydning i mangel av rettspraksis.

1.5 Avgrensninger og fremstillingen videre

I bekjempelsen av alvorlig kriminalitet er det spørsmål om hvilke metoder myndighetene skal ha tillatelse til å anvende overfor befolkningen. Det er flere viktige momenter og hensyn i ulik retning som må tillegges vekt ved vurderingen. Ved innføring av dataavlesning var dette en ny metode, og det vil derfor problematiseres hvorvidt behovet for metoden var reel og om metoden effektivt vil tjene formålet. Avhandlingen er begrenset til å behandle dataavlesning i etterforskende øyemed etter strpl. §216 o, og ikke forebyggende øyemed etter politiloven §17d.

Først i avhandlingen redegjøres det i kapittel 2 nærmere for vilkårene for å kunne anvende "dataavlesning". Videre skal dataavlesning sammenlignes med de "opprinnelige" skjulte tvangsmidler kommunikasjonskontroll og hemmelig ransaking. I kapittel 3 blir det sett på hensyn som er relevante for vurderingen av metoden. For å svare på problemstillingen vil tvangsmidler og deretter dataavlesning vurderes mot personvernet i kapittel 4. For å synliggjøre behovet og hva metoden tilfører som nytt, vil det foretas en sammenligning med utgangspunkt i kommunikasjonskontroll og hemmelig ransaking da metodene synes å ligge nær dataavlesning. Det avgrenses derfor mot de øvrige straffeprosessuelle tvangsmidler. Det skal ses på hvordan dataavlesning løser utfordringene den teknologiske utviklingen har hatt for etterforskingen for å tydeliggjøre det særegne med metoden. Til slutt behandles dataavlesning som inngrep i retten til privatliv og personvern hvor det vurderes hvorvidt dataavlesning er hensiktsmessig og formålstjenlig. I kapittel 5 er det på sin plass med en oppsummering og en konklusjon.

2 Dataavlesning som metode for å etterforske straffbare handlinger

Dataavlesning som metode åpner for ulike fremgangsmåter for å gi tilgang til informasjon som kommuniseres via eller produseres eller lagres i et datasystem. Metodens fremgangsmåte er ikke beskrevet i detalj og er således ikke teknisk begrenset.[23] På dette grunnlag er det nødvendig å klargjøre hva dataavlesning innebærer. En klarlegging vil også vise hvordan personvern og personopplysningsvern utfordres ved bruk av dataavlesning. Dette vil være av betydning for sammenligningen med kommunikasjonskontroll og hemmelig ransaking. Herunder vil også bakgrunn og historikk være av betydning, særlig med tanke på fremveksten av denne metoden og hvordan inngrepet er legitimert.

Formålet med dataavlesning er å innhente informasjon i *sanntid* før den krypters, og å kunne fremskaffe informasjon som den teknologiske utviklingen har gjort vanskeligere tilgjengelig. Politiet er gitt skjult tilstedeværelse i datasystemet og kan overvåke informasjonen i *sanntid*, altså fortløpende. Den andre fremgangsmåten er å fremskaffe krypteringsnøkler som er koder, fanget opp ved å avlese tastetrykk i avsender eller mottakers datasystem.[24] Metoden er ment å avhjelpe problemer den teknologiske utviklingen har medført for politiets etterforsking. I lys av dette er det interessant å se på dataavlesning som straffeprosessuelt tvangsmiddel sammenlignet med de opprinnelige tvangsmidlene.

2.1 Historikk bak dagens lovhjemmel

Kriminalitetsbildet er en samlebetegnelse for den kriminalitet samfunnet står overfor til en hver tid. Borgernes og samfunnets behov for beskyttelse defineres av risikoen for kriminalitet.[25] Det kan slås fast at det er en utvikling innen organisert kriminalitet. Lovbruddene er mer komplekse, utøver av kriminelle handlinger er i økende grad mer profesjonelle, internasjonalisering og multikriminalitet råder kriminalitetsbildet.[26] For å kunne bekjempe kriminalitet i samme grad som før er det sentralt at politiet har midler som kan tjene formålet, slik at utviklingen ikke stagnerer og forholdet mellom politiet og kriminell trussel

[23] Prop 68 L (2015-2016) s.13 jf NOU 2009: 15 s.236.
[24] NOU 2009:15 s 241-242
[25] Innst.343 L-2015-2016 s. 2
[26] Prop 68 L(2015-2016) s.26

ikke kun utvikles uforholdsmessig i den ene retning.[27] Kriminalitetssituasjonen i Norge kan på denne bakgrunn begrunne nye straffeprosessuelle tvangsmidler. Samtidig er det viktig å påpeke at det ved utvidelsen av anvendelse av tvangsmidler også har skjedd en utvikling av kontrollmekanismer og rettssikkerhetsgarantier.

Nyere tid har medført større forekomst av datasystemer med stigende praktisk og økonomisk betydning. I denne sammenheng har det også utviklet seg muligheter for straffbar befatning med eller ved hjelp av datasystemer. Mulighetene for kriminalitet er mange ikke bare av de fysiske objekter som datamaskiner, men også for innbrudd i datasystemer med motivasjon om å tilegne seg informasjon, å utnytte datasystemet, påføre det skadeverk eller å sette datasystemet ut av funksjon. Det er grunn til å anta at utviklingen vil påvirke kriminelle som har interesse i å kjenne politiets arbeidsmetode.[28] Det er ikke noe som tilsier at datakriminalitet kommer til å avta, det er heller en forventet økning av slik kriminalitet.[29] Utbredelsen av datasystemer spiller en betydelig rolle ved utøvelse av kommunikasjon, tapping av opplysninger, bedrageri, besittelse eller mulighet for produksjon av barnepornografi, terrorhandlinger, forbrytelser mot staten med mer. Med denne potensielle risiko for skade bør det også være mulighet for kontroll med handlingene.

Dataavlesning har vært et omstridt tema i norsk kriminalitetsdebatt i lang tid, og temaet har vært omtalt i flere lovutvalg de senere år. Lund-utvalget var inne på temaet i NOU 2003: 18, men mente det var mer naturlig å la spørsmålet løses av datakrimutvalget. Datakrimutvalget hadde kompetanse til å ta stilling til de kompliserte, tekniske problemstillinger metoden reiste, men mente på sin side at metoden måtte uredes nærmere.

Politimetodeutvalget drøftet deretter temaet i NOU 2004: 6. Bakgrunnen var at kommunikasjonskontroll gav mindre informasjon enn tidligere på grunn av økt bruk av krypteringsprogrammer. Flertallet foreslo regler om dataavlesning som forebyggende metode. Mindretallet mente utvalget ikke kunne ta stilling til de tekniske sidene forslaget reiste og mente at spørsmålet måtte overlates til Datakrimutvalget. Datakrimutvalget mente at metoden måtte utredes nærmere, da begrepet dataavlesning ikke hadde ettentydig fastlagt innhold.

---

[27] Prop. 68 L(2015-2016) s 26

[28] NOU 2009:15 s 241

[29]Se Årsmelding (NSM) Nasjonal sikkerhetsmyndighet 2008 s.21 flg.

Etter høringen var departementets oppfatning også at metoden måtte vurderes nærmere.[30] Spørsmålet kom så opp for Metodekontrollutvalget hvor utvalget ble bedt om å utrede og å foreslå regler som tillater at politiet tar i bruk dataavlesning som metode i etterforskningen. Justis og beredskapsdepartementet, fulgte opp deler av NOU 2009: 15 i Prop. L 68(2015-2016) men foretok enkelte utvidelser i forhold til metodekontrollutvalgets forslag.

Et trekk i samfunnsutviklingen er en stadig økende registrering og bruk av personopplysninger og elektroniske hjelpemidler. Den teknologiske utviklingen har medført økt innsamling, lagring og sammenkobling av informasjon. Mange handlinger mennesket foretar seg, etterlater elektroniske spor som er blitt mer innholdsrike som følge av aktivitet nært knyttet til mennesket. Slik informasjon kan være sårbar for mennesket da den kan si mye om en persons mønster, preferanser og kommunikasjon. En slik utvikling har medført tilgjengeliggjøring som kan utfordre personvernet. Særlig hensynet til personvern og rett til anonymitet utfordres med økt registrering, noe som har gitt bidrag til utvikling av metoder for å verne sine opplysninger eller skjule sine spor. Det kan generelt stilles spørsmål til anonymitet og om mennesket kan ferdes anonymt. Sett fra den annen side kan teknologi styrke personvernet. Teknologien kan innrettes og beskytte informasjon slik som ved kryptering og andre måter å forhindre tilgjengeliggjøring.

I samsvar med Strpl. §216 o, jf. NOU 2009:15 og prop. L 68 (2015-2016) er bruken av skjulte tvangsmidler forbeholdt politiet ved mistanke om alvorlig kriminalitet med høy strafferamme. Det følger av strpl §216 o at:

> *(1) "Retten kan ved kjennelse gi politiet tillatelse til å foreta avlesing av ikke offentlig tilgjengelige opplysninger i et datasystem (dataavlesing) når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling*
> *a)som etter loven kan medføre straff av fengsel i 10 år eller mer*
> *b) Som rammes av straffeloven §§..(..)"*
>
> *(3)"Tillatelse etter første ledd kan 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."*

[30] Ot.prp. nr.60 (2004-2005) s.141

(4) "Det kan 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. Avlesingen kan omfatte kommunikasjon, elektronisk lagrede data og andre opplysninger om bruk av datasystemet eller brukerkontoen".

Dataavlesning er regulert gjennom strpl. § 216 o. Ordlyden i § 216 o fjerde ledd angir at dataavlesning kan omfatte kommunikasjon, elektronisk lagret data og andre opplysninger om bruk av datasystemet eller brukerkontoen. Med dette åpner ordlyden for at dataavlesning kan gjennomføres i et relativt bredt spekter av kilder, hvor det kan fremstå som uklart hvilken informasjon det er adgang til avlesning av. I forarbeidene fremkommer det at informasjonsavlesning kun kan begrenses av type informasjonssystem og funksjonaliteten til program og maskinvaren. Det vil omfatte tastetrykk, videostrøm, lydstrøm, lagrede filer og kommunikasjon.[31] Det avgrenses mot manipulasjon av datasystemet for å anvende webkamera, mobilkamera eller mikrofon tilknyttet til systemet.[32] Dataavlesning er gitt med frihet til å velge en fremgangsmåte som anses passende for tilfellet som skal behandles. Det kan benyttes egne tekniske hjelpemidler, dataprogrammer, innbrudd for å installere i tillegg til flere tenkelige metoder. Dette stiller sikkerhetsmessige spørsmål og etiske dilemmaer med tillit til virksomheten og bruken av metoden, da det ikke fremgår klart av bestemmelsen hvilke inngrep en person kan utsettes for ved gjennomføring av dataavlesning.

Til sist peker NOU 2009: 15 og Prop. 68L (2015-2016) på tanker i motsatt retning av hensynet til effektiv kriminalitetsbekjempelse. Ved tidligere vedtakelse av lov, var fokus rettet mot mer inngripende og mer effektive tvangsmidler for å avdekke alvorlig kriminalitet. Tendensen i dag er at det stilles strengere krav til ivaretakelsen av personvern og rettsvern. Dette fremkommer gjennom den skepsisen som er kommet til utrykk via forarbeidene, hvor det foretas en avveining av de ulike hensyn.

[31] Prop. 68L(2015-2016) s.224

[32] Prop. 68L(2015-2016) s.246

2.2 Dataavlesning som skjult tvangsmiddel

Dataavlesning ble innført som selvstendig tvangsmiddel delvis i samsvar med departementets forslag i proposisjonen. Metodekontrollutvalget definerer dataavlesning som gjengitt i proposisjonen:

> *"Med dataavlesning menes avlesning av opplysninger i et ikke offentlig tilgjengelig informasjonssystem ved hjelp av programmer eller annet utstyr"*[33]

Det ble videre fastslått at reguleringen av dataavlesning i detalj, ikke var hensiktsmessig. Det er dermed ikke klart hva som ligger i tvangsmidlet dataavlesning og hvordan det anvendes. På den annen side gir en slik teknologinøytral beskrivelse hjemmelen lengre levetid ved at regelen kan tilpasses den teknologiske utviklingen.

I § 216 o første ledd gis det adgang til å "*foreta avlesning av ikke offentlig tilgjengelige opplysninger i et datasystem(dataavlesning)..".* En naturlig forståelse av begrepet "*dataavlesning*" indikerer en mulighet til å kunne se hva som foregår på en datamaskin. Derimot innebærer dataavlesning noe mer, en adgang til informasjon lagret på eller kommunisert via et *datasystem*. Som "*datasystem*" regnes blant annet smarttelefoner, datamaskiner og andre anlegg for elektronisk kommunikasjon som behandler data ved hjelp av dataprogrammer.[34] Dataavlesning kan foretas på ulike enheter. Avlesningen vil kunne omfatte lydstrøm tilknyttet mikrofon og høyttalere, videostrøm, tastaturtrykk, innhold på harddisk og data fra internett.[35] Dette medfører at også opplysninger som kun tastes på tastaturet vil kunne være gjenstand for avlesning, til tross for at opplysningene hverken lagres eller kommuniseres.

Gjennomføringen av dataavlesning er en prosess i tre ledd. Den må først skje en tilretteleggelse hvor virkemiddelet installeres eller monteres på datasystemet. Etter dette er gjort, kan politiet gis tilgang til opplysninger og til å overvåke bruken. Som en avslutning avinstalleres eller fjernes virkemidlet[36] og systemet skal gjenopprettes til normalen.

---

[33] Prop. 68 L (2015-2016) pkt.14.1

[34] Prop. 68 L (2015-2016) s 270-271

[35] Prop. 68 L (2015-2016) s.224

[36] NOU 2009:15 s.247

Avlesningen avhenger av tilretteleggelse som skjer ved å installere programvare eller maskinvare via fysisk eller elektronisk innbrudd i datasystemet. Ved elektronisk innbrudd plasseres programvare i mistenktes datasystem via trojanere og eventuelt andre programvarer i datasystemet. Ved fysisk innbrudd er det innbrudd i mistenktes hjem for å innrette nødvendig utstyr for gjennomføring av dataavlesning. Dataavlesning utgjør i utgangspunktet et straffbart innbrudd i et datasystem i samsvar med straffeloven § 204,[37] med formål å innhente informasjon fra mistenktes datasystem. For lovlig tilgang på slik informasjon kreves klar lovhjemmel.

Dataavlesning utgjør et inngrep i den private sfæren. Metoden vil innebære et inngrep på en ny måte med andre konsekvenser for den som blir overvåket enn det de opprinnelige metoder utgjorde. Før en vurdering av dataavlesning og inngrepsterskelen er det hensiktsmessig med en gjennomgang av vilkårene for dataavlesning. Vilkårene sier noe om terskelen for inngrep. I punkt 2.4 vil det foretas en sammenligning av inngrepene i den personlige sfære ved dataavlesning i forhold til kommunikasjonskontroll og hemmelig ransakelse.

2.3 Vilkårene for dataavlesning

2.3.1 Mistankekravet

Det første vilkåret for dataavlesning er at det må foreligge "skjellig grunn til mistanke" om handling i samsvar med strafferammekravet i § 216 o. Skjellig grunn til mistanke sier at det må foreligge en konkret mistanke for at tvangsmidlet kan benyttes. En ordlydsfortolkning av begrepet "*skjellig grunn*" tilsier at det kreves god eller rimelig grunn til mistanke. For å oppfylle mistankekravet må det foreligge objektivt forankrede holdepunkter i retning av at mistenkte har begått handlingen. Det kreves ikke sikker overbevisning, men en hver mistanke er ikke tilstrekkelig for å tilfredsstille kravet om "skjellig grunn". Mistanken må kunne begrunnes.

Høyesterett uttaler i Rt. 1993 s. 1302[38] om "skjellig grunn" at "*det må være mer sannsynlig at siktede har begått den straffbare handling saken gjelder enn at han ikke har det*". Kriteriene for

[37] Lov om straff (straffeloven) av 20. Mai 2005

[38] Høyesteretts kjæremålsutvalg behandlet anke over kjennelse om varetektsfengsling. I den forbindelse kom Høyesterett inn på hva som lå i kravet til "skjellig grunn til mistanke" og la til grunn Lagmannsrettens forståelse som lød: "det skal være mer sannsynlig at siktede har begått den

skyldvurderingen kan etter dette anses som veiledende da straffbarhetsvilkårene utgjør en indikasjon på sannsynlighetsovervekt på skyld er tilstrekkelig for anvendelse av straffeprosessuelle tvangsmidler.

Vilkåret om skjellig grunn til mistanke etter strpl. § 216 o, skal forstås på samme måte som vilkåret forstås ellers i straffeprosessloven. Det gjelder også de øvrige vilkår for dataavlesning.[39] Rettspraksis fra før strpl. § 216 o trådte i kraft er således relevant da vurderingen er den samme som for kommunikasjonskontroll. Vurderingen er skjønnsmessig, foretatt av retten ved avgjørelse om bruk av tvangsmiddel, og samme vurdering må derfor kunne anvendes ved dataavlesning.

2.3.2 Kriminalitetskravet og de to vurderingsstandarder

Det neste vilkåret er strafferammekravet på lovovertredelsen mistanken dreier seg om. Bestemmelsen deler strafferammekravet i to standarder. Det ene er et generelt krav om strafferamme på fengsel i minst 10 år, jf. strpl. § 216 o første ledd litra a. Det første alternativet er at handlingen "*kan medføre straff av fengsel i 10 år eller mer*". En naturlig språklig forståelse tilsier at avgjørende for om dataavlesning kan anvendes, er om strafferammen for straffbare handlingen mistanken gjelder er oppfylt. Strafferammen er gitt i den konkrete lovbestemmelsen mistanken omhandler. For vurderingen om dataavlesning kan skje, må den abstrakte strafferamme legges til grunn.[40] Med abstrakte strafferammekrav menes den høyeste straff som er angitt i straffebestemmelsen, ikke forventet straff i vurderingen av det konkrete tilfellet.

Annet alternativ henviser til konkrete straffebud som ikke fyller kravet om strafferammene, jf. § 216 o første ledd litra b. For dette alternativet må mistanken gjelde et straffebud som opplistet i §216 o første ledd litra b. Straffebudene omhandler grovt sett både deltakelse og planlegging av terrorvirksomhet, statssikkerhet, narkotika, frihetsberøvelse og hvitvasking blant annet. Listen over straffbare handlinger gir grunnlag for bruk av tvangsmidlet ut fra den

straffbare handling saken gjelder enn at han ikke har det". Uttrykket innebærer etter sikker rett sannsynlighetsovervekt.

[39] Prop.68 L (2015-2016) s. 284

[40] Rt-2006-1398 hvor det er uttalt at "straffebudenes abstrakte strafferamme som er avgjørende for adgangen til å fengsle"

oppfatning at forbrytelsens karakter et særlig behov for metoden.[41] Behovet er begrunne i at dette kan være handlinger som ellers kan være vanskelig å oppklare. Når terskelen for inngrep etter litra b gjelder handlinger med en lavere strafferamme ilegges en videre begrensning ved at også forholdsmessighetskravet jf. strpl. §170 a skjerpes.[42]

2.3.3 Indikasjonskravet

Det følger av straffeprosessloven §216 o tredje ledd, at dataavlesning bare tillates så fremt det "*antas at dataavlesning vil være av vesentlig betydning for å oppklare saken, og at oppklaringen ellers i vesentlig grad vil bli vanskeliggjort*". Dette kalles indikasjonskravet[43] og gjelder i tillegg til det generelle forholdsmessighetskravet etter straffeprosessloven § 170 a.

Vurderingen foretas konkret i hver sak hvorvidt det er et nødvendig behov for dataavlesning for å oppklare saken. Det er et viktig moment at samme formål ikke kan dekkes med mindre inngripende metoder. Metoden må gi politiet opplysninger som er nødvendige eller av vesentlig betydning for å oppnå formålet.[44] Det må således være et konkret behov for at tvangsmidlet skal kunne brukes[45] og at mildere midler ikke må kunne oppfylle samme formål. Nødvendighet indikerer at jo sterkere mistanken er, desto lettere kan inngrepet rettferdiggjøres.

2.3.4 Forholdsmessighetskravet

Inngangsvilkåret for anvendelse tvangsmidler følger av strpl. § 170 a som gjelder for alle straffeprosessuelle tvangsmidler. Bestemmelsen er en forholdsmessighetsregel og setter krav om at det må foreligge tilstrekkelig grunn til anvendelse av tvangsmiddel, og at det ellers ikke vil utgjøre et uforholdsmessig inngrep overfor mistenkte.[46]

Skjulte tvangsmidler representerer alvorlige inngrep i den private sfære. Strpl. §170 a er i norsk straffeprosess regnet som en sikkerhetsventil, hvor middelet må vurderes som

---

[41] NOU 2009:15 s.160

[42] Prop. 68L(2015-2016) s. 268

[43] Prop. 68 L (2015-2016) s. 230 Vilkåret lyder likt i Dansk og svensk rett, hvor det blir betegnet som indikasjonskravet.

[44] Ot.prp(2004-2005) s.46

[45] Ot.prp (2004-2005) s.33

[46] Andenæs (Norsk straffeprosess) s.280

hensiktsmessig etter bestemmelsen før det kan tillates anvendt. Bruken av dataavlesning tillates bare i tilfeller hvor det er egnet til å forebygge, avverge eller oppklare den aktuelle handlingen. Samme formål må ikke kunne oppnås med mildere inngrep, da vil dataavlesning være uforholdsmessig i forhold til bruken av tvangsmidlet. Dataavlesning er begrunnet i tilgangen til krypteringsprogrammer som gir kommunikasjonskontrollen i dag mindre informasjon enn tidligere. Metodeutvalget mente at en måte å få tak i innholdet på var ved avlesning før kryptering. Kan dette skje ved andre og mindre inngripende midler enn ved dataavlesning, skal dataavlesning ikke brukes.

2.4 Hva skiller dataavlesning fra andre sammenlignbare etterforskningsmetoder

Personvernkommisjonen påpeker at en hver av hensyn til personvern, i større grad bør kryptere informasjon som utveksles over internett.[47] Informasjonsbeskyttelse er åpenbart positivt, når formålet er å verne om lovlig aktivitet og personlig informasjon med den hensikt å hindre andre i å tilegne seg slik kunnskap. Imidlertid benyttes kryptering også for å unndra kriminelle handlinger fra kontroll. Fremveksten av informasjonsbeskyttelse er en utfordring for etterforsking og forebygging av kriminalitet. Bestemmelsene om kommunikasjonskontroll og hemmelig ransaking stod i utgangspunktet uendret. Adgangen til informasjon var rettslig sett den samme etter lovteksten. Derimot har den teknologiske utvikling svekket effekten av de opprinnelige tvangsmidler. En reell tilgang til samme informasjon krever ny teknologi, kompetanse og resurser.

Samfunnsforholdene er dynamiske og tilsier således tilsvarende dynamiske metoder for å imøtekomme de kriminelle arenaer dersom politiets tilgang til informasjon skal opprettholdes.[48] Denne dynamiske utviklingen utfordre derfor balansen mellom kriminalitetsbekjempelse, personvern og rettssikkerhet. Hvordan hensynene vektes fremkommer i forarbeidene til lovteksten hvor forslagene av dataavlesning fremsettes ulikt. Metodekontrollutvalget foreslo dataavlesning som gjennomføringsmåte innenfor rammene av etablerte tvangsmidler. Departementet på sin side hevdet dataavlesning må kunne brukes i større grad enn metodeutvalgets forslag, og foreslo innføring av dataavlesning som

[47] NOU 2009: 1 s.87-88.

[48] Innst. 343 L-2015-2016

selvstendig tvangsmiddel.[49] Dataavlesning ble senere vedtatt som selvstendig tvangsmiddel, men ved justiskomiteens uttalelse innsnevres dataavlesning i noen grad i forhold til departementets forslag. Sondringen mellom de tre leddene i prosessen før endelig lovgivningen er relevant i forhold til hvordan de ulike organene ser på behovet for metoden og hvordan de kryssende hensyn er vektet ved begrunnelsen for dataavlesning som metode.

Tilgangen til bruk skjulte tvangsmidler beror på hensynet til å oppklare alvorlig kriminalitet mot betenkelighetene ved bruk av metodene. Når dataavlesning ble innført ble det i flere sammenhenger anført som en særlig inngripende metode. Det første det må spørres om er i hvilken grad inngrepet skiller seg fra de opprinnelige metodene som har vært innarbeidet i norsk straffeprosess over lang tid. For å se på dette må det først kort redegjøres for hva de ulike metodene består i, og hvilke inngrep som gjøres ved disse metodene.

2.4.1 Kommunikasjonskontroll

Kommunikasjonskontroll er en betegnelse på kommunikasjonsavlytting og annen kontroll av kommunikasjonsanlegg, regulert i strpl. § 216 a og § 216 b. Kommunikasjonsavlytting består i å føre kontroll med samtaler, eller å avlytte samtaler eller annen kommunikasjon fra telefoner, datamaskiner eller anlegg for elektronisk kommunikasjon jf. strpl. § 216 a tredje ledd. Avlytningsadgangen gjelder alle "anlegg for elektronisk kommunikasjon". Dette omfatter all informasjonsutveksling mellom kommunikasjonsanlegg, uavhengig av form eller innhold på informasjonen.[50] Dette gjør at det er uvesentlig hvilket teknisk hjelpemiddel for kommunikasjon som skal avlyttes.[51] Kravet er at informasjon som kan føres kontroll med, formidles mellom kommunikasjonsanlegg fra avsender til mottaker.

Strpl. § 216 a er utformet med nøytral ordlyd, noe som gir rom for at gjennomføring kan skje uansett middel, så lenge fremgangsmåten er forenelig med resterende vilkår. En slik regelutforming gjør bestemmelsen tilpasningsdyktig etter samfunnsforholdene og tilsier at kommunikasjonskontroll også må kunne foregå ved datasystem eller annen ny teknologi. Kravet er at avlytningen må foregå under overføring av informasjon, uavhengig av kommunikasjonsmiddel for ivaretakelse av formålet ved kommunikasjonsavlytting.

---

[49] Prop. 68 L (2015-2016) s. 274

[50] Ot.prp.nr.64(1998-1999) s. 153.

[51] Ot.prp.nr.64(1998-1999) s.157.

Metodekontrollutvalget la til grunn at kommunikasjonsavlytting er et effektivt middel for kriminalitetsbekjempelse.[52] Bruken ble vanskeliggjort ettersom mye kommunikasjon foregår via internett og at den teknologiske utvikling har vanskeliggjort tilegnelse av informasjon ved kommunikasjonskontroll. Dataavlesning ville således tjene som middel for gjennomføring av kommunikasjonsavlytting etter metodekontrollutvalgets forslag. Hensikten er som tidligere å klarlegge informasjonen som utveksles mellom kommunikasjonsanleggene, noe som kan tilfredsstilles ved kommunikasjonskontroll og ved dataavlesning som gjennomføringsmiddel.

Kommunikasjonskontroll er opprettholdt og dataavlesning innført som selvstendig tvangsmiddel, fordi både departementet og justiskomiteen anså det for å være et stort og udekket behov for tilgang til elektronisk lagret og kommunisert informasjon. Med hensyn til kommunikasjonskontroll er det på bakgrunn av at informasjonen krypteres eller slettes forløpende noe mer som må tilføres før kommunikasjon blir tilgjengelig for kontroll. Dersom anlegget ikke er å anse som kommunikasjonsanlegg, kan det dermed ikke avlyttes. Departementet og justiskomiteen fant det mest hensiktsmessig å innføre dataavlesning i egen bestemmelse som kun skal kunne benyttes i samme type saker og på lignende vilkår som kommunikasjonsavlytting.

2.4.2 Hemmelig ransaking

Hemmelig ransaking er hjemlet i strpl. § 200 a. En tradisjonell oppfatning av ransakelse er fysiske undersøkelser med hensikt å finne gjenstander eller informasjon som kan tjene som bevis. Ved hemmelig ransaking kan politiet tilegne seg bevis mot mistenkte uten at mistenkte vet om ransakingen. Det som letes etter er for eksempel informasjon nedskrevet i notater eller informasjon via andre midler, gjenstander gjemt i hjemmet eller andre steder.

Ransaking foregår i mistenktes bolig, rom eller oppbevaringssted jf. strpl. §192. Bestemmelsen sier ikke eksplisitt noe om ransaking av mistenktes datasystem. Hjemmelen for dette er ikke klart forankret i lovteksten og er heller ikke fastslått i forarbeider eller gjennom tilgjengelig rettspraksis. Riksadvokaten uttalte derimot at dette var lagt til grunn i

[52] NOU 2009:15 punkt 10.2

underrettspraksis, som ikke er allment tilgjengelig.[53] Dette gjør det vanskelig for borgeren å forutse sin rettsstilling i forhold til ransaking av data. Til tross for dette anvendes bestemmelsen også som hjemmel for ransaking av datasystemer i mistenktes hjem. De generelle regler om ransaking hjemler således ransaking av det virtuelle rom og herunder ransaking av datasystemer jf. Strpl §200 a jf. §192.[54] Begrunnelsen for adgangen er at hjemmelen også tidligere er gitt en utvidet tolkning. Dette begrunner således en tolkning til at bestemmelsen også kan omfatte ny teknologi som dataavlesning og ransaking av data. En ransaking av datasystemer kan skje uten politiets fysiske tilstedeværelse, da dette verken er nødvendig eller praktisk for formålet. Dette vil fremstå som mindre integritetskrenkende da fysisk tilgang til hjemmet ikke er nødvendig og kan unnlates. På dette nivået kan ransaking av datasystem hjemles i de generelle regler om ransaking og tilgangen til informasjon på dette nivå vil kunne opprettholdes.

Metodekontrollutvalget legger samme begrunnelse for kommunikasjonsavlytting som for ransaking til grunn med hensyn til krypteringer, barrierer og informasjonstilgang.[55] Ved ransakelse er det eldre kommunikasjon som e-postkorrespondanse, Chat- meldinger, data lagret i systemet og lignende som gjøres til gjenstand for kontroll. Dersom formålet er å fange eldre kommunikasjon, kan ransakelse tilsynelatende være like inngripende som kommunikasjonsavlytting da det er samtaler som gjennomsøkes, selv om det ikke er kommunikasjon i *sanntid*. Derimot vil avlesning i sanntid og for å avdekke ny informasjon ikke kunne hjemles i de generelle bestemmelser om hemmelig ransaking og tilgang til slik informasjon vil kreve hjemmel.

Metodeutvalget foreslo dataavlesning som gjennomføringsmåte for hemmelig ransaking med hjemmel i strpl § 200 a.[56] Dette ville gi en klar hjemmel i lov om tilgang til lagret informasjon på mistenktes datamaskin, ikke en tolkning av lovtekst som ikke er like klar når det gjelder hvilke gjenstander som kan ransakes, herunder datasystem og datamaskin. En slik fremgangsmåte fremstår som mindre inngripende, da politiet ikke behøver å ta seg inn i

---

[53] NOU 2009: 15 s 246 om riksadvokatens uttalelse om adgangen til ransaking uten fysisk tilstedeværelse. Se også høringsuttalelse av 19. April 2010 s 13.

[54] Ot. Prp Nr.40(2004-2005) s.34

[55] Se avhandlingens pkt 2.3.1

[56] NOU 2009: 15 s 245-246 og 352-353

private hjem, men bare inn i datasystemet for en elektronisk ransakelse. Av hensyn til befolkningen vil en ny lovtekst skape klarhet og forutberegnelighet av hva som gjøres til middel for kontroll. Forslaget fra utvalget innebærer en adgang til å ransake datasystem uten at politiet er fysisk til stede,[57] selv om dette ikke klart fremkommer i lovforslaget. Effektivitetshensynet taler også for en slik metode.

Ransakningstillatelse åpner bare for en enkeltransaking. Lovteksten står ikke til hinder for at det gis tillatelse til flere ransakelser. Derimot er det presisert i forarbeidene at det ikke gis tillatelse for fortløpende eller gjentatt ransakelse.[58] Ny adgang krever rettens tillatelse.

2.4.3 Det særegne ved dataavlesning

Dataavlesning har til formål å bøte på utfordringene politiet møter ved bruk av opprinnelige tvangsmidler. Dataavlesning kan benyttes på samme måte og på liknende vilkår som kommunikasjonskontroll og hemmelig ransaking, som selvstendig metode. Dette innebærer at forslaget om en løsning med dataavlesning i begrenset utstrekning og kun som gjennomføringsmåte for de opprinnelige tvangsmidler, ikke anses tilstrekkelig til å møte dagens utfordringer.

Vedtakelsen av nytt tvangsmiddel og ny lovtekst beror på et dokumentert behov for ny politimetode, hvor utvidelser bare er aktuelt dersom metodene er å anse forsvarlige ut fra hensynet til personvern og rettssikkerhet.[59] Det er på det rene at inngrepet vil være av ny karakter, beror på nye fremgangsmåter og at dataavlesning åpner for tilgang til informasjon som tidligere metoder ikke hjemlet. Det som her skal vurderes er hvorvidt og på hvilke områder dataavlesning skiller seg fra de opprinnelige metoder.

Det som må vurderes er hva som oppnås ved dataavlesning som ikke kan oppnås ved andre metoder.

Informasjonen politiet kan få tak i ved dataavlesning er den samme som de ellers har rettslig tilgang til gjennom kommunikasjonsavlytting og hemmelig ransaking.[60] Formålet med dataavlesning er kompensasjon for tapt effekt ved kommunikasjonsavlytting og hemmelig

---

[57] NOU 2009: 15 s 352

[58] NOU 2009:15 s. 246 med videre henvisning til NOU 2004:6 s. 95 og 98

[59] Prop. 68 L (2015-2016) s.251

[60] Prop 68 L (2015-2016) s 264

ransaking, som resultat av teknologisk utvikling. Når kommunikasjonskontroll og ransaking gir tilgang til informasjon som kommuniseres i sanntid eller er lagret på datasystemet, vil en eventuell passordbeskyttelse eller kryptering kunne hindre tilgangen til enkelte deler av datasystemet. Informasjonsbeskyttelse og krypteringer gjør at informasjonen ikke sendes i klar tekst og avsender kan forhindre politiet tilgang til informasjon. Med utgangspunkt i dette er dataavlesning kun snakk om som effektivisering av fremgangsmåte, for å tilgjengeliggjøre informasjon de opprinnelige tvangsmidler hjemler og ikke en utvidet adgang til informasjon.

Dataavlesning som gjennomføringsmåte gir tilgang til alle opplysninger lagret eller som kommuniseres i datasystemet i perioden for metodebruken. Ut over dette gir dataavlesning som selvstendig metode tilgang til informasjon som "opprinnelige" metoder ikke gir tilgang til. Dataavlesning vil kunne fange opp aktivitet som foregår på datasystemet som verken kommuniseres eller lagres. Dette regnes som den kontinuerlige bruk av datasystemet hvor det gis tilgang til opplysninger om selve bruken av datasystemet over tid, hvilket er nytt i forhold til opprinnelige tvangsmidler.

Ved dataavlesning gis politiet skjult tilstedeværelse i datasystemet som vil kunne fange opp informasjon mens den kommuniseres, eller informasjon som kun inntastes uten å verken kommuniseres eller å lagres. [61] Ved å kunne se hvilke tastetrykk som foretas kan det oppfanges dekrypteringsnøkler[62] og eventuelle passord for å komme rundt krypteringene.[63] Ved tilstedeværelsen i datasystemet kan også annen informasjon fanges opp. På denne bakgrunn vil det løse de teknologiske utfordringer for opprinnelige metoder og tjene som selvstendig tvangsmiddel da metoden gir tilgang til informasjon utover det opprinnelige metoder hjemlet.

Hemmelig ransaking og kommunikasjonskontroll opererer med et skille mellom lagret informasjon og kommunikasjon. Før vedtakelsen av dataavlesning var det ikke lovhjemmel for kontroll utover informasjon som kommuniseres eller lagres i datasystemet. Det vil således være en forskjell på hvilken informasjon som er tilgjengelig etter hvilken metode som anvendes. Ved dataavlesning viskes således skillet ut. Dataavlesning gir tilgang til både lagret og kommunisert informasjon i datasystemet ved en begjæring om bruk av tvangsmidler og

[61] NOU 2009: 15 s.365

[62] NOU 2009:15 s 241-242

[63] NOU 2009:15 s.237

således ved en handling. På denne måten vil dataavlesning være mer inngripende overfor individet enn anvendelse av enten hemmelig ransaking eller kommunikasjonskontroll. Samtidig vil fjerning av skillet bidra til en mer effektiv måte å følge med på datasystemet for politiet ettersom det kun kreves en begjæring for å få tilgang til begge kategorier informasjon.

Politiet får ved dataavlesning tilgang til alt på datasystemet. Dette inkluderer informasjon om tidligere bruk og den pågående bruk av datasystemet. En slik adgang vil gi grunnlag for raskere å kunne fastslå ulovlig aktivitet. Derimot er det ikke bare ulovlig aktivitet, men all aktivitet ved datasystemet som vil kunne kartlegges ved denne metoden. Dataavlesning gir dermed tilgang til langt mer opplysninger av hva mistenkte foretar seg. Slik informasjon kan være av rent privat karakter som det heller ikke vil være av betydning for politiet å få kjennskap til. Tilgjengeliggjøring av slik materiale kan anses å være særlig inngripende i personvernet.

På den annen side har mennesket ført dagbok og kladdet på papir i lang tid. En ransaking vil kunne frembringe dette. Rettslig sett bør det dermed ikke være forskjell i notater foretatt på fysisk papir og notater ført i tekstbehandlingsprogram. Sett fra denne vinkelen er det i realiteten dermed tilgang til samme informasjon ved dataavlesning som ved hemmelig ransaking. På den annen side vil notater på et datasystem kunne spores opp etter sletting, noe destruering av papirer sjelden kan. Dataavlesning medfører dermed større adgang dokumenter enn opprinnelige metoder og gir tilgang til dokumenter som også kan være slettet så fremt de kan gjenopprettes.

De opprinnelige metoder hjemler tilgang til informasjon i transportfasen, hvor informasjonen innsamles ved hjelp fra tjenestetilbyder. Informasjonen som innhentes på denne måten skjer ikke i sanntid. Ved en begjæring om utskrift av e-postkorrespondanse eller tekstmeldinger er dette lagret materiale. I den grad de utgis i skrift er det heller ikke sikker de er i klar tekst, da de kan være krypterte. Utgangspunktet er at tjenestetilbyder gir adgang til informasjonen, men dette begrenses av krypteringer. Dette utgjør en hindring politiet må komme over før informasjonen blir tilgjengelig. I tillegg er det ikke sikkert tjenestetilbyder har lagret all informasjon da deres formål med informasjonen kun er av betydning for fakturering. I den grad er informasjonsadgangen vesentlig begrenset ved de nye teknologiske hjelpemidler. Dataavlesning vil på sin side kunne rette avlyttingen og avlesingen mot et spesifikt bestemt datasystem og gir informasjon uten bistand fra tjenestetilbyder.

Dataavlesning kan på dette grunnlag sies å ha visse fellestrekk med kommunikasjonskontroll og hemmelig ransaking som metode. På den annen side gir dataavlesning tilgang til mer informasjon om mistenkte ved å tilgjengeliggjøre flere arenaer for kontroll og nye metoder for innhenting av informasjon.

Videre må det ses på hva som gjør dataavlesning mer integritetskrenkende enn opprinnelig metoder.

Et hovedargument fra metodekontrollutvalget, departementet og justiskomiteen mot innføring av dataavlesning, var at dataavlesning er mer integritetskrenkende enn opprinnelige tvangsmidler. Dersom det tas utgangspunkt i kommunikasjonskontroll og ransakelse, er spørsmålet hvorfor dataavlesning er mer integritetskrenkende.

Kommunikasjonskontroll foregår i et gitt tidsrom i en konkret situasjon hvor det er en berettiget mistanke, og det er kommunikasjonsanlegg som kan avlyttes. Det samme gjelder for hemmelig ransaking hvor det er stedet mistenkte anvender som kan ransakes. Dataavlesning skal skje på tilnærmet samme vilkår. Dermed vil forholdene som berettiger bruken av de opprinnelige tvangsmidler også berettige dataavlesning. Forholdene som berettiger metodebruken er tilnærmet de samme, dette taler for at dataavlesning ikke er mer inngripende enn hemmelig ransaking og kommunikasjonskontroll.

Bruk av tvangsmidler utgjør generelt inngrep i den personlige sfære, men et inngrep i datasystem utgjør et inngrep på flere arenaer i dagliglivet. Datasystemer inneholder både dokumenter, notater, bilder og slikt, men det gir også tilgang til søk, nettbank, sosiale medier og mer. Befolkningen bruker mer tid på data i dag enn noen gang tidligere, noe som bidrar til at det legges igjen spor og informasjon overalt.[64] Den teknologiske utviklingen har medført at kildene som gjøres til rom for kontroll ligger stadig nærmere tankevirksomheten. Dette begrunner særlig individets behov for informasjonsbeskyttelse. Et slikt omfang av rom for kontroll er langt mer inngripende enn opprinnelige metoder gav tilgang til. Med tilgang til langt flere arenaer er det mange sider ved ens person som synliggjøres og vil virke særlig

[64] Statistisk Sentralbyrås statistikk for internettbruk fra andre kvartal 2015 https://www.ssb.no/teknologi-og-innovasjon/statistikker/ikthus/aar/2015-10-01 (April 17)

inngripende. Dette skiller seg fra opprinnelige tvangsmidler som har et mer begrenset bruksområde.

Med tilgang til mange kilder med innhold av personlig informasjon, skaper dataavlesning en frykt for generell overvåking av individets datasystem. Bekymringen ved dette var rettet mot at politiet skulle ha adgang til å anvende dataavlesning for å avdekke andre forhold, ett misbruk av metoden og omfanget av metoden.

Ransaking gir i hovedsak tilgang til undersøkelser i etterforskende, avvergende og i forebyggende øyemed av private hjem eller oppbevaringssted. Strpl. § 200 a hjemler også ransakelse av datasystemer som del av ransaking,[65] hvilket i realiteten taler for at forskjellen i inngrepet er relativt liten. Dataavlesning forutsetter innbrudd og tilstedeværelse i datasystemet som kan vare i inntil to uker jf. strpl. § 216 o femte ledd. Ved tilstedeværelsen i datasystemet gis det tilgang til å kontrollere informasjon som det tidligere ikke har eksistert hjemmel for, verken ved ransakelse eller kommunikasjonskontroll. Informasjonen som tilgjengeliggjøres faller ikke inn under det tradisjonelle skillet man har operert med.

Forskjellen er her at det ved ransaking vil måtte begjæres for hvert tilfelle hvor det skal føres kontroll, mens det ved dataavlesning må foretas en fortløpende eller kontinuerlig overvåkning innenfor den begrenset tidsperiode dersom det skal være gjennomførbart for krypterte områder.[66] Dataavlesning hjemler således et større tidsrom hvor datasystemet er disponibelt for kontroll, mens det ved ransakelse foretas en enkeltkontroll av datasystemet slik det foreligger på ransakelsestidspunktet. Mellom ransakingene kan det ha oppstått kommunikasjon eller dokumenter fra mistenkte som kan tenkes slettet før neste begjæring av ransakelse[67] som er rom for kontroll ved dataavlesning. I tillegg er det den kontinuerlige bruken av datasystemet som dataavlesning hjemler. Dette er informasjon som kan klarlegges ved dataavlesning og ikke ransaking. Således er mer informasjon tilgjengeliggjort for kontroll.

Politiet vil ved utøvelse av ordinær kommunikasjonskontroll og ransakelse gis tilgang til overskuddsinformasjon. Ved dataavlesning vil det fremkomme enda større mengder

---

[65] Se avhandlingens pkt 2.4.2

[66] Prop. L68(2015-2016) s.266

[67] Prop. L68(2015-2016) s. 262

overskuddsinformasjon. Hvilken informasjon som er tilgjengelig i et datasystem vil variere, fordi bruk og formål med bruk av et datasystem varierer. En person kan anvende datasystemer kun i arbeidsvirksomhet, mens en annen bruker systemet til alle personlige gjøremål og kan til og med leve store deler av sitt sosiale liv via datasystemet. Dette utgjør en vesentlig forskjell i hvor inngripende metoden vil føles for individet.

I tilfeller hvor informasjon verken lagres eller kommuniseres er det mye som taler for at informasjon ikke er ment meddelt andre. Slik informasjon er ikke tilknyttet anlegget og kunne ikke kontrolleres ved opprinnelige metoder. Kontroll av informasjon som ikke er ment kommunisert eller meddelt andre er klart mer inngripende enn kontroll med kommunisert informasjon. Det kan argumenteres med at informasjon som er kommunisert, har trådt ut av den private sfære. Hvorvidt denne informasjonen hemmeligholdes vil bero på om mottaker av informasjonen meddeler den. Informasjonen er således utenfor avgivers kontroll. Dette kan sammenlignes med kommunikasjon og håndtering av datasystem hvor det legges igjen spor. På lik linje må det kunne forventes kontroll med handlinger foretatt på internett da dette ikke forventes å være en privat sfære og hvor det kan forventes kontroll. Informasjon som ikke er kommunisert anses å være i den innerste personlige sfære og mer integritetskrenkende at det føres kontroll med. Dataavlesning går derfor utover opprinnelig tvangsmidlers kontrollområde og er mer inngripende enn kontroll i form av ransaking og kommunikasjonsavlytting.

Det er påpekt at dataavlesning til en viss grad gir innsyn i personlige betraktninger eller slik som brukeren ikke har tenkt til å lagre og heller ikke tenkt å meddele andre. For at dette skal skje må det utformes betraktninger i et program som verken lagres eller kommuniseres. Utvalget og departementet påpeker at det er sjelden ett system brukes på denne måten, men at det ikke kan utelukkes at det kan forekomme slik bruk.[68] Virkningen av inngrepsfølelsen vil i den grad ikke være av stor betydning dersom det ikke utgjør et reelt inngrep i mange tilfeller. Dersom dette er grunnlaget for at det ikke er særlig mer inngripende enn opprinnelige metoder, fremstår argumentasjonen tynn. En regel er utformet med formål. Er behovet der, kan bestemmelsen anvendes. Bare regelens eksistens utgjør således ett inngrep i den private sfære alene, da det er en risiko for inngrep.

[68] Prop. L68 (2015-2016) s.266-267

Dersom dataavlesning ses i sammenheng med kommunikasjonskontroll, foretas det skjult kontroll over kommunisert informasjon i begge tilfeller. Mistenkte vet aldri hvilke samtaler som kontrolleres, dermed kan mye av privat karakter avsløres også her, og metodene er på denne måte like inngripende. På den annen side er informasjonstilgangen begrenset ved kommunikasjonskontroll i forhold til dataavlesning. Dataavlesning fremstår som en mer kompleks metode for å danne et bilde av mistenkte da det er flere faktorer som tjener som grunnlag for kontroll. Ved kommunikasjonskontroll er grunnlag for kontroll mer begrenset da det bare er samtalen som kontrolleres.

Ved hemmelig ransaking er det adgang til å søke i vedkommende hjem eller også andre steder etter bevis og informasjon. Det følger av blant annet grunnloven §102 og EMK art. 8 at hjemmet i størst mulig grad skal unntas fra inngrep da det anses å være det mest private sted. Hemmelig ransaking er inngrep i hjemmet, da det i utgangspunktet kreves fysisk tilgang til området, eventuelt kan ransakelse av datasystem foregå uten fysisk tilstedeværelse fra politiet. Dette er en likhet ved dataavlesning. På den annen side vil det at det ikke gjøres fysisk innbrudd i hjemmet virke skjermende for mistenkte.

Et hensyn som gjør seg særlig gjeldende ved vurderingen av inngrepsstyrken er hensynet til tredjeparten. Tredjeperson er uten tilknytning til forholdet som søkes klarlagt ved metodebruken. Ved å kunne rette dataavlesning mot et bestemt datasystem som i utgangspunktet disponeres av mistenkte, vil dette begrense informasjonsomfanget og således begrense mot unødvendig inngrep i tredjepersons rett til privatliv. På denne måten anses dataavlesning ofte som en mer målrettet informasjonsinnhenting enn de opprinnelige tvangsmidler.

Et datasystem som anvendes av flere personer, utvider sannsynligheten for inngrep i tredjepersonens private sfære. Hensynet gjør seg særlig gjeldende når vedkommende er utenfor mistanke, det er således ikke oppklaringshensyn som kan begrunne inngrepet i tredjepersons rett til privatliv. Det er et krav om at metodebruken må være forholdsmessig jf. Straffeprosessloven §170a.[69] Av hensyn til tredjeparten tilsier dette et strengt krav for inngrep som kan ramme vedkommende. Ved vedtakelsen av dataavlesning i norsk straffeprosess, ble sannsynligheten for inngrep i retten til respekt for privatliv utvidet i vesentlig grad.

[69] Ot.prp.nr.60(2004-2005) s.73

Et spørsmål som må drøftes er om effektiv kriminalitetsbekjempelse kan tilfredsstilles med metoder som er mindre inngripende.

For at et inngrep i retten til privatliv skal være legitimt, må det være "necessary in a democratic sosicety" jf. EMK art 8 nr. 2. Det følger videre av konvensjonspraksis at inngrepet må svare til "*a pressing social need*"[70] og at inngrepet fremstår som "*propprtionate to the legitimate aim pursued*"[71]. For at dataavlesning skal anses nødvendig må det kunne påvises et pressende samfunnsbehov og behovet må være proporsjonalt i forhold til formålet som søkes nådd ved metodebruken.

Hvor inngrepet begrunnes i nasjonal sikkerhet og kriminalitetsbekjempelse, tillegges medlemsstatene et visst skjønn ved vurderingen av hvilke metoder som anses nødvendige.[72] Med dette tillegges staten en mulighet til å vurdere hvilke metoder som er nødvendige. For å være i tråd med EMK har nasjonal lovgiver måtte vurdert behovet for dataavlesning og konkludert med at det forelå et behov for metoden.

Videre er det et krav om at inngrepet er proporsjonalt i forhold til det formål som søkes oppnådd.[73] Vurderingen etter dette tar sikte på hvorvidt inngrepet er forsvarlig og hvorvidt metoden er nødvendig. I dette ligger at målet ikke kan søkes nådd ved lempeligere midler. Utgangspunktet er at politiets adgang til bruk av skjulte tvangsmidler, ikke må være videre enn nødvendig for å tilfredsstille behovet for effektiv kriminalitetsbekjempelse. Politiets metoder skal heller ikke dekke behovet for effektiv kriminalitetsbekjempelse fullstendig.[74] En utvidelse av bruken av opprinnelige metoder, eller en innføring av nye metoder kan gi positivt utslag for kriminalitetsbekjempelsen.

På den annen side er det ikke grunnlag for utvidelser eller metoder som vil være uforholdsmessig inngripende i personvernet overfor mistenkte og tredjepersoner.[75] Med dette

---

[70] Se Olsson dommen- +++

[71] Olsson dommen og Aall s.142

[72] Klass v. Germany avsnitt 49

[73] The Sunday Times v. The United Kingdom avsnitt 67

[74] Prop. 68L (2015-2016) s. 259-260.

[75] Sunday Times

menes at dataavlesning må være egnet til å ivareta sikkerhet, forebygge uorden eller kriminalitet og samtidig ivareta andre lovfestede rettigheter.
Det er enighet om behovet for å gi politiet tilgang på elektronisk kommunisert og lagret informasjon, og at tilgangen vil stå udekket dersom dataavlesning ikke er tillatt som middel for å tilgjengeliggjøre informasjonen. Forslaget om dataavlesning som gjennomføringsmåte utfordrer de opprinnelige hjemlene ved å tillegge dem en tolkning som opprinnelig ikke var tiltenkt dem ved utformingen. Dette vil også stride med hensynet til forutberegnelighet for borgerne. Et skjult inngrep i mistenktes datasystem synes vanskelig å kunne hjemles i bestemmelser om kommunikasjonskontroll. Adgang til ransakelse av datasystem synes noe enklere hjemlet i ransakelsesbestemmelsen da adgang til ransakelse også må gjelde elektronisk datasystem.

Det følger av EMD at det er et krav om at inngrepet er proporsjonalt i forhold til formålet som søkes oppnådd.[76] Vurderingstema blir hvorvidt det er nødvendig med et slikt inngrep i forhold til å verne individets rettigheter i et konkret tilfelle.

På bakgrunn av opplysninger fra Nasjonal sikkerhetsmyndighet, legger metodekontrollutvalget til grunn at bruken av krypteringer øker.[77] En utvikling i denne retning tilsier at politiet må være rustet til å kunne avdekke denne nyere kriminalitet. Vurderingen av om inngrepet kan anvendes beror på kriminalitetskravet. Kriminalitetskravet viser ikke ensidig til samfunnets behov for beskyttelse, men også til nødvendighetsvurderinger og setter således skranke for hvilke handlinger som begrunner bruk av dataavlesning. Kan resultatet oppnås med mildere middel enn dataavlesning taler dette for at mindre inngripende metoder skal brukes for tilfellet.

En risiko ved dataavlesning er dermed at også andre enn politiet kan utnytte informasjonen i datasystemet.[78]Politiet bør i følge departementet ha adgang til å installere og benytte egnet programvare, teknisk utstyr, sikkerhetshull eller sårbarhet i datasystemet, og foreta innbrudd for å installere og fjerne programvare eller maskinvare dersom det er nødvendig for å foreta

[76] Sunday Times v. The United Kingdom avsnitt 67.

[77] NSM foretok undersøleøser som metodekontrollutvalget la til grunn NOU 2009: 15 s.241.

[78] NOU 2009:15 s 249

dataavlesning. Disse fremgangsmåter øker risiko for skade på datasystemet og at andre kan skaffe seg uberettiget tilgang til systemet.

Skaderisikoen for datasystemet er drøftet i forarbeidene til loven hvor departementet i stor grad tilslutter seg metodekontrollutvalgets uttalelse. Det legges til grunn at skaderisikoen er liten, og uansett innenfor det akseptable.[79] Departementet påpeker at faren for at andre vil utnytte systemet vil sikres gjennom krav til fremgangsmåte og kompetanse fra de som utfører metodebruken. Det må kunne stilles krav til løsningen politiet velger i forhold til risikoen i for valg av metode. Sett i lys av dette er det ikke drøftet særlig i forarbeidende om den konkrete risiko dataavlesning medfører. Det stilles bare krav om at gjennomføringen må skje på sikrest mulig måte.[80]

2.5 Oppsummering

Selv om dataavlesning er ett nytt tvangsmiddel, skiller det seg ikke i vesentlig grad fra de opprinnelige metoder da det er basert på samme vilkår for inngrep.[81] Dataavlesning åpner for kontroll av informasjon som før krevde både adgang til kommunikasjonskontroll i tillegg til ransakelse. Dataavlesning kan foregå over lengre tid sammenlignet med ransaking som bare gav tillatelse til en enkeltransakelse. På denne måten blir rommet for kontroll i vesentlig grad utvidet og effektivisert.

Slik begrepet dataavlesning er drøftet overfor er det også en rekke forskjeller i forhold til opprinnelige tvangsmidler. Med tanke på kilder som kan gjennomsøkes, omfanget av informasjon, overskuddsinformasjonen og den skjulte innhentingen som er vanskelig å oppdage utgjør dataavlesning et mye større inngrep i retten til privatliv. Kilder til kontroll er utvidet og ikke i uvesentlig grad. Hva som kan gjøres til rom for kontroll angis ikke klart i lovteksten, men hemmelighold av politiets metode legitimeres med behovet for at de ikke skal bli for forutsigbare og at politiets adgang til datasystemet forringes. Det er helt klart uheldig at kriminelle kan opptre på arenaer hvor politiet ikke har metoder for å utøve kontroll.

Det fremkommer at dataavlesning er mer effektivt i forhold til å løse dagens teknologiske utfordringer. Det er på den annen side derimot ikke påpekt i like stor grad hvordan

---

[79] NOU 2009: 15 punkt 23.3.5 se videre Prop. 68L(2015-2016) s .266-267

[80] NOU 2009:15 s. 244

[81] Drøftelsen i punkt 2.4

dataavlesning vil være et større inngrep i den personlige sfære. Departementet har tidvis lagt til grunn samme begrunnelse som metodekontrollutvalget. Metodekontrollutvalget kom til at metoden var for integritetskrenkende i 2009, så det er betenkelig at departementet ikke viser en konkret endring i samfunnet som begrunner en utvidet adgang til dataavlesning.

3 Relevante hensyn ved vurdering av metoden

3.1 Innledning

Den teknologiske utviklingen vi står overfor og behovet for nye metoder for å kunne innhente opplysninger medfører tekniske, juridiske og etiske problemstillinger. Retten til respekt for privatliv er en menneskerettighet tillagt ethvert individ i kraft av å være menneske. Inngrep i rettigheten krever legitime og tungtveiende grunner som kan forsvare inngrepet. Vilkårene setter grensen for bruk av skjulte tvangsmidler. Enkelte av vilkårene er skjønnsmessige. Skjønnsmessige vilkår åpner for spørsmål om hvilke verdier og hensyn som kan begrunne bruken av tvangsmidlene overfor den enkelte, og tillegger politiet et visst spillerom for vurderingen innenfor vilkårenes ramme.

Dataavlesning gir mulighet til å føre kontroll med borgernes adferd. Ved å gi politiet rett til dataavlesning er dette en rett til overvåking av personer aktivitet ved datasystemer, med formål om å ivareta samfunnssikkerheten. Dette ville gå på bekostning av individets rett til privatliv, vern om personopplysninger, demokrati, ytringsfrihet og rettssikkerhet mens det til gjengjeld skal beskytte enkeltindividet eller samfunnet. Inngrepet i retten til privatliv må den enkelte stat i utgangspunktet avstå fra. Staten har videre aktivitetsplikt for å sikre ytringsfriheten, bevegelsesfrihet, handlingsfrihet og er forpliktet til at slike inngrep i privatsfæren må begrenses. Spørsmålet er hvor grensen for inngrep i den privates sfære trekkes, og reguleres av lovgiver innenfor rammen av de overordnede menneskerettslige grenser.

Etter norsk rett er det tradisjon for at politimetoder kun kan innføres eller anvendes dersom det er forsvarlig ut fra hensynet til personvern og rettssikkerhet.[82] Videre stiller lovteksten nærmere vilkår for bruk av metoden. Lovgiver har ved innføring av bestemmelsen generelt

[82] NOU 2009:15 pkt 23.2.3

vurdert de kryssende hensyn. Verdiene som ligger til grunn kommer til uttrykk gjennom vilkårene og også gjennom forholdsmessighetsvurderingen. Hensynene kommer også inn ved vurdering i den konkrete saken, men da som del av skjønnsutøvelse for om metoden skal brukes eller ikke. Dataavlesning kan ikke anvendes i et hvert tilfelle hvor det kan påberopes behov for konkrete opplysninger. Det må foretas en vekting av motstridende interesser i saken og nødvendigheten av metoden. Kapittelet vil derfor omhandle de relevante hensyn som gjør seg gjeldende ved klarlegging av terskelen for vurdering av anvendelse av dataavlesning. Formålet er å se på de motstridende interesser som berøres ved metodebruken.

3.2 Behovet for en effektiv kriminalitetsbekjempelse

Kriminalitet utgjør et avvik fra sosiale normer og leveregler slik vi kjenner dem. Kriminalitet anses å være et uberettiget angrep mot individer, grupper, miljø og samfunnet som skaper uro og usikkerhet i befolkningen. Store mengder uoppklarte saker tilsier en viss utrygghet i befolkningen.[83] Kriminalitetsbekjempelse er således en viktig samfunnsoppgave. Oppklaring i en sak gjenoppretter trygghetsfølelsen og er således viktig av hensyn til å bevare samfunnet.

Metodekontrollutvalget la til grunn at det overordnede formål ved politiets bruk av tvangsmidler er "*effektiv kriminalitetsbekjempelse*".[84] Kriminalitetsbekjempelse er den virksomhet som drives for å hindre at samfunnet og borgerne utsettes for kriminelle handlinger.[85] Utgangspunktet i dagens samfunn er at alle mennesker står fritt til å gjøre som de selv vil. Derimot er handlefriheten begrenset gjennom lov og normer. Begrensning i handlefriheten krever begrunnelse etter styrken på inngrepet og regulerer at handlefriheten ikke misbrukes.

Ved at metodekontrollutvalget og departementet påpeker hvilke utfordringer dagens samfunn står overfor og hvordan den teknologiske utvikling påvirker hverdagen, viser dette hvordan tvangsmidler som blant annet ransaking og kommunikasjonskontroll ikke tjener formålet i tilfredsstillende grad.[86]For en reell kriminalitetsbekjempelse må virkemidler som stilles til rådighet for politiet være egnet til å løse kriminaliteten de står overfor. Hvis ikke vil kriminalitetsbekjempelsen i samme grad vanskeliggjøres. Selv om kriminalitetsbekjempelse

[83] NOU 2009:15 s.68

[84] NOU 2009:15 pkt 6.6

[85] NOU 2009:15 s 68 pkt 8.1

[86] Prop. 68L (2015-2016) pkt 14.6.2

er en viktig samfunnsmessig oppgave, er det ikke gitt at virkemidlet for kriminalitetsbekjempelse kan anvendes i et konkret tilfelle. Metodebruken ved kriminalitetsbekjempelse stiller krav til det motstridende behov for blant annet beskyttelse av personvern. Inngrep i slike rettigheter må skje innenfor rammene av norsk lovgivning og folkerettslige forpliktelsene. Et kriminalitetsbilde i stadig utvikling krever at metodene møter utfordringene for at myndighetene skal kunne utøve sine oppgaver. Hensynet til effektiv kriminalitetsbekjempelse taler derfor for at politiet kan ha behov for nye skjulte tvangsmidler.

3.3 Demokrati mot behovet for kontroll

I demokratiske rettsstater er det forutsatt at det eksistere grenser for hvordan staten kan handle i forhold til borgerne med det formål å ivareta samfunnsinteresser. Videre følger det at det også er regulert hva borgerne kan gjøre overfor hverandre.[87] Lovgiver har kompetanse til å gjøre menneskets handlinger straffbare, med det formål å regulere befolkningens handlinger i ønsket retning. Det er ikke en ubegrenset adgang til å gjøre menneskers handlinger straffbare, da begrensninger følger av grunnloven og menneskerettighetene.

Norge er et folkestyrt land. Staten har mange oppgaver i et vidt spekter. Ved å ha tilgang til borgernes private samtaler, opplysninger og bevegelse, gjøre statens oppgaver enklere i kontrolløyemed. Dersom det gis adgang til å kunne foreta kontroll med enkeltpersoners kommunikasjon eller en generell kontroll av befolkningen vil dette kunne gjøre det enklere å avsløre kriminell virksomhet. Dette vil igjen kunne lede til bekjempelse kriminalitet og å kunne sikre statens sikkerhet.

Å sette personvernet til side for å kunne føre overvåkning av personer som er mistenkt for slik alvorlig kriminalitet som nevnt i strpl § 216 o, har positiv effekt for bekjempelse av kriminalitet og samfunnsvernet. I andre enden står vernet for enkeltindividet. En slik overvåkning vil ha negativ virkning da staten får tilgang til individers private sfære. I strpl. § 216 o er det oppstilt et krav om at inngrep i privatlivet må være proporsjonalt. Uproporsjonale inngrep vil kunne medføre en ubalanse i maktforholdet mellom stat og boger.

Forholdet mellom stat og borger reiser spørsmål ved hvilke hensyn som skal tillegges størst vekt. Hensynet til samfunnsvernet eller hensynet til privatlivet. Det er ikke noe absolutt vern om retten til privatliv eller om samfunnsvernet. Det beror på vektingen av mistankestyrken og

[87] Eskeland s. 63

alvorligheten av mistenkt kriminalitet. Et sentralt skille er her om personen kan knyttes til slik alvorlig kriminell handling som utgjør sikkerhetstrusler, eller om personen sannsynligvis er uskyldig. En sterkere mistanke om alvorlige kriminelle forhold, jo lettere må det kunne aksepteres inngrep i personvernet.

Overvåkning er et sterkt inngrep i den private sfæren og har potensiale til å svekke demokratiet. Et samfunn hvor det ikke er mulig å begå alvorlige lovbrudd, kan tale for at den demokratiske rettsstat er opphevet, da handlefriheten eller kontrollen er så streng at et hvert forsøk vil avverges eller være umulig å gjennomføre. Til gjengjeld vil hensynet til kriminalitetsbekjempelse være ivaretatt i stor grad. En demokratisk rettsstat beror på tillitsforholdet mellom borgere og staten, hvor handlefriheten er det sentrale utgangspunkt. Den dagen handlefriheten ikke eksisterer er også Norge å omtale som totalitært diktatur eller politistat, hvor handlefriheten er underlagt streng kontroll og de demokratiske verdier fraveket.

3.4 Rettssikkerhet

Begrepet rettssikkerhet er ikke entydig, da det er vanskelig å tillegge det et presist og allment innhold. Kjernen i begrepet går på at individet skal være beskyttet mot vilkårlighet og overgrep fra myndighetens side.[88] Selv om det ikke er konkret angitt hva rettssikkerhet er, uttaler Eckhoff at det er en egen kategori rettssikkerhetshensyn som har særlig vekt i juridiske sammenhenger.[89] Begrepet rettssikkerhet er tradisjonelt sentralt i forholdet mellom enkeltindividet og staten. Det gjør seg særlig gjeldende innenfor strafferetten med tanke på forsvarlig saksbehandling og muligheten til å forutberegne sin stilling. Hensynet til rettssikkerhet tillegges vekt både ved utforming av lov og ved tolkning.

De interesser hensynet til rettssikkerhet søker å ivareta er borgerens integritet og autonomi i forhold til statsmakten.[90] Med dette tas det sikte på å beskytte individet fra vilkårlig inngrep fra statsmakten og å sikre rettighetene i forhold til det offentlige. Rettssikkerhet skal verne mot inngrep i personvernet som vil forhindre misbruk og overgrep som følge av en innsamling av borgernes personopplysninger.

---

[88] Knoph s. 614-617

[89] Eckhoff s.395

[90] NOU 2009: 15 s 60

For ivaretakelsen av rettssikkerhetsgarantier krever makt fra det offentlige hjemmel i lov og andre konstitusjonelle garantier som setter rammer for statens maktbruk. Ved dataavlesning er det sentrale sikkerhet mot overgrep fra statsmakten. For anvendelse av dataavlesning skal det vernes mot inngrep i personvernet som kan medføre at staten får uberettiget informasjon om borgernes personlige forhold. Staten må ikke gis informasjon som anses å være uforholdsmessige i forhold til det målet det skal tjene. Rettssikkerhet ivaretar hensynet til at det ikke skal foretas overgrep og vilkårlighet, således skal rettssikkerhetskravene sørge for at inngrepet skjer innenfor rettslige rammer. Alle har krav på rettssikkerhet og det kan bare gjøres inngrep når vilkårene for dataavlesning er oppfylt jf. strpl. § 216 o. Vernet er således at kriteriene for tvangsmiddelbruk er oppfylt.[91] Den som selv velger å foreta handlinger som berettiger inngrep i retten til personvern, svekker selv sin rettssikkerhet og må akseptere tvangsmiddelbruk i samsvar med lovens vilkår. Det sentrale vern er således klare vilkår som sier noe om når metodebruken kan forekomme.

3.5 Ytringsfrihet

Ytringsfrihet er en grunnleggende rettighet i en demokratisk rettsstat. Ytringsfrihet er "den enkeltes rett til å gi uttrykk for sin mening offentlig".[92] Ytringsfriheten er nasjonalt forankret i Grl. § 100 og internasjonalt i blant annet EMK art.10. Grl. § 100 sier at "ytringsfrihet bør finne sted". At lovteksten bruker ordet bør trekker i retning av det ikke er en rettighet som må utøves. På den annen side skal det i tråd med dagens språkkultur forstås som "skal". Formuleringen slik den er inntatt i lovteksten er i følge kommisjonen begrunnet i grunnlovens språkdrakt. [93] Ytringsfrihet er en grunnleggende rettighet i et demokratisk samfunn og regelen skal anses som en bindende norm. Selv om det er en grunnleggende rettighet er ytringsfrihet ikke en absolutt rettighet. Staten kan legge føringer og begrense ytringsfriheten, men det må skje i samsvar med Grl. §§ 96 og 97.[94]

Formålene bak ytringsfriheten er av betydning både for samfunnet og enkeltindividet. Legges det for strenge føringer på ytringsfriheten vil det gå på bekostning av verdier som demokrati,

---

[91] NOU 2004: 6 punkt 6.4

[92] NOU 1995:3 Mangfold i media, om eierkonsentrasjon i massemedia kapittel 3.2

[93] NOU 1999:27 Ytringsfrihet bør finne sted kapittel 10, se særlig punkt 10.3.2 om grunnloven §100 første ledd.

[94] Aall s.243

åpenhet og tillit til myndighetene. Det er hensyn til demokratiet, sannhetsargumentet, selvutfoldelseshensynet og autonomiprinsippet som bakenforliggende hensyn for retten til ytringsfrihet.[95]

Ytringsfrihet er ikke bare retten til å foreta ytringer også retten til å forholde seg taus er et viktig rettsstatsprinsipp.[96] I tilfeller hvor regjeringen styrer informasjonstilgangen og mulighet for å foreta ytringer, eksisterer ikke frie valg. EMK art.10 uttaler at ytringsfrihet omfatter "*freedom to receive and impart information and ideas without interference by public authority and regardless of frontiers*". Viktigheten av EMK art.10 blir videre understreket i saken *Handysude v. United Kingdom* som sier at ytringsfrihet "constitutes one of the essential foundations of a democratic society, one of the basic conditions for its progress and for the development of every man".[97] Her fremkommer flere fundamentale sider ved ytringsfriheten. Også informasjonsfrihet må regnes med. Ytringsfrihet omfatter også informasjonsfrihet som er retten til informasjon.[98]

Innhenting av informasjon ved dataavlesning stiller spørsmål om ytringsfriheten på flere nivåer. Ett nivå er at retten til innsyn i en persons datasystem utfordrer ytringsfriheten i den grad frykten for at ens personlige og innerste tanker skal bli gjenstand for kontroll. En slik følelse kan medføre at en hver vil vurdere forholdene før en tør ytre seg. Dette vil stride mot prinsippet om ytringsfrihet, som staten skal tilrettelegge for. Hvis mennesket må tenke seg om før det fører en samtale i frykt for at informasjonen innsamles, vil dette utgjøre et stort inngrep i ytringsfriheten og også i demokratiet.

De færreste mennesker utgjør en trussel mot medmennesker, samfunnet og samfunnssikkerheten i den grad som berettiger dataavlesning. Dette begrunner at de færreste

---

[95] NOU 1999:27 s.20-24.

[96] Det er et grunnleggende prinsipp i rettsstaten og fremkommer bant annet i strpl. §§90, 123 og 232. Hensynet er at vedkommende skal slippe å lyve eller å bidra til egen domfellelse. Det fremkommer Funke v. Frankrike (avsn.44) at ble det ansett for å være i strid med kravet om "fair trial" jf. EMK art. 6 at franske myndigheter under trussel om løpende mulkt hadde pålagt en borger å avgi opplysninger som kunne medføre at han senere ble funnet skyldig i annet straffbart forhold.

[97] Handyside v United Kingdom avsn.49

[98] NOU 1995: 3 pkt 3.2

vil være omfattet av kontroll. Derimot vil dataavlesning gi myndighetene tilgang til mer informasjon om svært mange nordmenn. Bare det at staten har en regel som tillater omfattende overvåking herunder dataavlesning, vil gi borgerne en følelse av kontroll fra myndighetene. Denne følelsen vil kunne legge føringer på individets ytringer.

Vernet om ytringsfriheten må veies opp mot personvern og privatlivets fred og interesser beskyttet gjennom lovgivningen, for eksempel hatefulle og rasistiske ytringer. Ytringsfrihet og personvern er likeverdige rettigheter og hensyn.[99] Ingen av hensynene får generelt betydning foran den andre. Enkelte ytringer må begrenses når andre vektige hensyn går fremfor. Personvern er ikke en rettighet som alltid står i motstrid til ytringsfriheten

3.6 personvern og personopplysningsvern

Etter utgangspunktet om at rettsstatens borgere har krav på alminnelig handlefrihet, følger prinsippet om borgerens rett til privatliv. Retten til respekt for privatlivet innebærer at en borger fritt skal kunne leve uten frykt for å bli forstyrret av enkeltindivider eller av myndighetene, og utgjør begrunnelsen for personvernet.[100] Vernet er utstrakt både internasjonalt og nasjonalt. Det finnes ingen generelle regler om beskyttelse av personvern, og heller ingen legaldefinisjon, men det er en rekke spredte bestemmelser som tar sikte på å verne retten til privatliv, personvern og personopplysninger.

Personvern defineres på ulike måter. Kjernen i begrepet går på hvert menneskes ukrenkelige rett på respekt fra andre mennesker for egen integritet og fred i sitt privatliv.[101] Personvernet ligger på denne måte nært forholdet med den mer internasjonale termen "*retten til privatliv*".[102] Ved bruk av skjulte tvangsmidler gjøres det inngrep i disse rettighetene. Innhenting av informasjon utgjør således ett inngrep i retten til respekt for privatliv og vern om personopplysninger. Spørsmålet er således hvordan tvangsmiddelbruk gjør inngrep i de ulike vernede interesser.

Personvern og personopplysningsvern er to begreper som brukes om hverandre uten klart innhold. Begrepet personvern har det alltid vært diskusjon rundt preget av terminologisk

---

[99] NOU 2009: 1 s.96

[100] NOU 2009:15 s.50

[101] NOU 2009: 1 s.11

[102] NOU 2009: 1 s.30-31

uklarhet, forvirring og strid.[103] Begrepene tolkes ulikt og har noe ulikt innhold. Skillet mellom begrepene er ikke særlig klart i norsk rett, men er forsøkt klarlagt i blant annet Schartum og Bygrave og Stortingets IKT-melding av 2006.[104]

Personvern regnes som en *særnorsk* term som brukes sammen med eller istedenfor personopplysningsvern og privatliv.[105] Retten til privatliv går ut på at et hvert enkelt individ har en privat sfære hvor de kan leve uten innblanding fra staten eller andre personer. Det eksisterer ingen legaldefinisjon av personvernbegrepet. En språklig forståelse av begrepet tilsier et vern om privatliv og vern av personlige forhold. I retten til privatliv ligger retten til privatlivets fred og personlig integritet. Det er derfor nødvendig med en nærmere undersøkelse om hva som inngår i personvernet og personopplysningsvern, da det er relevant ved spørsmål om hvilke rettigheter som er vernet fra inngrep ved dataavlesning.

NOU 2009: 1 side 30 definerer personvernet som "et knippe av ideelle interesser som en tillegger enkeltmennesker".[106] I disse interesser inngår diskresjon, innsyn, fullstendighet og privatlivets fred. Dette innebærer ønsket om kontroll med opplysninger om seg selv, hvordan opplysningene behandles og at avgjørelser treffes på bakgrunn av rette og fullstendige opplysninger, og interessen individet har i respekt for privatlivet uten inngrep fra andre. Dette er interesser som ikke alltid står i harmoni, og en eventuell konflikt søkes løst ved avveining mellom interesser.

I forarbeidene til personopplysningsloven er det tre perspektiver på personvern; integritetsperspektivet, beslutningsperspektivet og maktperspektivet.[107] Integritetsperspektivet er et uttrykk for ønsket om kontroll over egne opplysninger, særlig personopplysninger. Ved politiets bruk av skjulte tvangsmidler gjøres observasjon, innsamling og behandling av personopplysninger. Bruken av skjulte tvangsmidler er derfor et inngrep i personvernet etter integritetsperspektivet. Beslutningsperspektivet går ut på at opplysninger som er innsamlet kan brukes som beslutningsgrunnlag. Maktperspektivet er basert på "kunnskap er makt" og at

---

[103] NOU 2009: 1 s.29

[104] NOU 2009: 1 s.32 se videre henvisninger til St.mld. nr.17(2006-2007) *Eit informasjonsamfunn for alle* s.130

[105] NOU 2009: 1 s.30

[106] NOU 1997:19 s. 24-26

[107] NOU 1997: 19 s.21-24

kunnskaper om andre mennesker kan gi makt overfor de mennesker opplysningene gjelder og i alminnelighet.

Utviklingen fra den gang har gått i retning av at personvern er en mye videre beskyttelsesverdig interesse, da personvernet nærmest er å beskrive som den personlige integritet.[108]

Personvernkommisjonen definerer "*personvern*" som "*ivaretakelsen av personlig integritet; ivaretakelse av enkeltindividers mulighet til privatliv, selvbestemmelse(autonomi) og selvutfoldelse*"[109]. Videre definerer de "*personopplysningsvern*" som "*regler og standarder for behandling av personopplysninger som har ivaretakelse av personvern som hovedmål. Reglenes formål er å sikre enkeltindivider oversikt og kontroll over behandling av opplysninger om dem selv. Med visse unntak skal enkeltpersoner ha mulighet til å bestemme hva andre skal få vite om hans/hennes personlige forhold*"[110]

Etter ordlyden i definisjonene personvernkommisjonen fremla i 2009 fremstår personopplysninger som en mer snever rettighet i forhold til retten til respekt for privatliv. Retten til respekt for privatlivet må anses å gjelde alle opplysninger som omhandler en persons liv. Personopplysninger omhandler opplysninger om privatlivet til individet.

Et sentralt element i personvernet er at individer skal ha mulighet til å kontrollere egne personopplysninger, vite hva andre kjenner til og hva ens personopplysningene brukes til. Dette er det lovregulerte personopplysningsvern og hvordan begrepet "personopplysninger" er definert i underlovgivningen.[111] Personvernet er derimot ikke et absolutt vern, og kan tenkes å måtte vike i møte med motstridende interesser.

Behovet for en privat sfære er kjernen i den personlige integritet. Personlig integritet omfatter individets selvbestemmelse over egen kropp, eiendom og tanke. Personvern og personlig integritet har således mye til felles. Forskjellen står i at personvernet tar sikte på retten til ikke

---

[108] NOU 2009: 1 s.36-37

[109] NOU 2009:1 s 32

[110] NOU 2009:1 s.32

[111] Personverndirektivets artikkel 2 litra a. Begrepet finnes definert i personopplysningsloven § 2 nr. 1

å bli overvåket eller observert i den private sfære, mens den personlige integritet er retten til å kunne tenke og bevege seg fritt i den private sfære. Ved anvendelse av skjulte tvangsmidler og herunder dataavlesning omhandles personvernet i større grad enn integritetsvernet, da metodebruken er i kjernen av behandling av opplysninger om ens person. Ved dataavlesning samler politiet inn informasjon. Slik informasjon kan være svært omfattende og av sensitiv karakter. Selv om opplysningene ikke er av sensitiv karakter, vil de derimot samlet sett kunne utgjøre sensitive opplysninger.[112] Bare eksistensen av regelen om dataavlesning vil således utgjøre inngrep i personvernet.

Når det kommer til bruk av skjulte tvangsmidler utgjør de et inngrep i personvernet uavhengig om tvangsmiddelbruken resulterer i videre forfølgelse. Det å drive kontroll med borgerne utgjør ett inngrep uavhengig av om informasjonen anvendes eller ikke. Andre personer enn den opplysningene dreier seg om har da fått kunnskap om slike opplysninger som er beskyttet av rettigheten. Dette er uttalt i *VUKOTA-BOJIĆ* hvor den innsamlede informasjon ble ansett som et inngrep[113] Om informasjonen anvendes i senere anledning er uten betydning for om overvåkningen skal anses som et inngrep i privatlivet.[114]

Et skille mellom begrepene vil klargjøre forskjellene mellom personvern og personopplysningsvern. Rettighetene ser ut til å henge tett sammen, og er gjensidig avhengig av hverandre da det er vanskelig å definere det ene begrepet, uten å avgrense opp mot det andre. Dette gjenspeiles også i personopplysningsloven §1 som karakteriserer personopplysningsvernet som en underkategori av personvernet. At det ikke har eksistert noe klart skille mellom begrepene er ikke ensbetydende med at det kun eksisterer rettigheter for den ene kategori.

Formålet med dataavlesning er å skaffe informasjon fra mistenkte og utgjør et inngrep i personvernet. Dette er et inngrep på to nivåer. Dataavlesning vil gjøre inngrep både i retten til personvern ved at noen foretar et inngrep i datasystemet og personopplysningsvern ved at

---

[112] NOU 2009: 15 s.58: *Det er imidlertid ikke mulig å gi noen uttømmende definisjon av opplysningstyper som generelt er sensitive. Sensitivitet påvirkes av flere ulike faktorer(..)..oppfatning kunne endre seg over tid og variere etter person*

[113] VUKOTA-BOJIĆ og NOU 2009:15 s.

[114] *Leander mot Sverige* (avsnitt 48) og *Gardel* (avsnitt 58)

noen kommer i befatning med ens opplysninger. Dataavlesning utgjør inngrep i personvernet ved at personer uten rådighet over et individs opplysninger ved hjelp av datainnbrudd og dataavlesning kan skaffe seg tilgang til slike opplysninger. Vedkommende kan ikke føre kontroll med hvem som skaffer seg opplysninger og hvilke opplysninger det er snakk om. Dataavlesning som tvangsmiddel er derfor svært inngripende i retten til den private sfære. Det kan ikke stilles noe generell forventning om at noen skal skaffe seg opplysninger om ens person dersom det er opplysninger som i stor grad ikke meddeles offentligheten. Hensynet til personvernet taler for at borgeren har rett til kontroll over sine personopplysninger, og kan forvente at myndighetene i minst mulig grad skal utøve inngrep for å gjøre seg kjent med opplysningene.

3.7 Oppsummering

Både kriminalitetsbildet og personvernets virkeområde er i konstant utvikling. Vurderingen av om skjult tvangsmiddelbruk bør tillates for å dekke samfunnets behov for effektiv kriminalitetsbekjempelse på bekostning av blant annet personvern, rettssikkerhet, ytringsfrihet, demokrati med mer, må foretas fortløpende. Området reglene regulerer, er i konstant utvikling og reglene må til en viss grad anvendes i takt med de endringer samfunnet gjennomgår. En rettsregel og lovtekst krever mye arbeid før den er ferdigstilt og utviklingen av lovtekst tar lengre tid enn samfunnet bruker på å ta nye retninger, eller at det utvikles for eksempel ny teknologi. Dette begrunner teknisk nøytrale regler som kan tilpasses samfunnsforholdene. Dette må utøves med forsiktighet for at anvendelsen ikke skal gå på bekostning av borgernes mulighet til å forutberegne sin rettsstilling.

Departementet har fremhevet at det er blitt en større utfordring å bekjempe visse typer kriminalitet, særlig organisert kriminalitet og terrorhandlinger.[115] Den utvidede adgangen til anvendelse av skjulte tvangsmidler i den nyere tid viser hvordan hensynet til effektiv kriminalitetsbekjempelse har vært et sentralt moment ved aksept av nye tvangsmidler, samtidig som det har medført at også personvernets virkeområde har stått i en konstant utvikling. På dette grunnlag mente departementet at samfunnets interesse i å avverge alvorlig kriminalitet måtte anses å være så tungtveiende at de betenkelighetene ved en utvidelse av politiets metodebruk, måtte kunne settes til side.[116] Tvangsmidlene er innført med

[115] Ot. Prp. nr.60(2004-2005) s.51

[116] Ot.Prp. nr.60(2004.2005) s.52

forebyggende, avvergende og oppklarende formål. Dersom kriminaliteten stadig utvikles i retning mer alvorlige konsekvenser, vil gjenoppretting vanskeligere kunne gjøres. Avverging og forebygging av kriminelle handlinger vil dermed ha økende betydning. Ved en slik vekting settes blant annet hensynet personvern, rettssikkerhet, ytringsfrihet og demokrati til side for å ivareta samfunnets behov for kriminalitetsbekjempelse. Det kan derfor sies at kravene til ivaretakelse av borgerens rettssikkerhet og personvern må sikres gjennom de vilkår som stilles for tvangsmiddelbruk. Dette må utøves innenfor den nasjonale lovgivning samtidig som bruken av tvangsmidler må foregå i tråd med de internasjonale forpliktelser.

4 Betenkeligheter ved bruk av dataavlesning sett i lys av personvern

4.1 Noen generelle betenkeligheter ved bruk av skjulte tvangsmidler

Adgangen til å benytte skjulte tvangsmidler har økt fra utviklingen ved kun bruk av tvangsmidler ved saker som omhandler narkotika. Utviklingen tatt retning til tillatelse på flere kriminalitetsområder på bakgrunn av et endret trusselbilde og av hensyn til beskyttelse av samfunnet. I politiets sikkerhetstjenestes trusselvurdering fra 2017 fastslås det at Norge og norske interesser utsettes for fremmed etterretningsvirksomhet som kan ha stort skadepotensial. Hvor aktiviteten blant annet rettes mot forsvars og beredskapssektor.[117] Myndighetenes adgang til å beskytte samfunnet mot den økende kriminalitet aktualiserte spørsmålet om adgangen til skjulte tvangsmidler[118] på bekostning av personvern.

Staten er pålagt ansvar for å sikre at handlefriheten ikke misbrukes til skade for enkeltmennesket eller felleskapet[119] og begrunner på den måten tvangsmiddelbruk overfor befolkningen. Inngrep i den enes private sfære begrunner dermed den andres rett til privat sfære.[120] I dagens samfunn stilles personvernet i en ekstra sårbar posisjon da det er mange

[117] PSTs trusselvurdering (2017), gjengitt fra «oppsummering»
[118] Bruce og Haugeland (2014) s.17

[119] NOU 2009:15 s. 49

[120] Ot.prp. nr. 60(2004-2005)

kryssende verdier og hensyn som gjør seg gjeldende mens personvernet kan i tilfeller tenkes byttet bort mot andre goder. Jo flere tvangsmidler som står til disposisjon for politiet, desto større inngrep i personvernet gjøres det, selv bare ved eksistensen av reglene.

Strafferetten ivaretar hensynet til at handlefriheten ikke skal skade enkeltmennesket eller samfunnet ved å gjøre uønskede handlinger straffbare. Straffeprosessuelle tvangsmidler er påvirket av verdiene som ligger til grunn for strafferetten. For at straffelovgivningen skal være effektiv, må politi og påtalemyndigheten være i stand til å følge opp handlingene. Det legges til grunn at straffeprosessuelle tvangsmidler er effektive verktøy i kriminalitetsbekjempelsen.[121] I noen tilfeller må personvernet vike for dette, men det må tas i betraktning hva som søkes oppnådd og at myndighetene ikke kan ha en ubegrenset rett til å gripe inn i den personlige sfære.[122] Vurderingen av om det foreligger en krenkelse av personvernet beror på vurderingen av hvor sterk interessene er i en konkret situasjon, mot vekten av motstridende interesser.

Metodekontrollutvalget evaluerte reglene om skjulte tvangsmidler og fastslo at de var effektive hjelpemidler. Videre ble det også konstatert at private samtaler uten betydning for saken, relativt ofte fanges opp ved eksempelvis kommunikasjonskontroll.[123] Dette vil virke særlig betenkelig og oppleves inngripende i retten til vern av personlige forhold. Betenkeligheten generelt ved anvendelse av skjulte tvangsmidler er begrunnet i at individet fritt skal kunne utvikle og utfolde seg, ha sosiale relasjoner og rett til å ytre seg uten å bli utsatt for inngrep fra myndighetene. Disse friheter verdsettes høyt av borgere i et demokratisk samfunn. En utvidelse av regler om bruk av skjulte tvangsmidler, innebærer en utvidet adgang til kontroll med arenaer hvor individet i utgangspunktet ikke skal overvåkes. Dette utvider inngrep i retten til privatliv og vern om personopplysninger.

Inngrepet skjer ikke bare ved politiets innhenting av opplysninger og dermed ved anvendelse av skjulte tvangsmidler, men ved all behandling av den innhentet informasjon.[124] En konsekvens av anvendelse av skjulte tvangsmidler er at bruken hemmeligholdes overfor den bruken er rettet mot. En omfattende innsamling av informasjon uten mistenktes kjennskap er

---

[121] NOU 2009:15 s. 114 flg.

[122] Rapport om elektroniske spor og personvern s. 28.

[123] NOU 2009:15 s.204

[124] Jf. Personopplysningsloven og NOU 1997: 19 s.29

betenkelig i forhold til egen ivaretakelse av personvern. Mistenkte har således ikke selv kontroll med hvilke personopplysninger andre er i befatning med, og vil ikke kunne argumentere mot grunnlaget myndighetene begrunner mistanken i som igjen begrunnet tvangsmiddelbruken. Dette gjør seg særlig gjeldende da mistenkte ikke har adgang til å ta til motmæle for måten informasjonen anvendes. Av hensyn til personvernet er dette særlig inngripende at vedkommende ikke kan hindre andre i innsyn i opplysninger som anses å være av privat karakter og en ikke ønsker at utenforstående skal komme i befatning med.

Av hensynet til rettssikkerhet skal det være prosessuelle garantier som skal kompensere for at mistenkte ikke selv kan ivareta egne rettigheter. Blant dette nevnes oppnevning av offentlig advokat jf. strpl. § 100 a. Dette kan virke inngripende for den enkelte da ytterligere en person gjøres kjent med informasjon som en i utgangspunktet ikke ønsker andre skal kjenne til. Det vil vurderes ut fra personvernet her. Derimot er det av hensyn til rettssikkerhet ansett å være en trygghet for mistenkte da advokaten skal ivareta mistenktes interesser og tale hans sak. Dersom tvangsmidlet anvendes, må dette vege opp for inngrepet at ytterligere en person kommer i befatning med mistenktes personopplysninger.

Økt tvangsmiddelbruk overfor mistenkte vil medføre økt risiko for at også personer som omgås med mistenkte vil bli overvåket, eller at det gjøres inngrep i privatlivet deres. Ved kontroll av mistenkte er det en risiko for innhenting av informasjon som også omhandler tredjeperson. Dette regnes som særlig betenkelig da det ikke er ønskelig at personer utenfor mistanke skal utsettes for overvåkning, da det i utgangspunktet ikke er noe grunnlag for kontroll med deres personopplysninger og liv.

I forlengelsen av prinsippet om individets handlefrihet følger at staten skal respektere borgerens rett til å leve uten inngrep i privatlivet. Et annet hensyn som gjør seg gjeldende er tilliten til politiet. Tilliten til politiet ligger i at samfunnet har tilkjent myndighetene midler for ivaretakelse av samfunnssikkerheten. I dette ligger at myndighetsutøvelsen må foregå innenfor de gitte rammer. Selv om tilliten til politiet ligger hos borgerne, tilsier en utvidet adgang til tvangsmiddelbruk en økt mulighet for misbruk. Myndighetens kunnskaper om private borgere øker ved økt overvåkning.[125] Overvåkningsmulighetene vil kunne skli utfor sitt anvendelsesområde og tilliten til myndighetene svekkes. Ved en utvidelse av

[125] NOU 2009:15 s.50

overvåkningsadgangen trekker dette i retning av en bevegelse bort fra den demokratiske rettstat og mot et overvåkingssamfunn hvor den privat sfære gjøres mindre privat.

I et samfunn hvor det anvendes skjulte tvangsmidler er et sentralt moment hvorvidt borgerne har adgang til å sikre seg mot registrering og en mulighet for å unngå tvangsmiddelbruk. At det foregår overvåkning av personer generelt og mot dem det ikke er grunnlag for overvåkning mot, anses som negativt. Kun ved å være sikker om at tvangsmiddelbruk og registrering ikke foregår overfor vedkommende, vil en føle seg trygg mot inngrep fra myndighetenes side. Personvernnemda har lagt til grunn at muligheten til å ferdes anonymt anses som en selvstendig verdi. All skjult informasjonsinnhenting anses som mer inngripende enn ved åpen kontroll.[126] Ved skjult tvangsmiddelbruk som omfatter innsamling av personopplysninger er muligheten for å sikre seg vanskelig. Av hensyn til inngrepets karakter er et sentralt moment hvorvidt borgerne har adgang til å sikre seg mot registrering og en mulighet til å unngå tvangsmiddelbruk.

Hvorvidt inngrepet kan forventes eller ikke og om muligheten for at inngrepet gjøres, beror på den subjektive formening om retten til privatliv mot forventingen av inngrep i rettigheten.[127] I utgangspunktet må det kunne forventes å bli observert i det offentlige rom, jo lengre ut man befinner seg i det offentlige rom desto mindre inngripende anses overvåkning å være. Til en viss grad må det kunne kreves privat sfære også i det offentlige rom. Den teknologiske utviklingen har gitt sitt bidrag til at man sjelden kan forvente å ikke bli observert, da mye av en persons handlinger registreres ved elektroniske spor. Ved overvåkning er det et skille på hvor overvåkning foretas. Hvorvidt bruk av skjulte tvangsmidler utgjør et personverninngrep, eller hvor sterkt inngrepet er beror på den subjektive formening om retten til privatliv står seg på området og forventningen om inngrep. Styrken på inngrepet kan begrunnes i borgernes forventning til inngrep.[128] Forventningen om en privat sfære er sterkest begrunner i det private hjem, jf. Grl § 102. Vernet kan ikke forventes like sterkt i det offentlige rom hvor det normalt ikke kan forventes at en ikke blir observert. Overvåkning i det offentlige rom kan således ikke sies å være helt uforventet.

---

[126] NOU 2009:15 s.57

[127] NOU 2009: 15 s.5 flg.

[128] Prop. 68 L(2015-2016) s.41

Informasjonsinnhenting skjer i flere sammenhenger og graden av sensitivitet av informasjonen, vil variere i den konkrete sak. Det er lovfestet i personopplysningsloven at noen opplysninger er å karakterisere som sensitive. I forhold til andre opplysninger enn de som er nevnt i loven, vil graden av sensitivitet bero på hvordan individet opplever forholdet.[129] Metodekontrollutvalget påpeker at metodebrukens inngripende karakter variere ut fra sannsynligheten for sensitiviteten av informasjon som fanges opp. Selve innsamlingen og behandlingen av personlig informasjon danner inngrepsstyrken. Det at politiet behandler personlig informasjon vil av de fleste oppleves som særlig inngripende.[130] Dette henger sammen med at politiet håndhever makten i samfunnet og kunnskapen de tilegner seg kan anvendes mot individet. Politiet befatning med personlig informasjon om individer, kan stille dem i en særlig sårbar posisjon.

Kriminelle har en særlig interesse i å hindre politiet fra innsyn i deres virksomhet. Ved å utvikle nye metoder for unndragelse av kontroll, er spørsmålet om politiet skal stilles med midler som muliggjør kontroll. Kriminelles adgang til å forhindre innsyn av politiet vil ikke kunne begrunne retten til privatliv og således unndragelse fra kontroll. Ett inngrep overfor kriminelle må anes å tjene et legitimt formål og hensynet til samfunnsbeskyttelse står sterkt. På den annen side må også kriminelle ha rett til et privatliv, da det ikke bare er informasjon om deres virksomhet som gjøres til rom for kontroll, men også annen informasjon. Av hensyn til de som har til hensikt å skjule informasjon fra myndighetene vil det ikke anses like inngripende med kontroll som for personer som er uskyldige. Det må kunne fastslås en viss forventning om inngrep.

Lovgiver har overordnet ansvaret for å sikre borgernes rettigheter og skal sammen med politiet ivareta borgernes sikkerhet, handlefrihet og velferd. Oppgavene utfordres av den stadig mer alvorlige kriminalitet. Denne kriminaliteten kjennetegnes med å foregå i særlig lukkede miljøer. For å ivareta sikkerheten kan dermed ikke overvåkningsnivået være for lavt. En innføring av de nye tvangsmidler tok generelt sikte på å lette oppklaring, forebygge og å avverge alvorlig og organisert kriminalitet, hvilket innebar et vesentlig innhugg i

[129] NOU 2009:15 s.56.

[130] NOU 2003:21 s.29

personvernet.[131] En sli utvidet adgang til overvåkning vil være negativt for den private sfære da myndighetene kommer tettere på individet.

4.2 Særlige betenkeligheter ved dataavlesning

Det er ikke bare de positive virkninger og behovet for metoden som må tillegges vekt, det må også belyses hvilke utfordringer og ulemper metoden medfører. I hvilken grad dataavlesning utgjør inngrep i personvernet og retten til privatliv beror på inngrepets karakter. Et viktig moment som her skal ses på er hvilke betenkeligheter dataavlesning utgjør i relasjon retten til retten til privatliv.

Inngrepets art

Bruk av datasystem foregår ofte i den mest private sfære, i det private hjem. På den annen side er det ved bruk av internett mange som har tilgang til området, noe som taler for at man også på samme tid befinner seg i det offentlige rom. For informasjonsinnhenting i et datasystem kan det problematiseres hvorvidt informasjonen politiet søker befinner seg i en privat eller offentlig sfære, da dette vil si noe om inngrepsfølelsen ved gjennomføringen. Skillet synliggjøres når det gjelder kontroll med ferdsel på internett og kontroll med informasjon som er lagret i mistenktes datasystem. Sondringen ved anvendelse av de opprinnelige tvangsmidler gikk ut på jo nærmere man befinner seg sted for alminnelig ferdsel, desto mindre inngripende vil overvåkning virke. Dette må på den annen side nyanseres da heller ikke alt kan tenkes overvåket på offentlig område.

Et element i vurderingen av om det foreligger inngrep i retten til respekt for privatlivet er om forventning om beskyttelse av sitt privatliv. En sak som drøfter retten til personvern i arbeidssammenheng og betydningen av forventningen av retten til privatliv er *Halford mot Storbritannia.*[132]Et av spørsmålene i saken var hvorvidt Halford hadde berettiget forventning om personvern på arbeidsplassen. I saken ble det lagt stor vekt på at det ikke var gitt noen form for advarsel om at telefonene som sto til arbeidstakers disposisjon ville avlyttes, av den grunn mente EMD at hun hadde en berettiget forventning om at samtalene foregikk privat[133]. Domstolen kom til at det var brudd med EMK art.8 og at hennes rettigheter var krenket.

---

[131] Andenæs (2009) s 276

[132] Halford v. Storbritannia avsn 45

[133] Dommens avsnitt 45

Saken viser således viktigheten av om det er en forventning om ikke å bli overvåket i gitte situasjoner. Det samme kan tenkes overført til dataavlesing. Det er klart mer inngripende å bli overvåket i situasjoner man tror man er alene, enn i de tilfeller det kan forventes å bli observert. Det råder her almen bevissthet om at alt en foretar seg, legger igjen elektroniske spor og det må således kunne forventes en viss kontroll.

Retten til privatliv kan også krenkes på offentlige områder, dersom personer har innrettet seg på privat samkvem. Dette fremkommer i EMDs dom i P.G og J.H mot Storbritannia. Vernet av privatlivet vil avta etter jo lengre inn i den offentlige sone en privatperson beveger seg.

Ved anvendelse av datasystemer er muligheten til anonym ferdsel og å unndra seg fra registrering av handlinger begrenset. Det etterlates elektroniske spor overalt, hvilket begrenser muligheten for anonym ferdsel. Når man sitter i hjemmet er det en berettiget forventning om at individet ikke overvåkes. Ved bruk av datamaskinen i det private hjem er det ikke noe som taler for at handlingene som foretas skal overvåkes. Det vil derfor anses som inngripende å føre kontroll med dokumenter, bilder, notater eller annet som ikke er meddelt andre eller trådt ut av den private sfære. Ved bruk av internett kan det argumenteres for at man ikke lenger befinner seg i den innerste private sfære. Sammenlignes forventningen om overvåkning med kommunikasjonskontroll kan ikke kommunikasjonsavlytting forventes registrert til enhver tid, og en kommunikasjonsavlytting vil fremstå som mer inngripende enn kontroll med bruk av internett. Dataavlesning vil på den måten være mer forventet kontroll med og kan trekke i retning av at en kontroll her er mindre inngripende enn kommunikasjonskontroll. Er informasjonen i tillegg allment tilgjengelig taler dette for at det ikke er et inngrep i den private sfære.

En interesse som inngår i personvernet og som gjør seg gjeldende ved dataavlesning er tilliten til myndighetene og vernet mot overdreven kontroll. Med dette menes at overvåkningsnivået skal være begrenset.[134] Kontrollen fra det offentlige må ikke være så omfattende at det stilles spørsmål ved tilliten mellom myndighetene og individet. Vernet mot overdreven kontroll gjelder generelt, men gjør seg særlig gjeldende ved dataavlesning, da et datasystem gir rom for kontroll på langt flere områder enn mange andre tvangsmidler. Kontrollen med all informasjon er kanskje ikke nødvendig, da det vil lede til mye overskuddsinformasjon.

---

[134] NOU 1997: 19 s 24

Informasjon om privatlivet til individet er inngripende i seg selv. Dersom det kan tjene målet om effektiv kriminalitetsbekjempelse vil det kunne begrunne tilgangen til informasjon. Tilgang på informasjon gir i utgangspunktet bedre grunnlag for å treffe riktige avgjørelser og å komme frem til for eksempel avverging av alvorlig kriminalitet i tide. På den annen side vil tilgang til mye informasjon vil kunne villede. En innsamling av for mye informasjon fra flere kilder vil kunne undergrave den viktige informasjonen, som kan forsvinne i mengden informasjon. Informasjonstilgjengelighet om individet vil således ikke bare gå på bekostning av retten til personvern, for mye informasjon vil også kunne gå på bekostning av hensynet til effektiv kriminalitetsbekjempelse og samfunnssikkerheten. Et slikt syn innebærer at uthenting av masse informasjon, ikke alltid vil være formålstjenlig. Innsamling av mye informasjon som er irrelevant for det formål som søkes nådd taler for at det er særlig inngripende å gi tilgang til personopplysninger.

Det sosiale liv leves i dag i større grad via internett og ved hjelp av datasystemer. Det er sosiale medier, datingsider, chattemuligheter, skype og mye mer. Ved hjelp av disse teknologiske hjelpemidler opprettholder individet sosiale relasjoner. Det avhenger av hvordan personen uttrykker seg, men det anses som svært sannsynlig at informasjon som fremkommer her kan være av svært personlig art. Informasjon i disse medier kan også være uten betydning for forholdet myndighetene søker klarlagt og en kontroll med dette anses som et stort inngrep i retten til den private sfære.

Måten mennesket opptrer på via datasystemer kan være preget av tilfeldighet. Det er ikke sikkert at enhver gjennomtenker sine handlinger en foretar på datasystemet. Valg mennesket tar, kan være både gode og dårlig. Det kan være søk, notater, bilder, samtaler, som foregår spontant. Kanskje angrer vedkommende seg og vil fjerne handlingen. Ved dataavlesning kan handlingen ses i øyeblikket den foretas, den kan spores tilbake og det er ikke gitt at sletting vil fjerne spor. Å føre kontroll med dette vil øke inngrepsfølelsen og flytter kontrollsonen nærmere den innerste personlige sfære, nær tankevirksomhet. Hjemmelen tjener like fullt som grunnlag for å føre kontroll med disse medier. Ved å ha tilgang til alle disse sider av en persons liv, er det et særlig stort inngrep i retten til å fritt kunne utvikle seg selv og sosiale relasjoner uten innblanding fra myndighetene som gjør seg gjeldene.[135]

[135] NOU 2009:15 s.35

Ved å komme så nært opp i en persons tankevirksomhet er det mye som kan avdekkes hos et individ. Hensynet til effektiv kriminalitetsbekjempelse kan begrunne kontroll med dette. Dersom en person har en ide om å foreta en alvorlig kriminell handling, og legger igjen spor i datasystemet, gjøres tanken til rom for kontroll og myndighetene kan komme i befatning med dette på et tidlig stadige. På den annen side kan det tenkes at personen har foretatt søk av ren nysgjerrighet uten å ha noe klart mål om å skride til verks med handlingen. Ved å gjøre dette til rom for kontroll, kan det tenkes at steget for myndighetenes inngrep inn vil bli vesentlig lettere å ta. På denne måten kan nysgjerrighet og handlinger som aldri var ment satt ut i live danne en uberettiget frykt for kriminalitet og således et urettmessig grunnlag å foreta inngrep på.

Et inngrep som dataavlesning må ha et klart formål. Selv om dataavlesning gir mye informasjon om individet er det ikke en adgang til mer informasjon om ethvert individ. Det er uttalt at dataavlesning vil være mer målrettet enn de opprinnelig tvangsmidler og dermed mindre inngripende i privat sfæren. Målrettet informasjonsinnhenting vil være mindre personvernskrenkende og skjerme tredjepersons kommunikasjon da det kan rettes mot mistenkte. På den annen side vil det være en risiko for at det er andre som har utført handlingen i datasystemet og ikke eieren. Det kan ikke vites med sikkerhet hvem som har foretatt handlingen. Dette er en særegen risiko ved dataavlesning. I dag har de aller fleste egen datamaskin, nettbrett og smarttelefon, noe som tilsier at sannsynligheten for at det ikke er eieren selv som handler er liten. Men sannsynligheten er et faktum.

Med tilgang til mye informasjon er det sentralt hvordan politiet forholder seg til informasjon.

Dataavlesning som skjult tvangsmiddel i en rettsstat må utgjøre tvangsmiddelbruk som er forutberegnelighet for borgerne. Inngrepet må fremstå som formålsrasjonell og forholdsmessig. I tillegg må personvern og personopplysningsvernet ses i sammenheng med dette. Eksistensen av dataavlesning som skjult tvangsmiddel utgjør ett inngrep i den private sfære i seg selv. Dette begrunner at lovteksten må fremstå som klar for borgen slik at de ved å holde seg unna handlinger som berettiger dataavlesning kan sikre seg mot inngrep og således i den grad som er mulig sikre sin private sfære og å leve uten inngrep fra myndighetene.

En problemstilling ved dataavlesning er risikoen og datasårbareheten metoden har medført, som er ny i forhold til opprinnelige metoder. Ivaretakelsen av sikkerheten til systemet er

begrunnet i politiets egeninteresse,[136] hvor det hevdes at risikoen vil regulere seg selv. Med en slik metodebruk setter politiet datasystemet i en sårbar stilling. Det er derimot ikke klart hvorvidt et system er sårbart fra før deres midler er installert på systemet og hvorvidt politiet kan holdes ansvarlig for risikoen systemet er utsatt for. Dette gjør at ansvaret for eventuelle sikkerhetshull er uklart. Det er uttalt at politiet skal sikre sin metode fra at andre kan utnytte samme svakhet.[137] Det må uansett ventes at politiet ikke stiller systemet i unødvendig fare. At det eksisterer en risiko er en særegen betenkelighet ved metoden. En slik risiko for å stille datasystemet og dets informasjon i en særlig sårbar posisjon, er en grunn til at dataavlesning ikke bør anvendes.

Med flere betenkeligheter angående anvendelsen av dataavlesning reiser det spørsmål om myndighetene har god nok grunn for å avlytte slik informasjon. Det er ikke vanskelig å se at en utvidet bruk av skjulte tvangsmidler kan ha gode grunner for seg. Derimot kan ikke bare de positive virkninger ved en slik bruk av informasjon som kan legges til grunn for vurderingen av om grunnlaget for å gjøre seg kjent med slik informasjon er tilstrekkelig. Det gjøres ved informasjonsinnsamlingen og informasjonsbehandlingen et innhugg i retten til den private sfære for å ivareta sikkerheten. Intensjonen er god, å opprettholde et trygt samfunn. Samtidig skal personvernet ivaretas. Betenkeligheten om adgangen til innsyn i personlige betraktninger eller informasjon som ikke vil lagres eller kommuniseres og må regnes å være så dypt i den private sfære, tilsier at inngrep av denne grad ikke bør forekomme. Dersom det kan sammenlignes med tankevirksomhet har et klart utgangspunkt vært at ingen kan straffes for sine tanker, derfor bør også slik materiale i utgangspunktet ikke gjøres til hjemmel for kontroll.

Med tilgang til informasjon som ikke er kommunisert til noen og nærmest bare en tanke, vil en straffbar handling kunne avverges på tidlig stadige. I tilfeller hvor virkningen av den kriminelle handlingen er ugjennoprettelig skade eller medfører særdeles alvorlige konsekvenser, taler hensynet til samfunnssikkerheten for at metoden skal tillates. I et samfunn hvor vi ser en utvikling til avansert kriminalitet med stort skadepotensiale, taler dette for at

[136] Nou 2009:15 s.248

[137] Prop. 68L (2015-2016) pkt 14.8.8

politiet må stilles med midler som kan løse kriminaliteten. Dette vil gå på bekostningen av retten til privatliv.

Tanken om at den som ikke har noe å skjule har heller ikke noe å frykte, kan begrunne manges villighet til å oppgi retten til privatliv til fordel for samfunnssikkerhet. På den annen side vil det å tilgjengeliggjøre alt på et datasystem ikke alltid være ønskelig. Dersom nysgjerrighet ved dataavlesing kan karakteriseres som en forbrytelse vil friheten til å søke kunnskap begrenses. Når retten til å søke kunnskap begrenses, begrenses både selvutvikling og muligheten til å stille seg kritisk til samfunnet noe som er en viktig side av det demokratiske samfunnet.

Mennesket er redd for det ukjente. Ofte innser vi ikke heller ikke verdien av det vi hadde, før vi ser oss tilbake og det er for sent. Internett gir adgang til nytenkning, delta i diskusjoner, kommunikasjon, fildeling med mer. Friheten er innbakt i teknologi og teknologien må beskyttes om friheten skal beskyttes. Åpne kanaler for kommunikasjon må regnes som en sentral funksjon for demokratiet. En for streng kontroll med dette vil ikke tjene alle de verdier vi bryr oss om. Individet må ha mulighet til å uavhengig jobbe mot målene de ønsker, kun på denne måten skapes nytenking og en videreutvikling som må anses å være en positiv verdi for samfunnet. En for streng kontroll vil kunne forhindre dette.

I utgangspunktet bør ikke informasjon fra den innerste private sfære være gjort til rom for kontroll av hensyn til retten til privatliv. Av hensyn til effektiv kriminalitetsbekjempelse kan argumentet også trekke i retning av at all informasjon ikke bør være undergitt rom for kontroll da det kan bli for mye å forholde seg til og at overskuddsinformasjon kan forringe effektiv kriminalitetsbekjempelse. Tilgjengeliggjøring av informasjon er nødvendig for å fremme effektiv kriminalitetsbekjempelse for det er dette som tjener som grunnlag for kriminalitetsbekjempelse. Om det skal være adgang til informasjon av slik karakter må bero på strenge vilkår som må være oppfylt, hvor også menneskets frihet skal være hensyntatt. For mye kunnskap om befolkingen gir makt. Myndighetens kunnskap om befolkningen, gjør at de sitter med makt overfor befolkningen utover den myndighet de alt har. Dette begrunner ikke sikkerhet i seg selv. Men for en reell adgang til kriminalitetsbekjempelse av alvorlig art i dag, må myndighetene ha adgang til å tilegne seg kunnskap.

5 Oppsummering og konklusjon

Det har i norsk strafferett vært et balansepunkt mellom hensynet til samfunnsvern og personvern. Innføring av dataavlesning strekker balansepunktet og krever et dokumentert behov. Dette henger sammen med utviklingen av trusselbildet og at kriminaliteten i stor grad utviklet seg i takt med den teknologiske utviklingen. Kriminelle benytter seg av ny teknologi hvor planlegging, gjennomføring og kommunikasjon foregår på nye måter. Tendenser trekker i retning av at det foregår en profesjonalisering av kriminelle[138] noe som tilsier at politiet må kunne følge utviklingen for å tilegne seg informasjon og ivareta samfunnssikkerheten. Nødvendigheten av metoden er påpekt i forarbeidene og drøftet grundig. Konsekvensene på den annen side fremkommer ikke like klart. Hvorvidt dataavlesning går utover det som er nødvendig er tvilsomt etter behovet, dersom formålet kan søkes nådd ved mildere midler anses metoden som å være uforholdsmessig inngripende i retten til privat sfære.

Datasystemer og internett var en plass mennesket tidligere kunne ytre seg fritt uten frykten for inngrep i større grad. Behovet for kontroll på området ble en realitet og resulterte i en ny og fremmed metode. Mennesket er trygg i vante forhold. På den annen side tilpasser mennesket seg samfunnsforholdene. Nye metoder vil virke inngripende og har alltid en innarbeidelsestid, før man blir vant med dem og aksepterer metoden. Dette er et skummelt argument for å tillate en ny metode da grensene for hva som er personlig stadig forskyves i samsvar med den teknologiske utviklingen. Om 10 år virker kanskje ikke metoden like inngripende, fordi den fremstår som "naturlig" i samfunnet. Risikoen er at steget kan tas videre i retning mer kontroll og videre overvåkningsadgang på bekostning av retten til privatliv.

Lovteknisk er det svakheter med bestemmelsen da det bevist er gitt stort spillerom for hvordan dataavlesning skal foretas. Svakheten er at metoden medfører sterkt inngrep i privatlivet, uten at borgerne har tilstrekkelig klar beskrivelse for hvilke metoder kan utsettes for. Ordlyden åpner for et bredt spekter metoder for gjennomføring Et klart vilkår for anvendelsen av dataavlesning er at det må være nødvendig i et demokratisk samfunn. På dette nivå har lovgiver gjennom forarbeidene belyst behovet for metoden. Derimot på den annen side fremgår det ikke klart hvilke utfordringer man møter på ved ivaretakelsen av retten til personvern. Ved innføringen av strpl. § 216 o var det heller ikke foretatt noen vurderinger om

[138] Prop 68L (2015-2016) punkt 4.1

hvorfor metoden var mer nødvendig 7 år senere enn ved metodekontrollutvalgets vurdering i NOU 2009:15. Dette medfører at det kan stilles spørsmål til om en mildere metode ville være tilstrekkelig.

Kjernen er hvilke metoder staten kan tillate seg. Nasjonal lovgivning forutsetter en vurdering av hensynene til effektiv kriminalitetsbekjempelse mot blant annet personvern. Hensynene vil stå i spenning til hverandre og verken hensynet til effektivitetsbekjempelse eller personvern, kan gis fullstendig uttelling. Dataavlesning har med dette potensiale til å tjene formålet om effektiv kriminalitetsbekjempelse, samtidig som ivaretakelsen av personvern skal forekomme. Dataavlesning etter metodekontrollutvalgets forslag ville gjort mindre inngrep i retten til private sfære i større grad enn det hjemmelen gjør i dag. Slik vurderingen av nødvendigheten fremstår, er det ikke vist til ett større behov for en videre metode. Den minst inngripende metode ville tjene formålet som fremstår som hovedbegrunnelsen i forarbeidene, å avhjelpe politiets utfordringer knyttet til den teknologiske utviklingen.

Det er lett å argumentere for at samfunnet er sårbart og at det krever beskyttelse mot alvorlig kriminalitet. På dette grunnlaget kan personvern tenkes byttet bort mot kontrolltiltak som skal føre kontroll med borgerne og forhindre alvorlig kriminalitet. Dette stiller personvernet i en ekstra sårbar posisjon når dette er prisen for et sikrere samfunn.

Referanseliste

Norske Lover

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

Straffeprosessloven	Lov 22. mai 1981 om rettergangsmåten i straffesaker. Lov 17. juni 2016 nr. 54 om endringer i straffeprosessloven mv. (skjulte tvangsmidler)
Politiloven	Lov 4. August 1995 Lov om politiet
EØS-loven	Lov 27. november 1992 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS).
Menneskerettsloven	Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett.
Personopplysningsloven	Lov 14. april 2000 nr. 31 om behandling av personopplysninger.

Forskrift

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

Internasjonale kilder

Personverndirektivet	Europaparlaments- og rådsdirektiv av 24. Oktober 1995 nr. 46 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.
Datalagringsdirektivet	Europaparlaments- og rådsdirektiv av 15. mars 2006 nr. 24 om lagring av data som fremkommer ved bruk av offentlig elektronisk kommunikasjon, samt endring i europaparlaments- og rådsdirektiv 2002/58/EF.

Lovforarbeider

NOU 1995: 3	NOU 1995: 3 Mangfold i media, om eierkonsentrasjon i massemedia
NOU 1997: 19	NOU 1997: 19 Et bedre personvern- forslag til lov om behandling av personopplysninger

NOU 2003: 18	NOU 2003: 18 Rikets sikkerhet Straffelovkommisjonens delutredning VIII
NOU 2004: 6	NOU 2004: 6 Mellom effektivitet og personvern Politimetoder i forebyggende øyemed
NOU 2009: 1	NOU 2009: 1 Individ og integritet, personvern i det digitale samfunnet
NOU 2009:15	NOU 2009: 15 Skjult informasjon åpen kontroll
Prop. 68 L (2015-2016)	Endringer i straffeprosessloven mv. (skjulte tvangsmidler)

Rettspraksis

Avgjørelser fra EMD

Klass and others v. Germany	Klass mot Tyskland, EMDs dom 18. Desember 1978
Sunday times v. Storbritannia	*Sunday Times mot Storbritannia,* EMDs plenumsdom 26. april 1979
Leander v. Sweeden	*Leander mot Sverige,* EMDs dom 26. mars 1987
Funke .v Frankrike	Funke mot Frankrike, EMDs dom 25. Februar 1993
Halford v. Storbritannia	Halford mot Storbritannia EMDs dom 25. Juni 1997
P.G and J.H v. The United Kingdom	P.G og J.H mot Storbritannia EMDs dom 25. september 2001.

Gardel v. Frankrike *Gardel mot Frankrike* EMDs dom 17. desember 2009

Zakharov v. Russland Dom avsagt 4. Desember 2015

Vukota-Bojic v. Sveits *Vukota-Bojic mot Sveits*, EMDs dom 18. Oktober 2016

Avgjørelser fra Høyesterett

Rt.1993 s.1302

Rt.2005 s1137

Rt.2006 s.1398

Rt.2014 s.1105

Rt. 2015 s.1456

Litteratur

Aall 2015 Aall, Jørgen, *Rettsstat og menneskerettigheter*, 4. Utgave (Bergen 2015).

Aarli 2005 Aarli, Ragna, *Vern av privatlivets fred",* Tidsskrift for rettsvitenskap (2005) s.525 og ut.

Andenæs 2014 Andenæs, Josh, *Alminnelig strafferett*, 5. Utgave ved Matningsdal og Rieber- Mohn (Oslo 2014)

Andenæs, Josh, *Norsk straffeprosess*, 4 utgave, Samlet utgave ved Tor-Geir Myhrer (Oslo 2014)

Bekkedal 2014 Bekkedal, Terje, «Avveiningen mellom ytringsfriheten og privatlivets fred – om EMDs balansetest», *Lov og Rett,* nr. 6, 2014, s. 316-333.

Blume 2015	Blume, Peter, «Persondatabeskyttelse i stormfyldt hav», Tidsskrift for Rettsvitenskap, vol. 123, nr. 2, 2015 s. 222-246.
Bruce og Haugland	Bruce Ingvild, Haugland Geir Sunde, *Skjulte tvangsmidler*, 1. utgave (Oslo 2014)
Eckhoff	Eckhoff Torstein, *Rettskildelære*, 5. Utgave (Oslo 2000)
Eskeland 2015	Eskeland Ståle, *Alminnelig strafferet*, 4. Utgave (Oslo 2015)
Lilleholt 2009	Lilleholt, Kåre, *Knophs oversikt over Norges rett*, 13. utgave (Oslo 2009).
Myhrer 2001	Myhrer, Tor-Geir, *Personvern og samfunnsansvar*, 1. Utgave (Oslo 2001)
Nygaard 2004	Nygaard, Nils, *Rettsgrunnlag og standpunkt*, 2. Utgave (Bergen 2004)
Rainey, Wicks, Ovey 2014	Bernadette Rainey, Wicks Elizabeth and Ovey, Clare, *The European Convention on Human Rights*, sixth edition (Oxford 2014)

Sunde 2012 Sunde, Inger Marie, "Dataavlesning som etterforskningsmetode", tidsskrift for retfærd, årgang 35 nr. 1/136, 2012 s.3-35.

Andre kilder

PRE-2016-09-09-1046, PRE-2016-09-09-1047, PRE-2016-09-09-1048 *Delvis ikraftsetting av lov 17. juni 2016 nr. 54 om endringer i straffeprosessloven mv. (skjulte tvangsmidler) ny kommunikasjonskontrollforskrift og endringer i politiregisterforskriften*
Kongelig resolusjon. Statsråd Anders Anundsen

FOR-2016-09-09-1047 *Forskrift om kommunikasjonskontroll, romavlytting og dataavlesning (kommunikasjonskontrollforskriften)*

Teknologirådets rapport om *Elektroniske spor og personvern.* Nr 1. 2005 (mars 2005) Oslo

Nettbaserte kilder

Aftenposten http://www.aftenposten.no/kultur/Michal-Kosinski--Retten-til-et-privatliv-slik-vi-kjenner-det_-er-definitivt-over-617749b.html (sist besøkt 01.05.17)

Soundcloud https://soundcloud.com/vgno/benedicte-bjornland-religion-og-terror-om-svensker-og-om-kvinnesyn (sist besøkt 01.05.17)

Datatilsynet
https://www.datatilsynet.no/globalassets/global/04_analyser_utredninger/2017/tilstand-og-trender-2017-web.pdf (sist besøkt 01.05.17)