UiO : Det juridiske fakultet

Skjulte tvangsmidler og personvernutfordringer

En sammenlikning av reglene om kommunikasjonskontroll og dataavlesing, og deres forhold til personvern og rettssikkerhet

Kandidatnummer: 671

Leveringsfrist: 25.04.2023

Antall ord: 16448

Innholdsfortegnelse

1 INNLEDNING

1.1 Tema og problemstilling

Tema for avhandlingen er politiets bruk av skjulte etterforskningsmetoder som ledd i kriminalitetsbekjempelse og forholdet til personvern og rettssikkerhet. Politiets bruk av skjulte etterforskingsmetoder i politiarbeid kan gripe inn i vernet til privatliv, som er gitt etter henholdsvis Grunnloven § 102 og Den Europeiske menneskerettighetskonvensjonen (EMK) artikkel 8. Dette temaet vil belyses gjennom en analyse av straffeprosesslovens bestemmelser om kommunikasjonskontroll og dataavlesing. Det vil først redegjøres kort for bakgrunnen for reglene, fremgangsmåte ved begge metodene, og de materielle og prosessuelle vilkårene som etter gjeldende rett må være oppfylt for å ta i bruk metodene. Et siktemål med avhandlingen er også å vurdere metodebruken i lys av hensynet til personvern og rettsikkerhet.

1.2 Begrepsavklaring

1.2.1 Etterforskingsmetoder

Politiet kan benytte seg av ulike etterforskningsmetoder for å bekjempe kriminalitet. Disse kan anvendes åpent eller skjult. Videre kan metodene være lovfestet eller ulovfestet.

Forskjellen mellom ordinære (åpne) og skjulte etterforskingsmetoder ligger i hvorvidt personene får underretning om tvangsmiddelbruken som er rettet mot dem. Skjulte etterforskingsmetoder er metoder som retter seg mot enkeltpersoner, uten at det gis underretning om det, og som det senere kan besluttes utsatt eller unnlatt underretning om.[1]

Det er også viktig å presisere forskjellen mellom lovfestede og ulovfestede etterforskingsmetoder. Ulovfestede skjulte etterforskingsmetoder er metoder som utøves med hjemmel i ulovfestet rett. Som eksempel kan nevnes spaning, bruk av informanter, infiltrasjon og provokasjon. Rammene og grunnprinsippene er dannet gjennom rettspraksis og deres fremgangsmåte er regulert i rundskriv og interne instrukser.

Kommunikasjonskontroll og dataavlesing er skjulte etterforskningsmetoder som har hjemmel i lov. Det vil si at de anvendes skjult, og de har hjemmel i nedskrevet rett. Begge metodene har hjemmel i Straffeprosessloven lov 22. mai 1981 nr. 25 om rettergangen i straffesaker

[1] Bruce og Haugland (2018) side 15.

(strpl) kommunikasjonskontroll i kapittel 16 a og dataavlesing i kapittel 16 d. I det følgende vil betegnelsen «tvangsmidler» brukes om lovfestede etterforskingsmetoder.

Begrepet tvangsmidler er ikke definert i loven, og bestemmelsene i straffeprosesslovens fjerde del angir ingen uttømmende liste over de tvangsmidler som finnes i norsk rett. Det ligger likevel i ordlyden at dette er metoder som kan brukes ved tvang. Det betyr at det skjer inngrep i «enkeltmenneskets autonomi» eller selvbestemmelsesrett fordi personene må gjøre eller tåle noe.[2]

Tvangsmidler kjennetegnes ved at de er myndighetenes virkemidler, herunder politiets virkemidler i straffeprosessuell sammenheng.[3] Det er viktig å merke seg at ikke ethvert inngrep fra staten mot borgerne uten deres samtykke kan betegnes som tvangsmiddel. Betegnelsen tvangsmidler har vært benyttet til å karakterisere politimetoder som medfører krenkelser i den personlige integriteten slik at det kreves lovhjemmel.[4]

1.2.1.1 Etterforskning og politiets samfunnsoppdrag

Politiets etterforskingsmetoder bør sees i sammenheng med politiets samfunnsoppdrag. Det er statens ansvar å verne borgerne sine mot alvorlig kriminalitet som kan krenke enkeltpersoners og kollektivets rettigheter og interesser.[5] Dette ansvaret er i praksis pålagt politietaten gjennom Politiloven lov 4. august 1995 nr. 53 (politil.). Politiet, som statens forlengede arm, skal bidra til å håndheve loven gjennom å forebygge, avdekke og etterforske kriminalitet samt bidra til å skape trygghet og opprettholde ro og orden i samfunnet jf. politil. § 1. Hva politiet konkret skal gjøre for å oppnå disse målsettingene, kommer frem av politil. § 2. Politiet skal etter politiloven § 2 nr.2 *«forebygge kriminalitet og andre krenkelser av den offentlige orden og sikkerhet»,* samt etter § 2 nr. 3 *«avdekke og stanse kriminell virksomhet»*. Førstnevnte, nr.2, retter seg mot deres forebyggende virksomhet, mens sistnevnte, nr.3, peker mot den avvergende funksjonen. Deres straffeforfølgende funksjon er angitt ved *«forfølge straffbare forhold» § 2* nr.3.

På et overordnet nivå er ansvaret for politiets samfunnsoppdrag delt mellom Justisdepartementet og riksadvokaten, grunnet det to-sporede systemet. Riksadvokaten har ansvar for straffesaksbehandling, herunder det som kan betegnes som «etterforskning» i straffeprosessloven. Ansvaret for politiets ordenstjeneste og forebyggende virksomhet hører til Justisdepartementet.

[2] Bruce og Haugland (2018) side 16.
[3] Bruce og Haugland (2018) side 16.
[4] NOU 2004:6 side 55.
[5] Bruce og Haugland (2018) side 49.

Tvangsmidler kan anvendes under straffesaksbehandling og i forebyggende øyemed av Politiets Sikkerhetstjeneste (PST). Skal politiet benytte seg av tvangsmidler som ledd i etterforsking, er det en forutsetning at vilkårene for å igangsette etterforskingen etter strpl. § 224 er til stede. Formålene med etterforskingen er nærmere angitt i straffeprosessloven § 226. Politiet har også adgang til å anvende tvangsmiddelbruk etter strpl. § 222 d i avvergende øyemed. Ettersom strpl. § 222 d er plassert i straffeprosessloven, forutsettes det her også at vilkårene for igangsetting av etterforskning i § 224 jf. § 226 er oppfylt. PST kan videre anvende tvangsmidler som ledd i forebygging etter politil. § 17 d.

Kommunikasjonskontroll og dataavlesing kan dermed begjæres ved etterforskning av straffbare handlinger med hjemmel i straffeprosessloven (knyttet til «straffeforfølgende funksjon»). Samtidig kan begge metodene anvendes som politimetoder ved forebygging av kriminalitet med hjemmel i politiloven § 17d. (knyttet til «forebyggende funksjon».) Dette viser at politiet har adgang til å bruke skjulte etterforskingsmetoder i ulike kontekster under sin tjeneste.

1.2.2 Kommunikasjonskontroll

Kommunikasjonskontroll er en fellesbetegnelse på kommunikasjonsavlytting etter strpl. § 216 a og annen kontroll av kommunikasjonen etter strpl. § 216 b.[6]
Kommunikasjonsavlytting er en etterforskningsmetode som brukes for å kontrollere kommunikasjonen til en mistenkt gjennom å avlytte et kommunikasjonsanlegg, for eksempel en mobiltelefon eller datamaskin. Det skjer dermed en avlytting av samtaler eller annen kommunikasjon etter strpl. 216 a. Politiet er også gitt adgang til å foreta annen kontroll av kommunikasjonen etter strpl. § 216 b gjennom å innhente informasjon om kommunikasjonsdata eller innstille, stenge, identifisere og lokalisere kommunikasjonsanlegg.

1.2.3 Dataavlesing

Dataavlesing ble innført som et skjult tvangsmiddel i 2016 fordi eksisterende skjulte tvangsmidler hadde tapt sin effekt som følge av den teknologiske utviklingen og fremveksten av ulike løsninger for informasjonsbeskyttelse.[7] Befolkningens bruk av telekommunikasjonsmidler hadde muliggjort behovet for å utveksle «følsom» informasjon på en hurtig måte.[8] Man så en økt bevissthet i befolkningen om å beskytte sin kommunikasjon og mye tydet på at bruken

[6] Bruce og Haugland (2018) side 196.
[7] Prop. 68 L (2015-2016) side 259-260.
[8] NOU 1997:15 punkt 3.2.4.

av krypteringsprogrammer ville øke.[9] Videre var det en økt tilgjengelighet av disse krypteringsprogrammene, der programmene krypterte i tillegg kommunikasjonen uten at brukeren trengte å gjøre noe aktivt for det. Dette skapte tilsvarende bevissthet hos kriminelle, som særlig er opptatt av å «beskytte» sin kommunikasjon fra politiets innsyn. Ulike krypteringsprogrammer sørget for at kriminelle kunne kryptere sin kommunikasjon, noe som gjorde lovbestemmelsene om kommunikasjonskontroll mindre effektivt. Teknologiske krypteringsløsninger og passordbeskyttelser reduserte også effekten av reglene om ransaking og beslag, fordi de hindret politiet i nå fram til innholdet på en datamaskin og beslaglegge dette.[10]

Lovens skille mellom hemmelig ransaking og kommunikasjonskontroll, altså elektronisk lagret informasjon og informasjon som var under overføring, var en svakhet tatt den teknologiske utviklingen i betraktning.[11]

Dataavlesing løser utfordringer knyttet til kryptering ved at metoden gir politiet adgang til å lese informasjonen mens den ligger åpent i et datasystem hos brukeren, før den sendes eller lagres kryptert. Metoden gir politiet tilgang til sanntidsovervåking av datasystemer. Dataavlesing gir dermed politiet tilgang til informasjon som det ikke er mulig å nå frem til gjennom reglene for kommunikasjonskontroll, ransaking og beslag. Lovproposisjonen beskriver dataavlesing som en fremgangsmåte for «skjult innhenting» av informasjon fra «informasjonssystemer» som benyttes av mistenkte.[12] Metoden innebærer at politiet gis full adgang til å kontrollere det som gjøres og registreres i et datasystem.

Både kommunikasjonskontroll og dataavlesing er politimetoder som er utformet i lys av teknologisamfunnet. Utvikling innenfor kommunikasjon- og datateknologi har gjort at kommunikasjon kan skje raskt og hurtig gjennom mobiltelefoner og datamaskiner uavhengig av avstand. Bestemmelsene om kommunikasjonskontroll og dataavlesing er verktøy som er ment å tilpasse politiets bekjempelse av kriminalitet til denne utviklingen i samfunnet.

[9] NOU 2009:15 side 241.
[10] Prop. 68 L (2015-2016) side 241.
[11] Prop. 68 L (2015-2016) side 256.
[12] Prop. 68 L (2015-2016) side 224.

1.3 Formål og avgrensning

Da oppgaven setter søkelys på forholdet mellom bestemmelsene om kommunikasjonskontroll og dataavlesing som ledd i etterforsking, vil det dermed avgrenses mot bruken av tvangsmidler i avvergende og forebyggende øyemed etter henholdsvis strpl. § 222 d og politil. § 17 d. Det avgrenses også mot ordinære tvangsmidler, fordi oppgaven tar sikte på bruken av kommunikasjonskontroll og dataavlesing med utsatt underretning. Det trekkes også en avgrensning mot ulovfestede etterforskingsmetoder, ettersom disse per dags dato ikke anses å ha et «tvangs»-element knyttet til seg, sammenlignet med for eksempel kommunikasjonskontroll og dataavlesing, selv om dette også er under diskusjon i dag.

1.4 Rettskildebildet og metode

Ved bruken av skjulte tvangsmidler er politiet bundet av konstitusjonelle og internasjonale forpliktelser. Politiet sitt bruk av kommunikasjonskontroll og dataavlesing må ligge innenfor rammene som er gitt i nasjonal og internasjonal lovgivning. I denne sammenheng er retten til privatliv i Grunnloven § 102 og EMK artikkel 8 og legalitetsprinsippet relevant for metodebruken.

Grunnlovsbestemmelsen § 102 kom i Grunnloven i 2014 og bygger på EMK artikkel 8. Grunnloven § 102 er av grunnlovsrang, mens EMK artikkel 8 er inkorporert i norsk rett gjennom Menneskerettsloven lov § 21. mai 1999 nr. 30 § 2. Grunnloven er lex superior, og vil ved motstrid gå foran lover og forskrifter siden den har høyere rang. Konvensjoner og protokoller er inkorporert på lovsnivå, og er likestilt med annen norsk lovgivning jf. menneskerettsloven § 2. Det fremkommer imidlertid av menneskerettsloven § 3 at inkorporerte konvensjoner og protokoller nevnt i § 2 går foran norsk lov ved motstrid. De inkorporerte konvensjonene har ved forrangsbestemmelsene fått en «halvkonstitusjonell» eller «semikonstitusjonell» karakter.[13]

Norge har gjennom internasjonalt samarbeid og inngåelse av traktater og konvensjoner påtatt seg en rekke forpliktelser. Det kommer frem av strpl. § 4 at straffeprosessloven gjelder med *«de begrensninger som er anerkjent i folkeretten eller som følger av overenskomst med fremmed stat»*. Gjennom EMK artikkel 1 har Norge forpliktet seg til å «respektere» og «sikre» konvensjonsrettigheter. Ansvaret innebærer både en negativ og en positiv forpliktelse for staten. Den negative forpliktelsen innebærer at staten forplikter seg til å avstå fra inngrep i borgernes konvensjonsrettigheter, mens den positive forpliktelsen går ut på at staten må gi

[13] Skoghøy (2002) side 340.

konvensjonsrettigheter en effektiv beskyttelse. Dette forutsetter en aktiv oppfølging i forvaltnings- og rettspraksis, særlig ved etterforskning og eventuell iretteføring av forhold som menes å krenke noens konvensjonsrettigheter.[14] Dersom konvensjonsrettighetene skal ha en reell og effektiv beskyttelse, betyr det at staten må etterforske disse, om nødvendig også bruke skjulte tvangsmidler for å avdekke konvensjonsbrudd.

I det følgende vil den alminnelige rettskildelæren, den juridiske metoden, benyttes som fremgangsmåte for tolkning og fastsettelse av innholdet i lovbestemmelsene om kommunikasjonskontroll og dataavlesing. Ved tolkning av menneskerettigheter må norske rettsanvendere ha en annen innfallsvinkel til fremgangsmåte.[15] Denne ulike tilnærmingen til rettskildene og metodespørsmål som gjelder forholdet mellom nasjonal og internasjonal rett, vil ikke bli problematisert i oppgaven. Ettersom Grunnloven § 102 er inspirert av EMK artikkel 8, er det en presumsjon for at innholdet i den norske Grunnlovsbestemmelsen er i samsvar med våre folkerettslige forpliktelser. Ved anvendelsen av EMK artikkel 8, vil EMD sin tolkning av innholdet i konvensjonen legges til grunn.

1.5 Videre fremstilling

Oppgaven vil gi en fremstilling av lovbestemmelsene om kommunikasjonskontroll og dataavlesing under etterforskning. Under overskriften «grunnleggende hensyn og retten til privatliv» i kapittel 2 fremheves relevante hensyn som får betydning i forbindelse med metodebruken. Hovedfokus i oppgaven er en analyse av likheter og forskjeller mellom bestemmelsene om kommunikasjonskontroll og dataavlesing ettersom dette er to sett med bestemmelser som har både fellestrekk og ulikheter. Denne analysen er fremstilt i kapittel 3. I kapittel 4 vil kommunikasjonskontroll og dataavlesing knyttes opp mot hensynene til personvern og rettsikkerhet og det vil vurderes hvordan de hensynene er ivaretatt av de respektive regelsettene. Avslutningsvis i kapittel 5 gis det en oppsummering av lovbestemmelsene om kommunikasjonskontroll og dataavlesing.

[14] Aall (2018) side 60.

[15] Graver (2003) side 479-480.

2 GRUNNLEGGENDE HENSYN OG RETTEN TIL PRIVATLIV

Bruken av skjulte tvangsmidler ligger i skjæringspunktet mellom hensynet til kriminalitetsbekjempelse på den ene siden, og hensynet til personvern og privatliv på den andre. Begge hensynene gjenspeiler viktige verdier i en demokratisk stat og inngår i avveiningen av om det skal besluttes iverksetting av kommunikasjonskontroll og dataavlesing.

2.1 Personvern

Etter Grunnlovsrevisjonen i 2014 er personvern og rettssikkerhetshensyn blitt tydeligere reflektert i Grunnloven.[16] Personvern er ikke et entydig begrep og kan defineres på ulike måter. Personvernkommisjonen definerer personvern som ivaretakelse av personlig integritet: ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse.[17] Helt sentralt står menneskets ukrenkelighet, krav på respekt fra andre, respekt for egen integritet og privatlivets fred.[18] Alle mennesker har krav på en «privat sfære» som de selv kontrollerer og kan handle fritt uten innblanding fra staten eller andre. Personvern reflekteres også som et ideal, ved at retten til respekt for privatlivet er en menneskerettighet etter EMK artikkel 8 og FNs konvensjon om sivile og politiske rettigheter artikkel 17.[19] Et vesentlig element av personvernet er at den enkelte skal ha kontroll over og innflytelse på bruken og delingen av personopplysninger om seg selv.[20] Regler og standard for behandling av personopplysninger som har ivaretakelse av personvern som hovedformål, kalles personopplysningsvern. [21]

Personlig integritet er en del av personvern, og omfatter friheten til å tenke og bevege seg fritt innenfor den «private sfæren». Det er et samspill mellom disse to elementene i den personlige integritet, fordi frihet fra overvåking fra offentlige myndigheter, legger til rette for fri tenking, selvrealisering og utvikling.[22] Uten rett til privatliv, mister borgerne mulighet til selvutfoldelse og rom for å reflektere og tenkte fritt, uten å bli kontrollert av andre.[23]

[16] Bruce og Haugland (2018) side 35.
[17] NOU 2009:1 side 32.
[18] Datatilsynet (2019).
[19] Prop. 68 L (2015-2016) side 20.
[20] Regjeringen (2019).
[21] NOU 2009:1 side 32.
[22] Bruce og Haugland (2018) side 23.
[23] Datatilsynet (2019).

Personvern er en betegnelse på et bredt sett med individuelle interesser, og det hensyn som er i spill, mens privatlivet er den delen av personvernet som er vernet etter Grunnloven § 102 og EMK artikkel 8.

2.2 Rettssikkerhet

Et hensyn som er nær knyttet til personvern, er hensynet til rettssikkerhet. Overordnet dreier rettsikkerhet seg om en rettsikkerhet mot overgrep og vilkårlighet fra statsmakten. En sentral del av rettsikkerhet innebærer at borgerne skal kunne forutberegne sin rettsstilling gjennom sine handlinger. Statens maktbruk må være regulert i lover. Det er også et krav om likebehandling og rettferdighet.[24] Retten til kontradiksjon, innsyn og underretning anses som sentrale prosessuelle rettssikkerhetskrav.[25] Kontradisjonsprinsippet (imøtegåelsesprinsippet) innebærer at en part skal gis mulighet til å ta til motmæle og imøtegå anklager som rettes mot vedkommende. Dette prinsippet er kommet til uttrykk blant annet i straffeprosessloven § 86 om innkalling til rettsmøter og rett til å gjøre seg kjent med sakens dokumenter i § 242.

Flere sentrale rettsikkerhetsgarantier utgår ved bruken av skjulte tvangsmidler.
Personer under skjult tvangsmiddelbruk, får status som «siktet» etter strpl. § 82 først når de blir underrettet om tvangsmiddelbruken jf. strpl. § 82 tredje ledd annet punktum. Mistenkte mister retten til dokumentinnsyn eller mulighet til kontradiksjon. Mistenkte har ikke mulighet til å motsi eller utfordre politiets grunnlag for metodebruken.

Bruken av skjulte tvangsmidler står i et spenningsforhold til rettssikkerheten til borgerne, noe som har sammenheng med at personene ikke underrettes om tvangsmiddelbruken og mister retten til kontradiksjon. Rett til offentlig oppnevnt advokat etter strpl. § 100 a er ment å veie opp for de sikkerhetsutfordringene bruken av skjulte tvangsmidler fører med seg.

2.2.1 Forholdet mellom personvern og rettsikkerhet

Begrepet rettssikkerhet og personvern har samme kjerne, å beskytte individets integritet mot overgrep.[26] Rettssikkerhet regulerer imidlertid forholdet mellom staten og individene, mens personvern også verner om private aktørers virksomhet.[27] Videre er det vanlig å avgrense

[24] Bruce og Haugland (2018) side 26.
[25] Prop. 68 L (2015-2016) side 21.
[26] NOU 2009:1 side 33.
[27] NOU 2009:1 side 33.

personvern til de regler som har som formål å beskytte den psykiske integriteten. Rettssikkerhet derimot gjelder i større grad fysisk integritet.[28]

2.3 Kriminalitetsbekjempelse

Samfunnets ønske om å bekjempe kriminalitet er et kryssende hensyn og står i motstrid til hensynet til den enkeltes personvern og rettssikkerhet. Hensynet til kriminalitetsbekjempelse er selve grunnen til at politiet er gitt adgang til å anvende kommunikasjonskontroll og dataavlesing som skjulte tvangsmidler.

Det er påpekt at det i de senere årene har skjedd endringer i «kriminalitetsbilde», som har økt behovet for å anvende skjulte tvangsmidler for å bekjempe alvorlig kriminalitet. Metodeutvalget la i NOU 1997:15 til grunn at kriminaliteten hadde undergått en rekke kvalitative endringer. Miljøene var lukket, man så en økt grad av profesjonalitet og hensynsløshet i forhold til omverdenen.[29] Globalisering og internasjonalisering har lagt til rette for dannelse av kriminelle nettverk, slik at disse kunne finne sted på tvers av grenser.[30]

Samme syn ble delt av Politimetodeutvalget i NOU 2004:6 der man så at de nye trekkene ved kriminalitetsbildet skilte seg fra kriminaliteten man så tidligere. Det var bedre organisering, økt fleksibilitet hos kriminelle, større grad av samarbeid mellom ulike kriminelle nettverk, økt internasjonalisering, økt bruk av avansert teknologi og økt spesialisering og profesjonalisering samt blanding av legal og illegal virksomhet.[31] Politianalysen gitt i NOU 2013:9 tilsa at den overskridende organiserte kriminaliteten hadde gitt politiet nye utfordringer ved at den stadig bli mer kompleks, grenseoverskridende og organisert.[32] Et viktig element ved den organiserte internasjonale kriminaliteten, er at den krever sikker og rask kommunikasjon, som en forutsetning for å gjennomføre kriminelle handlinger som ulovlig innførsel og omsetning av narkotika.[33] Mulighet til å kartlegge kontakten og kommunikasjonen mellom de ulike leddene vil dermed være en forutsetning for å avdekke resten av virksomheten.[34]

Politiets verktøy for bekjempelse av kriminalitet må tilpasses dagens kriminalitetsbilde for å fungere effektivt. Dersom trusselen om kriminalitet blir for stor fordi politiet mangler

[28] NOU 2009:1 side 33.
[29] NOU 1997:15 kapittel 2 punkt 2.2.
[30] NOU 1997:15 kapittel 3 punkt 3.1.3.4.
[31] NOU 2004:6 side 163.
[32] NOU 2013:9 side 18.
[33] NOU 1997:15 kapittel 3 punkt 3.2.3.
[34] Bruce og Haugland (2018) side 65.

kapasitet og ressurser til å etterforske kriminaliteten, vil folk begynne å ta retten i sine egne hender.[35] For å imøtekomme samfunnets forventninger, må politiet benytte effektive etterforskingsmetoder, også bruke skjulte tvangsmidler når dette er nødvendig.

2.4 Internasjonale og konstitusjonelle rammer

Politiet er i kraft av sin posisjon gitt en viss handlefrihet for å imøtekomme lovpålagte plikter. Politiets handlefrihet er imidlertid begrenset til tiltak i forebyggende arbeid og omfatter ikke «inngrep» som gjøres i borgernes rettsfære. Skal politiet gjøre inngrep i borgernes rettsfære, må disse oppfylle kriteriene i nasjonal og internasjonal rett.

Den retten som har størst betydning for skjult tvangsmiddelbruk er retten til respekt for privatliv som i dag er vernet gjennom Grunnloven § 102 og EMK artikkel 8, og det generelle legalitetskravet i Grunnloven § 113. Legalitetsprinsippet i Grunnloven § 113 innebærer at myndighetens inngrep overfor den enkelte må ha grunnlag i lov og fungerer som en skranke for politiets handlemåter.

2.4.1 Grunnloven § 102 og EMK artikkel 8

Etter EMK artikkel 8 har enhver «rett til respekt for sitt privatliv, familieliv, sitt hjem og sin korrespondanse». Retten til privatliv i Grunnloven § 102 bygger på EMK artikkel 8.

Privatliv kan beskrives som en sfære hvor individet kan motsette seg at andre, enten private eller offentlige myndigheter, griper inn uten samtykke.[36] Begrepet privatliv gir et vern av den fysiske og psykiske integritet.[37]

EMK artikkel 8 verner også om retten til «familieliv». Videre gir EMK artikkel 8 et vern om inngrep i eget «hjem». EMD har tolket «hjem» vidt i praksis og i saken Chappell mot Storbritannia er det slått fast at også kontorlokaler kan omfattes.[38] Dette er begrunnet med at grensen mellom privatliv og hjem, og yrkesliv ikke er skarp i moderne samfunn.

Videre gir EMK artikkel 8 beskyttelse mot inngrep i retten til «korrespondanse».

[35] Prop. 68 L (2015-2016) side 21.
[36] Aall (2018) side 215.
[37] HR- 2013- 00881-A avsnitt 34.
[38] Aall (2018) side 251.

Begrepet «korrespondanse» dreier seg om kommunikasjon, typisk ved hjelp av telefon, brev eller e-post.[39] Begrepet «kommunikasjon» sikter til informasjonsutveksling uavhengig av form eller innhold.[40] Korrespondanse dekker dermed alle former for utveksling av informasjon. Det fremgår av EMDs praksis at privatlivsbegrepet er tolket vidt i praksis og er ment å konsumere de tre andre begrepene, «familieliv, hjem og korrespondanse».[41]

2.4.1.1 *EMK artikkel 8. annet ledd*

Etter EMDs praksis er det oppstilt tre hovedvilkår for inngrep i retten til privatliv. Det skal ikke skje inngrep fra offentlige myndigheter i retten til privatliv med mindre inngrepet har hjemmel i lov, forfølger et legitimt formål og er nødvendig i et demokratisk samfunn.

2.4.1.1.1 Lovkravet

Myndighetenes inngrep i retten til privatliv må ha hjemmel i lov. Begrunnelsen for et lovkrav ligger i hensynet til forutberegnelighet og rettsikkerhet mot vilkårlig maktmisbruk fra statsmyndighetene. Lovkravet er særlig antatt å ha betydning for bestemmelser på strafferettens område.[42]

For nasjonal del følger lovkravet av Grunnloven § 113. Slik hjemmel i nasjonal rett kan være Grunnloven, lover og eller forskrifter. Norsk rett er strengere på dette punktet enn EMD, ettersom EMD godtar ulovfestet rett, internasjonal rett og alminnelige rettsprinsipper.[43] EMD likestiller ulovfestet rett med formell lov under forutsetning av at visse kvalitetskrav til forutberegnelighet er oppfylt.[44]

Ved skjult tvangsmiddelbruk stiller EMD strenge krav til kvaliteten av lovbestemmelser. Det påpekes at risikoen for vilkårlighet er særlig stor, når den utøvende makt utøves i det skjulte.[45] EMD uttalte i R.E mot Storbritannia at tiltaket må ha grunnlag i den interne loven og loven må være presist formulert slik at borgeren kan forutsette konsekvensene.[46]
EMD har likevel i flere saker uttalt at kravet til forutberegnelighet i relasjon til hemmelig overvåking ikke kan praktiseres på en måte som gjør borgerne i stand til å forutse akkurat når myndighetene vil overvåke kommunikasjonen deres.[47]

---

[39] Aall (2018) side 252.
[40] Ot.prp. nr. 74 (1998-1999) side 156.
[41] Aall (2018) side 252.
[42] Aall (2018) side 116.
[43] Aall (2018) side 145.
[44] Aall (2018) side 124.
[45] Malone v. United Kingdom (1984) avsnitt 67.
[46] R.E v. United Kingdom avsnitt 120.
[47] Big Brother Watch and others. v. United Kingdom (2018) avsnitt 306 og Malone v. United Kingdom (1984) avsnitt 67.

2.4.1.1.2 Formålskravet og forholdsmessighetskravet

Videre må inngrepet være nødvendig i et demokratisk samfunn i lys av hensynet til "nasjonal sikkerhet, offentlig trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter" Formålene som er opplistet i EMK artikkel 8 er formulert åpent og bredt, for å gi statene fleksibilitet i forhold til når det kan foretas inngrep.

EMD har presisert at innblandingen må svare til «et pressende sosialt behov», den må være i «proporsjonal med det legitime mål som ble forfulgt» og om de begrunnelser de nasjonale myndighetene har gitt for å begrunne den er «relevante og tilstrekkelig».[48]

Nødvendighetskravet innebærer at inngrepet må ta sikte på å realisere et legitimt formål. Videre innebærer kravet at midlene som brukes er «egnet» til å ivareta formål nevnt i EMK art. 8 nr. 2. Inngrepet må være nødvendig, slik at myndighetene ikke kan benytte seg av mindre inngripende midler for å oppnå formålet. Tiltaket som brukes må videre stå i forhold til det legitime målet som forfølges.[49]

EMD er tilbakeholden med å foreta en inngående prøving av inngrepets egnethet eller effektivitet i saker om kommunikasjonskontroll eller innhenting av personlige opplysninger.[50]

Til tross for at statene er gitt en vid skjønnsmargin, stiller EMD strenge prosessuelle krav til utforming av reglene og til kontroll. EMD har uttalt at det er «essential to have clear, detailed rules» ved skjult tvangsmiddelbruk.[51] Videre vektlegger EMD om staten har ordninger og varslingsmekanismer for å overvåke gjennomføringen av hemmelige overvåkingstiltak.

Det kan gjøres inngrep i borgernes privatliv dersom vilkårene i EMK artikkel 8 annet ledd er oppfylt. Vernet mot overgrep og vilkårlighet gir dermed ikke et vern mot inngrep i seg selv, det innebærer «*kun*» at inngrepet skjer innenfor de rettslige rammene for inngrepet.[52]

[48] Sunday times v. United Kingdom avsnitt 62.
[49] Gillow v. United Kingdom avsnitt 64.
[50] Bruce og Haugland (2018) s. 45
[51] Bruce og Haugland (2018) side 44.
[52] Prop. 68 L (2015-2016) side 21.

3 SAMMENLIKNING AV REGLENE OM KOMMUNIKASJONSKONTROLL OG DATAAVLESING

Dette kapitlet skal gi en analyse av bestemmelsene om kommunikasjonskontroll og bestemmelsene om dataavlesing. Hovedfokuset vil være rettet mot hva som skiller disse bestemmelsene fra hverandre. Jeg vil starte med bestemmelsene om kommunikasjonskontroll, og underveis under fremstillingen av bestemmelsene om dataavlesing påpeke forskjeller og likheter. I kapittel 3.1 redegjøres det for historikk og bakgrunn ved begge regelsettene. I kapittel 3.2 gis det en oversikt over vilkårene i bestemmelsene og beskrivelse av deres fremgangsmåter for å innhente informasjon. Mens kapittel 3.3. tar for seg de materielle vilkårene, er kapittel 3.4 rettet mot de prosesuelle vilkårene, som etter gjeldende rett kreves for å ta i bruk metodene. Kapittel 3.5 gir en fremstilling av kontrollsystemet generelt.

3.1 Historikk og bakgrunn

I dette kapitlet vil jeg forklare utviklingen av regelverket innenfor kommunikasjonskontroll og dataavlesing. Hovedfokus vil være på å gi en historisk fremstilling og fremheve begivenheter som har bidratt til utviklingen.

3.1.1 Kommunikasjonskontroll

Bestemmelsene om kommunikasjonskontroll har blitt revidert en rekke ganger og senest utvidet i 2016. Frem til 1999 var politiets adgang til telefonkontroll begrenset til etterforskingen av narkotikaforbrytelser og visse saker om rikets sikkerhet.[53] Hjemmelen for å avlytte telefonsamtaler i narkotikasaker var en midlertidig lov av 17 desember 1976 nr. 99. Hjemmelen for telefonavlytting i saker om rikets sikkerhet var lov 24.juni 1915 nr. 5 om kontroll med post- og telegrafforsendelse og med telefonsamtaler. Begge hjemlene ble senere gjort permanent og inntatt i straffeprosessloven kapittel 16 a, førstnevnte i 1992 og sistnevnte ved lovendring i 1999.[54]

[53] Bruce og Haugland (2018) side 196.

[54] Bruce og Haugland (2018) side 197.

Hensikten var først og fremst å få en felles regulering av kommunikasjonskontroll i straffeprosessloven, fordi det ville gi et oversiktlig system og skape bedre klarhet.[55] Videre var hensikten å tilpasse hjemlene til den nye utviklingen man så i kriminalitetsbildet. Metodeutvalget begrunnet telefonavlytting i narkotikasaker med at narkotika forbrytelser ble ansett som «svært alvorlige og samfunnsskadelige forbrytelser», der tradisjonelle etterforskingsmetoder ikke var tilstrekkelig. Metodeutvalget mente at det samme måtte gjelde i dag for andre typer kriminalitet, og underbygget dette med at samfunnsforholdene og kriminalitetsbildet hadde endret seg. Kriminelle hadde blitt mer profesjonelle og opererte på tvers av grenser samt miljøene var lukket.[56]

Departementet mente at anvendelsesområdet for telefonavlytting bare burde utvides dersom det var «forsvarlig» i forhold til hensynene til personvern og rettssikkerhet.[57] Etter departementets syn var telefonavlytting aktuelt ved etterforskingen av den mest alvorlige kriminaliteten, der andre etterforskingsmetoder ikke var tilstrekkelig. Dette ser man gjennom videreføringen av tilleggsvilkåret om at avlyttingen må være av «vesentlig betydning for å oppklare saken» og at «oppklaring ellers i vesentlig grad vil bli vanskeliggjort». Sistnevnte indikerer at telefonavlytting skal benyttes kun når kriminaliteten vanskelig kan avklares ved åpen etterforskning. Departementet fant det forsvarlig å utvide anvendelsesområdet for telefonavlytting fordi hensynet til bekjempelse av alvorlig kriminalitet veide tungt.

I 2005 ble regelverket på nytt endret. Den største endringen var at det ble åpnet for bruk av romavlytting som etterforskingsmetode, samt for bruk av tvangsmidler i avvergende og forebyggende øyemed.[58] Dette gir politiet adgang til å anvende tvangsmidler for å avverge nært forstående lovbrudd eller som ledd i sitt forebyggende arbeid. Innføringen av tvangsmidler i forebyggende øyemed var en utvidelse av anvendelsesområdet til bruken av tvangsmidler, fordi politiet nå fikk adgang til å bruke skjulte etterforskingsmetoder også utenfor en «etterforskning». Det betyr at tvangsmidlene anvendes på et stadium der det enda ikke er grunn til å undersøke om det foreligger et straffbart forhold jf. strpl. § 224.
Politiet fikk videre adgang til å identifisere mobiltelefoner og andre kommunikasjonsanlegg ved hjelp av teknisk utstyr. Samtidig ble det gjort små endringer i reglene om hemmelig ransaking, kommunikasjonskontroll, teknisk sporing, utleveringspålegg fremover i tid og avlytting av samtaler med samtykke fra en av samtalepartene.[59]

[55] Ot.prp. nr. 64 (1998-1999) side 41.
[56] Ot.prp. nr. 64 (1998-1999) side 42.
[57] Ot.prp. nr. 64 (1998-1999) side 46.
[58] Bruce og Haugland (2018) side 197.
[59] Bruce og Haugland (2018) side 19.

3.1.1.1 Metodekontrollutvalget

Metodekontrollutvalget ønsket å åpne for bruk av kommunikasjonsavlytting i flere saker enn gjeldende rett på det tidspunktet. Det ble vist til at visse kriminalitetsformer representerer en etterforskningsmessig utfordring, der det er «nødvendig» å tillate ekstraordinære metoder selv om strafferammekravet ikke er oppfylt.[60] Av forslaget fremgår det at anvendelsesområdet for kommunikasjonsavlytting etter § 216 a bokstav b ble utvidet til å omfatte etterforskning av saker om offentlig oppfordring, rekruttering eller opplæring til terrorhandlinger, befatning med overgrepsbilder av barn, frihetsberøvelse, menneskehandel og grov menneskesmugling.[61] Disse er i dag angitt i § 216 a første ledd, alternativ b.

I § 216 b annet ledd bokstav c ble det foreslått en presisering av at kommunikasjonskontroll etter § 216 b kan gå ut på å bruke teknisk utstyr for å lokalisere et kommunikasjonsanlegg. I annet ledd bokstav d, ble det foreslått et tillegg om at politiet kan innhente opplysninger om den geografiske plasseringen til et bestemt kommunikasjonsanlegg, uavhengig om anlegget er i bruk til kommunikasjon.[62] Videre fikk man ny bokstav e som gir politiet anledning til å overføre signaler i hemmelighet til et bestemt kommunikasjonsanlegg, for å effektivisere tiltak som nevnt i bokstav c og d.[63]

I NOU 2016:24 ble det fremmet forslag til ny straffeprosesslov. Her ble det ikke foreslått omfattende endringer i reglene om skjulte tvangsmidler med begrunnelse at dette regelverket vi har i dag er et resultat av omfattende lovarbeid og politiske kompromisser gjennom årene.[64] Det ble imidlertid foreslått en omstrukturering og forenkling av tvangsmiddelregelverket generelt, herunder justering av terskelen for ulike typer inngrep, samt lovfesting av enkelte av ulovfestede politimetoder (spaning, infiltrasjon og provokasjon).[65] Straffeprosesslovutvalgets forslag om ny straffeprosesslov er foreløpig ikke fulgt opp.

[60] Prop. 68 L (2015-2016) side 94.
[61] Prop. 68 L (2015-2016) kapittel 16.1 til endringene i § 216 a.
[62] Prop. 68 L (2015-2016) kapittel 16.1 til endringene i § 216 b.
[63] Prop. 68 L (2015-2016) side 282.
[64] NOU 2016:24 side 298.
[65] Bruce og Haugland (2018) side 19-20.

3.1.2 Dataavlesing

I 2016 ble dataavlesing foreslått som et nytt skjult tvangsmiddel.[66] Proposisjonen bygget på Metodekontrollutvalgets evaluering av politiets bruk av skjulte tvangsmidler i NOU 2009:15 Skjult informasjon–åpen kontroll. Politiet hadde behov for tilgang til lagret og kommunisert informasjon som var kryptert. Det ble vist til økning i bruk av krypteringsløsninger hos kriminelle.[67] Informasjonsbeskyttelsen tilbys ofte som «standardløsning», og er ikke alene forbeholdt profesjonelle.[68]

Denne problemstillingen ble også drøftet av Metodeutvalget i NOU fra 1997:15 om kriminalitetsutviklingen. Der ble det påpekt at moderne teknologi og etterfølgende krypteringsløsninger har gjort det enkelt for kriminelle å skjule sin kommunikasjon for politiet. Krypteringsprogrammer ble ansett å være offentlig tilgjengelig for allmennheten, der alle kunne få tak i disse. Videre påpekes det at kryptering av en datamaskin er en enkel prosess i dag, der krypteringen skjer enkelt ved inntasting av kodeord.[69]

3.1.2.1 Omstridt lovforslag

Det har vært mange synspunkter på innføringen av dataavlesing om politimetode. Metodekontrollutvalget har særlig pekt på at dataavlesing vil utgjøre et svært kraftig inngrep i enkeltmenneskers personvern.[70] Dette ble begrunnet med at fremgangsmåten vil kunne gi politiet tilgang til innholdet *i* et datasystem, og ikke bare opplysninger *om* bruken av det. Videre vil bruken kunne medføre inngrep i andre enn mistenktes personvern, dersom et datasystem for eksempel brukes av flere.

Lund-utvalget har i sin utredning NOU 2003:18 om Rikets sikkerhet berørt personvern- og rettssikkerhetsspørsmål i sin vurdering av hvorvidt det bør benyttes spesielle datatekniske metoder i etterforskingen, såkalte trojanske hester, ormer, sniffere mv.[71] Metodenreiste tekniske og rettssikkerhets spørsmål som etter deres syn lå i kjerneområdet for Datakrimutvalget til å utrede nærmere.[72]

---

[66] Prop. 68 L (2015-2016) side 12.
[67] Prop. 68 L (2015-2016) side 12.
[68] Prop. 68 L (2015-2016) side 12.
[69] NOU 1997:15 kapittel 3 punkt 3.2.4.
[70] Prop. 68 L (2015-2016) side 243.
[71] NOU 2003:18 side 126-127.
[72] NOU 2003: 18 side 127

I NOU 2004:6 Mellom effektivitet og personvern foreslo Politimetodeutvalgets flertall å innføre regler som tillater dataavlesing som forebyggende metode.[73] Dataavlesing skulle defineres slik i loven «*Med dataavlesing forstås avlesing av opplysninger i et ikke offentlig tilgjengelig elektronisk informasjonssystem ved hjelp av programmer eller på annen måte*».[74] Det ble vist til at tilgang til krypteringsprogrammer ga politiet mindre informasjon enn tidligere. Videre påpekes det at krypteringsprogrammer er så kompliserte at meldingene ikke lot seg dekryptere og at eneste alternativ til å få tak i innholdet, var å gi politiet tilgang til avlesing før meldingen krypteres. Departementet anså dataavlesing som en svært integritetskrenkende metode og mente det var behov for å utrede metoden nærmere. Det ble vist til at man måtte gå inn på kompliserte teknologiske spørsmål for å kunne avveie de ulike hensyn på området på en tilfredsstillende måte.[75]

Dette foranlediget departementet til å be om en utredning av Datakrimutvalget. Datakrimutvalget mente at dataavlesing var et begrep uten entydig fastlagt innhold og det måtte utredes nærmere hva metoden besto i.[76] Dette arbeidet ble satt på vent, og senere fikk Metodekontrollutvalget i sitt mandat å vurdere dataavlesing i sammenheng med andre metodespørsmål. Dette viser at spørsmålet har vært løftet opp gjennom årene, av forskjellige utvalg og i ulike sammenhenger, uten at man har klart å bli enig om innføringen av metoden og i så fall hvordan.

3.1.2.2 Selvstendig etterforskingsmetode eller teknologisk tilpasning?

Metodekontrollutvalget sin oppfatning i evalueringen i NOU 2009:15 var at innføring av nye tvangsmidler eller utvidelse av eksisterende hjemler, måtte bygge på solid dokumentasjon av behovet.[77] Ved innføringen av dataavlesing som metode måtte det påvises et behov for metoden samt at metoden skulle være egnet til å tilfredsstille behovet på en effektiv måte.[78] Videre var det også usikkerhet rundt om dataavlesing skulle bli innført som en selvstendig etterforskingsmetode, eller som en teknologisk tilpasning for å videreføre eksisterende politimetoder.[79] Metodekontrollutvalget foreslo en løsning der dataavlesing skulle tillates som ledd i gjennomføringen av de eksisterende metodene kommunikasjonskontroll og hemmelig ransaking, men ikke som selvstendig metode i form av sanntidsovervåking av et datasystem.

[73] NOU 2009:15 side 235.
[74] NOU 2009:15 side 235.
[75] Ot.prp. nr. 60 (2004-2005) side 141.
[76] NOU 2009:15 side 235.
[77] NOU 2009:15 side 240.
[78] NOU 2009:15 side 240.
[79] NOU 2009:15 side 237.

Ved kommunikasjonsavlytting samler politiet inn materielle fra avlyttingen i transportfasen mellom avsender og mottaker, normalt hos en tele- eller internettilbyder.[80] Den teknologiske utviklingen har gjort det mulig for kriminelle å sørge for at innholdet ikke lenger vil være forståelig eller leselig når den når teletilbyderen. Krypteringsprogrammer «lukker» informasjonen når den overføres eller lagres, eller ved automatisk kryptering som tjenesteleverandøren har implementert.[81] Programmene kan sørge for at en e-post som hos avsenderen og mottakeren kan leses, vil fremstå kryptert og uleselig for politiet. For å oppnå tilgang måtte politiet enten knekke krypteringen eller ha krypteringsnøkkelen. Dette er imidlertid en tungvint fremgangsmåte å lene seg på, fordi krypteringsprogrammer i dag i forbindelse med kommunikasjon er så avanserte at kryptering ikke kan omgås.[82] Politiet møtte på tilsvarende utfordringer ved bruk av tvangsmidler som hemmelig ransaking og beslag, når informasjonen var «kryptert» eller passord beskyttet.[83]

Metodekontrollutvalget mente at begge hovedutfordringene- kryptering og annen beskyttelse- ved eksisterende metoder, kunne møtes effektivt dersom politiet gis adgang til dataavlesing.[84] Dataavlesing kunne muliggjøre kommunikasjonsavlytting, ved å gi politiet adgang til å avlytte kommunikasjonen før den blir kryptert eller skaffe seg krypteringsnøkkelen på mistenktes datamaskin, som senere kan brukes til å dekryptere meldingen i transportfasen.[85] Alternativt kunne dataavlesing innføres som en metode i forbindelse med hemmelig ransaking og beslag. Det kunne tenkes at man gjennom dataavlesing ville få avlesing av mistenkte inntasting av passord, og dermed lettere få tilgang til den aktuelle informasjonen på maskinen, i programmer eller i dokumenter ved ransaking og beslag.[86] Det var forutsatt at ransakinger nå kunne skje digitalt, noe som gjør det enklere med fortsatt og gjentatt ransaking og beslag.

Det var ikke adgang til gjentatt eller fortløpende ransaking, fordi enhver ransaking krevde rettens tillatelse.[87] Metodekontrollutvalget mente at det ellers ville innebære en utvidelse av dagens adgang til hemmelig ransaking dersom det ble gitt tillatelse til gjentatt ransaking på generelt grunnlag. Skulle det åpnes for fortløpende ransaking på generelt grunnlag, «vil adgangen i praksis innebære at dataavlesing innføres som en selvstendig metode hvor politiet gis

[80] NOU 2009:15 side 241.
[81] Prop. 68 L (2015-2016) side 259.
[82] NOU 2009:15 side 241.
[83] NOU 2009:15 side 241.
[84] NOU 2009:15 side 241.
[85] Prop. 68 L (2015-2016) side 241.
[86] Prop. 68 L (2015-2016) side 241.
[87] NOU 2009:15 side 246.

adgang til å kontinuerlig overvåke et datasystem og registrere enhver endring bruken gjør».[88] I sin utredning lander Metodekontrollutvalget på at de ikke har funnet «dokumentert tilstrekkelig behov for å innføre dataavlesing som nytt selvstendig metode».[89]

Departementet var enig i at eksisterende skjulte tvangsmidler hadde tapt sin effekt.[90] Videre vises det til et særlig trekk ved utviklingen innen elektronisk kommunikasjon. Det benyttes i større grad kommunikasjonstjenester som ikke er bundet av et bestemt kommunikasjonsanlegg eller nettverksforbindelse, men derimot «virtuell» brukerkonto med brukernavn og passord som benyttes fra ulike plattformer.[91] Dette er en utfordring når man ser på bruken av e-post og fildelingstjenester som kan brukes av flere, med tilgang til brukerkontoen, til å dele og redigere informasjon. De med tilgang kan lese og redigere informasjonen som lagres på tjenestetilbydernes servere, uten at informasjonen utveksles mellom ulike kommunikasjonsanlegg.[92] «Et kjent eksempel» er når kriminelle fra hver sine kommunikasjonsanlegg logger seg på samme e-postkonto for å utveksle informasjon.[93] Det blir påpekt at kommunikasjonskontroll ikke gir politiet en «oversikt» over informasjonen som sendes, fordi politiet kun har anledning til å avlytte et bestemt kommunikasjonsanlegg, for eksempel en datamaskin eller avlytting via en nettverkforbindelse.

Departementet vurderte disse nye trekkene ved elektronisk kommunikasjon i lys av reglene om ransaking og beslag. Det påpekes at ransakinger forutsettes å gjennomføres som enkeltstående handlinger. Det gir ikke adgang til å overvåke «ransakingsobjektet» over tid, og for eksempel forbli pålogget på e-post konto, for å fange opp informasjon fortløpende.[94] Ransakingstillatelser vil dermed bare gi «øyeblikksbilder» og ikke en full oversikt over informasjonsutvekslingen. Da er det tilfeldigheter som avgjør om politiet får tak i nyttig og betydningsfull informasjon.

Departementet var av den oppfatning at politiet bør gis adgang til å benytte dataavlesing i videre utstrekning enn det Metodekontrollutvalget foreslo.[95] På bakgrunn av dette mente departementet at dataavlesing heller bør innføres som et selvstendig tvangsmiddel.

[88] NOU 2009:15 side 246.
[89] NOU 2009:15 side 244.
[90] Prop. 68 L (2015-2016) side 259-260.
[91] Prop. 68 L (2015-2016) side 260.
[92] Prop. 68 L (2015-2016) side 260.
[93] Prop. 68 L (2015-2016) side 260.
[94] Prop. 68 L (2015-2016) side 261.
[95] Prop. 68 L (2015-2016) side 264.

3.2 Selve fremgangsmåten

I det følgende gis det en fremstilling av bestemmelsene om kommunikasjonskontroll og dataavlesing. Dette kapitlet skal beskrive de teknologiske fremgangsmåtene å innhente informasjon på ved begge regelsettene. Jeg starter med fremstilling av bestemmelsene om kommunikasjonskontroll og behandler dataavlesing deretter.

3.2.1 Kommunikasjonsavlytting

Hemmelig avlytting eller opptak av telefonsamtaler er straffbart etter straffeloven § 205 første ledd bokstav a. Det betyr at politiets telefonavlytting under etterforskning er ulovlig, med mindre det foreligger hjemmel som gir fullmakt til dette. Slik hjemmel for dette er i dag strpl. § 216 a.

Straffeprosessloven § 216 a regulerer telefonavlytting og avlytting av kommunikasjon mellom datamaskiner eller andre kommunikasjonsanlegg. Strpl. § 216 a tredje ledd angir nærmere hva kommunikasjonsavlyttingen kan bestå i. Det åpnes for det første for avlytting, opptak/lagring av samtaler eller annen kommunikasjon til og fra bestemte telefoner, datamaskiner eller andre anlegg for elektronisk kommunikasjon som den mistenkte besitter eller kan antas å ville bruke.

3.2.1.1 Kommunikasjon mellom kommunikasjonsanlegg

Med «kommunikasjon» menes overføing av informasjon fra en avsender til mottaker.[96] Forarbeidene nevner at avlyttingsadgangen retter seg mot all informasjonsutveksling mellom kommunikasjonsanlegg, uavhengig av form eller innhold informasjonen måtte ha. Overføring av tekst, bilde og film er også antatt å omfattes, selv om ordlyden «avlytting» i den henseende kan virke misvisende.[97]

Det ligger i ordlyden i lovbestemmelsen at adgangen er begrenset til avlytting eller annen kommunikasjon mellom «kommunikasjonsanlegg». Kommunikasjonsanlegg er bredt og kan dekke telefon, datamaskin eller nettbrett.[98]

Det er videre krav om at kommunikasjonsanlegget som ønskes avlyttet identifiseres. Rettens tillatelse må gjelde et bestemt kommunikasjonsanlegg.[99] Mobiltelefoner kan identifiseres gjennom telefonnumre eller et enkelt IMEI-nummer som svarer til serienummeret på

[96] Ot.prp. nr. 74 (1998-1999) side 156.
[97] Ot.prp. nr. 74 (1998-1999) side 156.
[98] Ot.prp. nr. 74 (1998-1999) side 157.
[99] Ot.prp. nr. 64 (1998-1999) side 157.

mobiltelefonen, eller et IMSI-nummer som er unikt for telefonens SIM-kort.[100] Avlyttingen kan knyttes til en eller flere av disse identitetene. Avlytting som er knyttet til IMEI og eller IMSI-nummeret vil bare fange opp informasjon som skjer over dette telenettet, og ikke andre trådløse nettverk vedkommende kobler seg på.[101]

Kravet om identifikasjon innebærer også at kommunikasjonskontrollen ikke kan knyttes til en person generelt, for eksempel alle anlegg det antas vedkommende vil bruke. Dette er gjeldende rett i norsk, svensk og finsk rett. Dansk rett er mer liberalt og tillater dette i forbrytelser mot statens selvstendighet og sikkerhet, mot statsforfatningen og de øverste statsmyndigheter og i terrorsaker.[102] Metodekontrollutvalget vurderte om det bør gis tillatelse til kommunikasjonskontroll knyttet til en person generelt, men mente at dette ville i stor grad legge opp til en kontrollordning hos advokaten, og bort fra dommeren. Hensynet til rettslig kontroll med politiets bruk av kommunikasjonskontroll måtte veie tyngre enn politiets ressurshensyn.[103]

3.2.1.2 Kun anledning til å avlytte signalstrømmer

En naturlig tolkning av ordlyden «til og fra» kommunikasjonsanlegg tilsier at avlytting bare kan skje mens samtalen pågår eller passerer gjennom et kommunikasjonsanlegg. Dette har også støtte i forarbeidene der det nevnes at det bare er «signalstrømmen mellom to kommunikasjonsanlegg som kan avlyttes».[104] Denne avgrensningen innebærer at kommunikasjonsavlytting må foregår i «transportfasen», når informasjonen er under overføring fra avsenderanlegget til mottakeranlegget.[105] Det dermed utelukket å avlytte informasjon som allerede er sendt og finnes lagret i for eksempel et kommunikasjonsanlegg. Ønsker politiet å avlytte kommunikasjon som er sendt og allerede lagret, må de benytte seg av andre inngrepshjemler, for eksempel reglene om ransaking og beslag.

Det er videre adgang til å avlytte anlegg som «mistenkte besitter» eller «kan antas å ville bruke». Det avgjørende er ikke eierskap, men besittelse eller bruk. Anlegg som mistenkte antas å ville kommunisere med, omfattes ikke.[106]

[100] Bruce og Haugland (2018) s. 200
[101] Bruce og Haugland (2018) s. 201
[102] Bruce og Haugland (2018) side 203.
[103] NOU 2009:15 side 198.
[104] Ot.prp. nr. 64 (1998- 1999) side 156.
[105] Prp. 68 L (2015-2016) side 226.
[106] Bruce og Haugland (2018) side 202.

3.2.1.3 Temporær masseavlytting etter strpl. § 216 a

Som kommunikasjonsavlytting regnes også *identifisering av kommunikasjonsanlegg* ved hjelp av teknisk utstyr, der dette skjer ved å avlytte samtaler eller annen kommunikasjon jf. strpl. § 216 a tredje ledd annet punktum. Dersom identifisering kan skje *uten* at kommunikasjonen avlyttes, kan det hjemles i straffeprosessloven § 216 b annet ledd bokstav c.[107] Metoden kalles «temporær masseavlytting», der politiet i en periode ved hjelp av teknisk utstyr avlytter all kommunikasjon innenfor en avgrenset området, som antas at mistenke vil befinne seg.[108] Formålet er å finne identiteten, for eksempel IMEI- eller IMIS-nummeret til et kommunikasjonsanlegg som mistenkte besitter.[109] I disse tilfellene er det gjort unntak fra kravet om identifisering av kommunikasjonsanlegg i rettens kjennelse for å få rettens tillatelse.[110]

Temporær avlytting etter § 216 a tredje ledd annet punktum har som formål å identifisere et kommunikasjonsanlegg i forbindelse med begjæring om kommunikasjonsavlytting.[111] Politiet kan benytte fremgangsmåten foreskrevet for å identifisere et medium/tjeneste de ønsker å kontrollere. En tillatelse fra retten til å identifisere kommunikasjonsanlegg gir ikke videre automatisk grunnlag for å foreta avlytting av kommunikasjonsanlegg.[112] Det må innhentes egen tillatelse for avlyttingen.

Ettersom temporær masseavlytting kan fange opp samtaler fra utenforstående som befinner seg i området, har lovgiver bestemt at det må gjelde et tilleggskrav ved slik avlytting. Etter strpl. § 216 c annet ledd kreves det at «særskilte grunner» tilsier slik avlytting.

Avlyttingsadgangen etter § 216 a gjelder uavhengig av hvem som er eier eller tilbyder av nett eller tjeneste som brukes ved kommunikasjonen jf. § 216 a fjerde ledd første punktum. For å kunne avlytte samtaler etter strpl. §216 a må politiet henvende seg til en teletilbyder for å få adgang til avlytting. Politiet får tak i dataene ved at det sendes kopi av datapakkene til politiet når disse passerer tilbyderens servere.[113] Etter § 216 a fjerde ledd annet punktum plikter eier eller tilbyder å gi politiet nødvendig bistand ved gjennomføringen av avlyttingen.

[107] Bruce og Haugland (2018) side 203.
[108] Bruce og Haugland (2018) side 203-204.
[109] Bruce og Haugland (2018) side 204.
[110] Ot.prp. nr. 60 (2004-2005) side 144-145.
[111] Bruce og Haugland (2018) side 204.
[112] Ot.prp. nr. 60 (2004-2005) side 145.
[113] Prop. 68 L (2015-2016) side 226.

3.2.2 Andre former for kommunikasjonskontroll

Politiet kan også foreta andre former for kontroll av kommunikasjonsanlegg enn kommunikasjonsavlytting. Etter straffeprosessloven § 216 b tredje ledd kan kontrollen gå ut på å innhente informasjon om kommunikasjonen (trafikkdata), innstill og stenge samtaler samt identifisere og lokalisere kommunikasjonsanlegg.

3.2.2.1 Kontroll av kommunikasjonsanlegg

Etter strpl. § 216 a retter avlyttingsadgangen seg mot innholdet i kommunikasjonen. Motsetningsvis gir straffeprosessloven § 216 b kun tilgang til opplysninger *om* kommunikasjonen. Som «kommunikasjonsanlegg» regnes samme anlegg som etter straffeprosessloven 216 a.[114] Kravet om identifikasjon av kommunikasjonsanlegget gjelder i utgangspunktet etter § 216 b også.[115]

Bokstav a til e i 216 b annet ledd angir hva kontrollen kan gå ut på.
Etter bokstav a kan politiet «innstille eller avbryte» kommunikasjon til eller fra bestemte anlegg mistenkte besitter eller antas å ville bruke. Bokstav b åpner for å «stenge anlegg for kommunikasjon» og antas å være aktuell under aksjoner der politiet vil hindre kontakt mellom flere mistenkte.[116] Bokstav e gir blant annet hjemmel for bruk av «stille» SMS. Signalene som frembringes ved overføringen kan nyttiggjøres ved å begjære basestasjonsopplysninger utlevert fra nett- eller tjenestetilbyder.[117]

3.2.2.2 Identifisering og lokalisering av anlegg

Etter bokstav c har politiet adgang til «å identifisere eller lokalisere anlegg som nevnt i bokstav a ved hjelp av teknisk utstyr». Det er samme formål som med identifisering av kommunikasjonsanlegg i strpl. 216 a tredje ledd annet punktum. Ettersom fremgangsmåten retter seg mot å innhente informasjon *om* kommunikasjonen, og ikke innholdet i kommunikasjonsstrømmen mellom anleggene, er metoden ikke underlagt vilkåret om «særlige grunner» slik det kreves for avlytting etter straffeprosessloven § 216 a tredje ledd annet punktum jf. § 216 c tredje ledd. [118]

---

[114] Bruce og Haugland (2018) side 206-207.
[115] Ot.prp. nr. 64 (1998-1999) side 159.
[116] Bruce og Haugland (2018) side 206 jf. NOU 2004:6 side 75.
[117] Prop. 68 L (2015-2016) side 282.
[118] Bruce og Haugland (2018) side 207.

Her gjelder heller ikke kravet om identifisering av det aktuelle anlegget i rettens kjennelse. Henvisningen til bokstav a, innebærer at det er en forutsetning at lokaliseringen gjelder kommunikasjonsanlegg som den «mistenkte besitter» eller «antas å ville bruke».[119]

Bokstav c gir videre adgang for kommunikasjonskontroll med formål å *lokalisere kommunikasjonsanlegg*. Endringen i loven kom i 17.juni 2016 nr. 54, på bakgrunn av Høyesteretts ankeutvalgs kjennelse i Rt.2009 s. 394.[120] Ankeutvalget konkluderte med at bestemmelsen bare ga adgang til kommunikasjonskontroll med sikte på å identifisere kommunikasjonsanlegg, og ikke for å identifisere person som bruker anlegget. Å identifisere en mistenkt og deretter vedkommende sin adresse, var ikke dekket av ordlyden i § 216 b andre ledd bokstav c.[121] Det ble her understreket at kravet til klar lovhjemmel står sterkt, etter både det generelle legalitetsprinsippet og ut fra lovskravet i EMK artikkel 8.

Identifisering og lokalisering etter bokstav c må skje ved hjelp av «teknisk utstyr». Det kan blant annet brukes mobile GSM- identifiseringssystem (såkalte IMSI-catchere) som fungerer som en mobil basestasjon som henter inn kortnummer (IMSI) og apparatnummer (IMEI) for mobilanlegg som befinner seg innenfor dens dekningsradius. [122] Det kan ikke benyttes ulike programvarer for å lokalisere kommunikasjonsanlegg.[123] Identifisering og lokalisering av kommunikasjonsanlegg må skje ved hjelp av teknisk utstyr som politiet benytter. I kjennelsen Rt. 2010 s. 1232 konstaterte Høyesteretts ankeutvalg at straffeprosessloven § 216 b annet ledd bokstav c ikke gir hjemmel for å innhente lagrede samtaledata fra tilbydernes basestasjon for å identifisere mistenktes telefon. Det ble uttalt at bestemmelsen kun gir hjemmel for situasjoner der politiet bruker eget teknisk utstyr til å identifisere og lokalisere anlegg.

3.2.2.3 Innhenting av trafikkdata

Etter strpl. § 216 b annet ledd bokstav d har eier eller tilbyder plikt å gi politiet opplysninger om trafikkdata. Trafikkdata er definert som opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom har vært satt i forbindelse med et annet bestemt kommunikasjonsanlegg. Eksempel teleselskapenes registreringer av samtaler til og fra en telefon.[124] Videre omfatter dette «andre trafikkdata knyttet til kommunikasjonen», som for eksempel samtalens

[119] Prop. 68 L (2015-2016) side 281.
[120] Bruce og Haugland (2018) side 208.
[121] Rt.2009 s. 394 side 3.
[122] Bruce og Haugland (2018) side 206.
[123] Prop. 68 L (2015-2016) side 130.
[124] Ot.prp. nr. 64 (1998-1999) side 159.

varighet, geografisk plassering eller pålogget person på datamaskin mens den var i bruk under kommunikasjonen.[125]

Her gjelder krav om å identifisere kommunikasjonsanlegget i rettens kjennelse, og alternativ d gir ikke adgang til å innhente trafikkdata med sikte på å identifisere kommunikasjonsanlegg.[126] Henvisningen til bokstav a innebærer her også at det er en forutsetning at lokaliseringen gjelder kommunikasjonsanlegg som den «mistenke besitter»» eller kan «antas å ville bruke».[127]

Tilbyderne kan utlevere kommunikasjonsdata dersom kunden samtykker til det.[128] Videre kan politiet få tilgang til kommunikasjonsdata dersom vilkårene for nødrett er oppfylt.[129] For det tredje kan politiet med hjemmel i strpl. § 216 b annet ledd bokstav d be retten om å pålegge eier eller tilbyder om å gi opplysninger om kommunikasjonsdata knyttet til kommunikasjonsanlegg som mistenkte besitter eller kan antas å ville bruke. Bestemmelsen brukes i hovedsak til innhenting av trafikkdata der man samtidig gjennomfører kommunikasjonsavlytting.[130]

Strpl. § 216 a fjerde ledd gjelder tilsvarende ved kontroll av kommunikasjon jf. strpl § 216 b tredje ledd. Eier eller tilbyder av nettverk har plikt til å yte bistand ved politiets kontroll av kommunikasjonen.

[125] Ot.prp. nr. 64 (1998-1999) side 159.
[126] Bruce og Haugland (2018) side 207.
[127] Prop. 68 L (2015-2016) side 281.
[128] Bruce og Haugland (2018) side 226.
[129] Bruce og Haugland (2018) side 226.
[130] Bruce og Haugland (2018) side 226.

3.2.3 Dataavlesing

Etter straffeprosessloven § 204 er det straffbart å «bryte en beskyttelse» eller ved annen «uberettiget fremgangsmåte» skaffe seg tilgang til datasystem eller del av det.

Politiet har imidlertid hjemmel til å utføre datainnbrudd i strpl. § 216 o og § 216 p. Bestemmelsene om dataavlesing i §§ 216 o og § 216 p er plassert sammen med andre «tvangsmidler» i straffeprosesslovens fjerde del. Etter strpl. §216 o kan retten 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 med ti års strafferamme jf. bokstav a eller som faller under ett av kategoriene i bokstav b.

Den juridiske definisjonen for dataavlesing er at dette er en metode for «avlesing av ikke offentlig tilgjengelige opplysninger i et datasystem». Dette er ikke en entydig definisjon og kan omfatte mange teknologiske fremgangsmåter. Forarbeidene understreker at «begrepet dataavlesing kan være dekkende for ulike fremgangsmåter for å skaffe tilgang til informasjon som produseres, lagres eller kommuniseres i eller mellom elektroniske informasjonssystemer».[131]

3.2.3.1 Objektet for avlesing

Begrepet «datasystem» er det objektet som kan avleses.[132] Det er dermed en forutsetning at den informasjonen politiet ønsker tilgang til finnes innenfor et datasystem.

«Data» er etter informasjonsteknologisk terminologi definert som enhver representasjon av informasjon som ikke er lesbar uten bruk av teknisk hjelpemiddel.[133] Forarbeidene definerer «datasystem» som enhver innretning bestående av maskinvare og programvare, som foretar behandling av data ved hjelp av dataprogrammer. [134]

I tillegg til å avlese datasystemer, gir bestemmelsene om dataavlesing også politiet mulighet til å avlese brukerkontoer til nettverksbaserte kommunikasjons og lagringstjenester jf. strpl. § 216 o fjerde ledd. Avlesing av nettverksbaserte kommunikasjons og lagringstjenester forutsetter at politiet har informasjon om brukernavn og passord, for å få «tilgang» til kontoen.[135]

[131] Prop. 68 L (2015-2016) side 224.
[132] Bruce og Haugland (2018) side 252.
[133] Ot.prp. nr. 22 (2008-2009) side 400.
[134] Prop. 68 L (2015-2016) side 283.
[135] Prop. 68 L (2015-2016) side 270.

3.2.3.1.1 «Datasystem» favner videre enn «kommunikasjonsanlegg»

Objektet for avlesing er forskjellig ved dataavlesing og kommunikasjonskontroll. For kommunikasjonskontroll er avlyttingen og kontrollen begrenset til «kommunikasjonsanlegg». En vesentlig forskjell mellom lovbestemmelsene om dataavlesing og kommunikasjonskontroll er at «datasystem» er mer vidt og omfatter mer enn det «kommunikasjonsanlegg» gjør.

Som eksempel nevner forarbeidene at en kopi maskin vil kunne betegnes som et «informasjonssystem», men ikke nødvendigvis som «kommunikasjonsanlegg». Dersom dette holdes opp mot definisjonen av «datasystem» ovenfor, vil det være logisk at en kopimaskin kan betegnes som et datasystem, fordi en kopimaskin vil være en maskinvare med installerte programmer. Dette vil gjøre en kopimaskin til et datasystem, som vil falle under ordlyden i strpl. §216 o første ledd.

Det kommer frem av lovproposisjonen at kopimaskinen kan manipuleres til å lagre informasjon som normalt ikke lagres.[136] For eksempel kan kopimaskinen lagre bilder av dokumenter som kopieres på den. Det har gode grunner for seg at en kopimaskin kan manipuleres til å lagre informasjon. Dette vil gi politiet mulighet til å få innsyn i informasjon som verken blir «lagret» eller «kommunisert», med den følge at reglene om ransaking og beslag samt kommunikasjonskontroll ville vært utilstrekkelig i slike tilfeller.[137]

En kopimaskin kan ikke anses som et «kommunikasjonsanlegg», fordi denne betegnelsen brukes om anlegg som er ment å veksle informasjon med. Det er ikke mulig å utveksle informasjon mellom ulike kopimaskiner.

Begrepet «datasystem» er hentet fra straffeloven § 204 og skal være «teknologinøytral» i den forstand at det ikke spiller noen rolle om systemet mottar, behandler eller videreformidler informasjon, og at det også omfatter kommunikasjonsanlegg av ulike slag.[138] Utvalget har forutsatt at begrepet i tillegg til kopimaskiner, også kan omfatte GPS-ser og skannere. Det er en fordel dersom politiet kan avlese for eksempel en GPS og se hvor kriminelle befinner seg. Dette kan være spesielt aktuelt når kriminelle er på «ferd» og politiet ikke kan gå til umiddelbar pågripelse, men må vente og vurdere når det vil være hensiktsmessig å gripe inn fysisk. Politiet kan også i slike situasjoner ha alternativ om avvente og følge med på kriminelles «bevegelser», i håp om at de kan bli ledet til andre og eventuelt større spor. Overvåking av en GPS vil kunne være nyttig for å bekjempe kriminalitet.

[136] Prop. 68 L (2015-2016) side 224.
[137] Prop. 68 L (2015-2016) side 226.
[138] Prop. 68 L (2015-2016) side 244.

Videre vil betegnelsen «datasystem» også dekke det som ellers betegnes som «kommunikasjonsanlegg» som datamaskiner og mobiltelefoner.[139]

Etter § 216 o fjerde ledd, kan dataavlesing bare omfatte «bestemte» datasystemer eller brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester som den «mistenkte besitter» eller kan «antas å ville bruke». Her gjelder samme krav om identifikasjon som ved kommunikasjonskontroll. Når det gjelder brukerkontoer, kan disse identifiseres ved hjelp av brukernavn eller e-post adresse.[140] Kravet om at mistenkte må besitte eller kan antas å ville bruke datasystemet, vil etter forarbeidene forstås på samme måte som kravet for kommunikasjonsavlytting i § 216 a tredje ledd. Det bør likevel ut fra objektive kriterier kunne konstateres en viss sannsynlighet for at mistenkte vil bruke datasystemet eller brukerkontoen.[141]

3.2.3.2 Hvilke typer informasjon kan politiet avlese?

Videre må informasjonen som avleses være «ikke offentlig tilgjengelige opplysninger». Dette tilsier at det er opplysninger som ikke deles med allmennheten, noe som indikerer at opplysningene bærer karakter av å være personlig.

Etter § 216 o fjerde ledd annet punktum, kan avlesingen omfatte kommunikasjon, elektronisk lagrede data og andre opplysninger om bruk av datasystemet eller brukerkontoen. Dette omfatter informasjon som politiet ellers har rettslig adgang til gjennom reglene om kommunikasjonskontroll og ransaking.[142] Forarbeidene har en oppregning av hvilke typer informasjon det kan tenkes at dataavlesing kan omfatte. Dataavlesing kan innebære avlesing av for eksempel lydstrømmen som sendes utfra fra en tilknyttet mikrofon eller høyttaler fra operativsystemets drivere, videostrømmen som sendes ut fra tilknyttet kamera, tastetrykk som sendes fra tastaturet, innholdet på harddisk, minnepenn osv.[143] Videre omfatter det data som hentes inn fra eller sendes ut på internett eller andre nettverk samt IP-adresser knyttet til nettverksenhetene.[144] Tillatelse til dataavlesing gir dermed også mulighet til å kontrollere kommunikasjon.

[139] Prop. 68 L (2015-2016) side 224.
[140] Prop. 68 L (2015-2016) side 270.
[141] Prop. 68 L (2015-2016) side 271.
[142] Prop. 68 L (2015-2016) side 264.
[143] Prop. 68 L (2015-2016) side 224.
[144] Bruce og Haugland (2018) side 257.

3.2.3.3 Fortløpende overvåking av all aktivitet i et datasystem

Skillet mellom elektronisk lagret informasjon og informasjon som er under overføring, har ikke betydning ved dataavlesing.[145] Dataavlesing som metode gir adgang til å følge med på bruken av datasystemet over tid, og samle inn informasjon som genereres.[146] Overvåkningen retter seg mot all aktivitet som gjøres på en datamaskin. Ved kommunikasjonskontroll derimot er politiet er avhengig av at meldingene sendes fra avsender til mottaker.[147] Dette skillet mellom informasjon som er under overføring og det som kun er skrevet, men ikke sendt videre, har ikke betydning under dataavlesing.

Det har videre ikke betydning at informasjonen ikke er lagret elektronisk. Ved ransaking og beslag er politiet avhengig av at informasjonen finnes lagret et sted. Ved dataavlesing har politiet kontroll over alt som gjøres og eksisterer på en datamaskin i nå tid, selv informasjon som ikke er lagret, sendt videre eller kryptert enda.

Dataavlesing kan dermed også fange opp tanker, assosiasjoner og ønsker som ikke var ment kommunisert til andre.[148] Meldinger som er nedskrevet, men ikke sendt, havner i utkastmapper på e-post som kan avleses av politiet. Personen har kanskje overveid dette som informasjon vedkommende har ønsket å holde for seg selv og dermed ikke «kommunisert» til andre. Dette vil være opplysninger som metodene kommunikasjonskontroll, ransaking og beslag ikke ville gitt tilgang til.[149] Dataavlesing fanger opp selv disse aspektene, noe som byr på personvernutfordringer.

Ettersom overvåkingen er rettet mot all aktivitet i et datasystem, kan dataavlesing også fange opp opplysninger om hvilke datasystemer som har vært i kontakt med hverandre, deres geografiske plassering samt tidspunkt og varighet av kommunikasjonen. Dataavlesing kan dermed også brukes til å innhente det som betegnes som «trafikkdata» etter strpl. § 216 b annet ledd bokstav d.

Det ligger en begrensning i metodebruken ved at informasjonen som avleses må generes *i* og *av* datasystemet som kan avleses.[150] Tilfeller som åpenbart vil falle utenfor rammene for hva politiet kan gjøre med grunnlag i tillatelsen til dataavlesing, vil for eksempel være å aktivere mikrofoner tilknyttet datasystemet for å fange opp lyd i et rom eller slå på et kamera på egen

[145] Bruce og Haugland (2018) side 256-257.
[146] Bruce og Haugland (2018) side 257.
[147] Prop. 68 L (2015-2016) side 226.
[148] Prop. 68 L (2015-2016) side 252.
[149] Bruce og Haugland (2018) side 257.
[150] Prop. 68 L (2015-2016) side 264 (min kursiv)

hånd.[151] Dette må hjemles i reglene for romavlytting i strpl. § 216 m eller bestemmelsene om skjult kameraovervåking i kapittel 15 a.[152]

3.2.3.4 Teknologinøytral ved fremgangsmåte

Bestemmelsen om dataavlesing er teknologinøytral i den forstand at fremgangsmåten ikke er beskrevet konkret, og en vet ikke hvilke teknologiske fremgangsmåter politiet kan benytte. Dataavlesing ville etter Metodekontrollutvalgets vurdering referere seg til en gjennomføringsmåte, som det ikke er tradisjon for å beskrive i detalj under de enkelte tvangsmidler i straffeprosessloven.[153] Videre nevner departementet at politiet også av taktiske årsaker bør levnes en viss mulighet til å utvikle og benytte fremgangsmåter som ikke i detalj blir kjent.[154] Dette har gode grunner for seg. Hadde kriminelle hatt kjennskap til politiet sine fremgangsmåter, kunne man risikere at kriminelle systematisk ville motarbeidet disse og hatt kunnskap om på hvilke områder de kunne utvikle sine metoder på, for å beskytte seg mot innbrudd fra politiet.

Det som skiller fremgangsmåten ved dataavlesing fra kommunikasjonskontroll, er at informasjonen ved dataavlesing kan avleses i selve datasystemet.[155] Dette står i kontrast til kommunikasjonskontroll der politiet må innhente informasjonen hos teletilbyder. Ved dataavlesing er det ikke nødvendig for politiet å gå via en tredjeperson.

Hvordan politiet konkret skal gå frem, er til en viss grad presisert nærmere i § 216 p første ledd femte punktum der det står at «tekniske innretninger» og «dataprogram» kan «installeres i datasystemet» og «annen maskinvare kan knyttes til datasystemet».[156]

Dette betyr at politiet må installere sine tekniske innretninger eller dataprogrammer i datasystemet de ønsker å avlese. Politiet kan alternativt «knytte» «annen maskinvare» til datasystemet. Forarbeidene definerer «annen maskinvare» som tilbehør som ikke nødvendigvis er en del av datamaskinen, som for eksempel hodetelefoner, tastaturer eller eksterne lagringsmedier, herunder «minnepenner».[157] Da vil dataprogrammer og tekniske innretninger installeres i slike tilbehør og komponenter, som politiet deretter kan knytte til datamaskinen.

[151] Prop. 68 L (2015-2016) side 264.
[152] Prop. 68 L (2015-2016) side 264.
[153] NOU 2009:15 side 244.
[154] Prop. 68 L (2015-2016) side 264.
[155] Bruce og Haugland (2018) side 248.
[156] Bruce og Haugland (2018) side 253-254.
[157] Prop. 68 L (2015-2016) side 271.

Politiet har flere tekniske muligheter å benytte ved gjennomføring av dataavlesing. Metodekontrollutvalget ønsket ikke å gå nærmere inn på en beskrivelse av de teknologiske fremgangsmåtene fordi de raskt kunne bli utdatert.[158] Metodekontrollutvalget ser likevel for seg to hoved gjennomføringsmåter, henholdsvis en «softwarebasert» og en «hardwarebasert» løsning. I praksis gjøres dette gjennom at det innhentes informasjon ved å installere programvare «software» eller en maskinvare «hardware» på eller i et datasystem.

3.2.3.4.1 Softwarebasert løsning

Ved en «software» basert løsning installerer politiet et program i vedkommende sin datamaskin, som gjør politiet i stand til å hente ut informasjon fra datasystemet.[159]

For å installere en programvare, kan politiet velge å gå frem på ulike måter.[160] Politiet kan utnytte sikkerhetshull i systemet og modifisere filer som lastes ned av bruker eller sende e-post med vedlegg, eventuelt som skjult vedlegg, med det aktuelle programmet. Disse programmene kan for eksempel omfatte «trojanske hester». Trojanske hester er dataprogrammer som skjuler seg inne i andre nyttige programmer eller dokumenter.[161] De kan ha ulike funksjoner, og for eksempel legge «vertsmaskinen» åpen for «innbrudd» utenfra eller lagre/sende informasjon som ligger på maskinen.[162] Når programmet er installert, vil det registrere all aktivitet på maskinen i en logg, som med jevne mellomrom overføres til politiet via e-post.[163] Brukeren vil ikke merke at dataprogrammer blir installert eller at data overføres.

Videre har politiet mulighet til å installere programvaren fysisk, det vil si i forbindelse med en hemmelig ransaking. En mulighet er også å utføre innbrudd i datasystemet for å installere programvare.[164] De ulike fremgangsmåtene krever dermed ikke nødvendigvis at politiet gjør et elektronisk «innbrudd» i datasystemet for å få tilgang.

[158] NOU 2009:15 side 247.
[159] NOU 2009:15 side 247.
[160] Prop. 68 L (2015-2016) side 224.
[161] Ot.prp. nr. 64 (1998-1999) side156.
[162] NOU 2003: 18 side 126.
[163] Ot.prp. nr. 64 (1998-1999) side 156.
[164] Prop. 68 L (2015-2016) side 224.

3.2.3.4.2 Hardwarebasert løsning

Denne fremgangsmåten kan kobles til «annen maskinvare som kan knyttes til datasystemet» i strpl. § 216 p første ledd femte punktum.

Her installeres komponenter typisk på mistenktes datamaskin, som gjør politiet i stand til å skaffe seg tilgang til informasjonen.[165] Metodekontrollutvalget har beskrevet nærmere hvordan utstyr kan benyttes til å «avlese» informasjonen i datasystemet. Som eksempel nevnes at «utstyr som leser av tastetrykkene monteres i tastaturet (key-logging) eller at det monteres utstyr i overgangen mellom tastaturet og selve datamaskinen, for eksempel i en usb-port, som leser av informasjonen som går fra tastaturet til maskinen, eller at det monteres utstyr i headsett eller mikrofon som gjør det mulig å fange opp lydsignalene ved kommunikasjon over Internett».[166] En hardwarebasert løsning fordrer at tilbehør og komponenter kan «knyttes» til «datamaskinen». Plassering av maskinvare forutsetter i utgangspunktet at politiet har fysisk tilgang til datasystemet.[167]

3.2.3.4.3 Utfordringer

Fremgangsmåtene ved dataavlesing byr på flere utfordringer, sammenlignet med kommunikasjonskontroll. I tillegg til at det skjer et inngrep i form av at politiet griper inn i privatlivet til den enkelte, kan det også skje et enda inngrep i form av at politiet skaffer seg tilgang til datasystemet. Politiet kan foreta innbrudd enten fysisk eller digitalt for å skaffe seg tilgang.

For å skaffe seg tilgang, kan politiet «bryte eller omgå beskyttelse i datasystemet dersom det er nødvendig for å kunne gjennomføre avlesingen» jf. § 216 p første ledd fjerde punktum. Politiet har dermed adgang til å gjennomføre datainnbrudd for å gjennomføre avlesingen.

I tillegg kan politiet etter strpl. § 216 p første ledd siste punktum foreta fysiske innbrudd som er nødvendig for å plassere eller installere hardware eller software i forbindelse med dataavlesingen, så fremt retten ikke bestemmer noe annet. Slike innbrudd vil utgjøre ytterlige ett inngrep. Et alternativ til fysisk innbrudd ved hardwarebasert fremgangsmåte, er å få bistand fra utenforstående, for eksempel et selskap med kundeforhold til mistenkte, som enten kunne gitt bistand ved å installere ulike komponenter eller kanskje forledet mistenkte til selv å installere programvaren.[168]

---

[165] NOU 2009:15 side 247.

[166] NOU 2009:15 side 248.

[167] Prop. 68 L (2015-2016) side 224.

[168] Bruce og Haugland (2018) side 258.

For å innhente den avleste informasjonen må politiet kanskje hente dataene via bakdør til programvaren fra internettet, fange opp via kommunikasjonskontroll, få programvaren til å lagre dataene på datautstyret, eventuelt sende dem via internettet eller annet installert nettverk/radioutstyr som politiet råder over.[169] Metodekontrollutvalget understreker videre at det kan tenkes at politiet må innhente den avleste informasjonen eventuelt ved et nytt innbrudd i datasystemet. Dette vil da utgjøre et ytterligere innbrudd. Det er vanskelig å si noe om hvor ofte denne fremgangsmåten brukes i praksis, siden politiets fremgangsmåter holdes utenfor offentligheten. Ved dataavlesing kan det dermed skje flere «inngrep» (og eventuelt «innbrudd») avhengig av fremgangsmåte politiet velger.

[169] NOU 2009:15 side 248.

3.3 Materielle vilkår

Selv om det er grunnleggende forskjeller mellom lovbestemmelsene om kommunikasjonskontroll og dataavlesing, finnes det også flere likheter. I det følgende foretas en gjennomgang av de materiellene vilkårene for kommunikasjonskontroll og dataavlesing.

3.3.1 Kommunikasjonskontroll

Det vil først redegjøres for vilkårene for kommunikasjonsavlytting i § 216 a og deretter for annen kontroll av kommunikasjonsanlegg i § 216 b.

3.3.1.1 Kommunikasjonsavlytting strpl. § 216 a

Etter § 216 a kan retten ved kjennelse gi politiet tillatelse til å foreta kommunikasjonsavlytting, når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling som kan medføre straff av fengsel i ti år eller mer jf. bokstav a eller som faller under de særskilt angitte straffebudene i bokstav b.

Bokstav a angir handlinger som etter loven kan medføre straff av fengsel i 10 år eller mer. Det er strafferammen i straffebudet som er avgjørende, og ikke forventede straff for vedkommende mistenkt.[170] Dersom strafferammekravet ikke er oppfylt, er det også adgang til å iverksette tvangsmiddelbruken etter alternativ b, for handlinger som rammes av visse lovbestemmelser.

Av oppregningen, kan straffebudene sorteres i ulike kategorier ut fra type kriminalitet. Dette omfatter for det første straffebud som truer statens selvstendighet og sikkerhet. Videre omfatter det terror og militær relatert virksomhet. Opplæring og oppfordring til terrorvirksomhet er kanskje ikke så alvorlige handlinger sammenlignet med terrorhandlinger, men disse handlingene kan foranledige senere terrorhandlinger og det er gode grunner for å tillate kommunikasjonsavlytting i slike saker. Videre omfatter bokstav b narkotikavirksomhet, heleri og hvitvasking av utbytte fra narkotikalovbrudd, frihetsberøvelse og menneskehandel og fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn. Alle disse forbrytelsene er av alvorlig karakter og er kjennetegnet av særlig etterforskningsmessige utfordringer.[171]

[170] Haugland (2021) note til straffeprosessloven § 216 a

[171] Innst. 343 L (2015-2016) side 11.

Strafferammekravet viser at kommunikasjonsavlytting brukes i etterforskning av den mest alvorlige kriminaliteten. Lovbestemmelsene er gitt etter en vurdering av typer straffbare handlinger skjult tvangsmiddelbruk er ansett særlig egnet til oppklaring av.[172]
Visse typer kriminalitet er kjennetegnet som «offerløs» kriminalitet. Ved narkotikavirksomhet, får politiet sjelden en anmeldelse eller en ytre manifestasjon av forbrytelsen, utenom tollvesenets kontroll.[173] Videre er skjult tvangsmiddelbruk særlig egnet til å avklare typer kriminalitet som er preget av en manglende eller redusert tilgang på mer tradisjonelle typer bevis.[174]

Dersom vilkårene i strl. § 79 om forhøyelse av straff er oppfylt, vil kommunikasjonsavlytting kunne foretas i saker med over fem års strafferamme.[175]

3.3.1.2 Annen kontroll med kommunikasjonen strpl. § 216 b

Retten kan også ved kjennelse gi politiet tillatelse til å foreta annen kontroll av kommunikasjonsanlegg, når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling som kan medføre straff av fengsel i fem år eller mer eller som omfattes av kapittel 21 jf. bokstav a eller som faller under et av de særskilt angitte straffebudene i bokstav b.
Tilsvarende krav gjelder for «forsøk» her som i § 216 a.

Strafferammekravet i § 216 b bokstav a er handlinger som kan medføre straff av fengsel i fem år eller mer. Her gjelder et lavere strafferammekrav enn i § 216 a som krever 10 år.
I likhet med § 216 a, er det også her adgang til å iverksette tvangsmiddelbruken etter alternativ b, dersom straffekrammet kravet i bokstav a ikke er oppfylt. Mange av straffebudene i oppregningen er de samme som nevnt i § 216 a bokstav b, men opplistingen er imidlertid ikke helt identisk. Noen straffebud er utelatt, mens andre er tilføyd.

Strl § 257, 145 og 146 er ikke inntatt i § 216 b fordi straffebudene har seks års strafferamme, og dermed uansett oppfyller strafferammekravet i § 216 b, som er fem år. Videre omfatter § 216 bokstav b i tillegg handlinger i § 198 om forbund om alvorlig organisert kriminalitet, § 266 om hensynsløs atferd og avtaler om møte for å begå seksuelt overgrep etter § 306.

Dersom vilkårene strl. § 79 om forhøyelse av straff er oppfylt, vil annen kontroll av kommunikasjonsanlegg kunne foretas i saker med tre års strafferamme.[176]

[172] Bruce og Haugland (2018) side 65.
[173] Rt. 1984- 1076 (307-84) side 1080.
[174] Bruce og Haugland (2018) side 65.
[175] Bruce og Haugland (2018) side 211.
[176] Bruce og Haugland (2018) side 211.

3.3.1.3 Felles inngangsvilkår strpl. § 216 c

Ved kommunikasjonskontroll gjelder to tilleggsvilkår**.** Tillatelse til kommunikasjonskontroll kan bare gis dersom det må antas at slik avlytting eller kontroll vil være av «vesentlig betydning for å oppklare saken» og «oppklaring ellers i vesentlig grad vil bli vanskeliggjort» jf. § 216 c.

Førstnevnte kalles også indikasjonskravet og innebærer at metodebruken må frembringe opplysninger av betydning for etterforskning.[177] Ordet «antas» forstås som at det må foreligge noe mer enn ren formodning om at metodebruken vil føre til dette.[178]
Sistnevnte vilkåret kalles subsidiaritetskravet, og stiller et krav om at inngripende metodebruk bare skal finne sted når mindre inngripende metoder ikke anses anvendelige.[179] Hvis de samme opplysningene kan innhentes like enkelt på en mindre integritetskrenkende måte, er det dette å foretrekke. Hensynet til ressursbruk, ulemper, risiko og tidsmoment er relevante momenter i vurderingen av en alternativ innhenting.[180]

Vilkårene i strpl. § 216 c gjelder ved «kommunikasjonskontroll» og kommer derfor til anvendelse både for beslutning om kommunikasjonsavlytting og for beslutning om annen kontroll av kommunikasjonsanlegg.

3.3.1.4 Tilleggsvilkår

I visse type situasjoner er det også et krav om «særlige grunner» jf. § 216 c annet ledd i tillegg til inngangsvilkårene. Dette gjelder for eksempel under temporær masseavlytting, der politiet kanskje må avlytte telefonautomater som brukes av allmennheten.[181] Identifisering av kommunikasjonsanlegg gjennom avlytting av alle samtaler i et bestemt tidsrom, utfordrer personvern og rettssikkerhetshensyn på en annen måte enn der identifiseringen kan skje uten avlytting.[182]

Dersom de hensynene som begrunner adgang til kommunikasjonskontroll gjøre seg sterkt gjeldende, vil kravet om særlige grunner være oppfylt.[183] For eksempel der kommunikasjonskontroll er nødvendig for å oppklare saken eller det gjelder et alvorlig forhold.[184] Kravet om særlige grunner skal imidlertid ikke praktiseres slik at den mistenkte kan unndra seg

[177] Bruce og Haugland (2018) side 212.
[178] Ot.prp.nr. 60 (2004-2005) side 71.
[179] Ot.prp.nr. 60 (2004-2005) side 71.
[180] Ot.prp.nr. 60 (2004-2005) side 71.
[181] Haugland (2021) note til straffeprosessloven § 216 c.
[182] Ot.prp. nr. 60 (2004-2005) side 110.
[183] Prop. 147 L (2012-2013) side 177.
[184] KK-2002-2-Rt. 2005-199.

kommunikasjonskontroll.[185] Samme vilkår gjelder dersom kontrollen retter seg mot personer som av tradisjon fører samtaler av fortrolig art, som advokater, leger, prester og journalister, med mindre de er selv mistenkt i saken jf. § 216 c annet ledd annet punktum.

3.3.2 Dataavlesing

Etter § 216 o kan retten ved kjennelse gi politiet tillatelse til å foreta avlesing av ikke offentlig tilgjengelige opplysninger i et datasystem, når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling som kan medføre straff av fengsel i ti år eller mer jf. bokstav a eller som faller under de særskilt angitte straffebudene i bokstav b.

Strafferammekravet for dataavlesing er tilsvarende det som gjelder for kommunikasjonsavlytting etter § 216 a første ledd bokstav a. Opplistingen av straffebudene er omtrent de samme som kommunikasjonsavlytting etter § 216 a første ledd bokstav b.

Bestemmelsene i strl. §§ 145 og 146 er utelatt. Førstnevnte har seks års strafferamme, og dataavlesing vil kunne anvendes dersom reglene om forhøyelse av straff i strl. § 79 kommer til anvendelse. Forarbeidene nevner at forhøyelse av straff i strl. § 79 bokstav a og b ved gjentakelse eller sammenstøtt av forbrytelser ikke kommer i betraktning ved dataavlesing.[186] Forhøyelse av straff kan likevel komme i betraktning etter strl. § 79 bokstav c, dersom handlingen er utført som ledd i organisert kriminalitet.

Slik bestemmelsen står i dag kreves det grov narkotikaovertredelse § 232 og grovt heleri §333 for at dataavlesing skal kunne anvendes i saker om narkotika og heleri. Lovbestemmelsen åpner for å benytte dataavlesing i saker om hvitvasking og uaktsom hvitvasking av utbytte fra simpelt narkotikalovbrudd i § 231, men dataavlesing i slike saker vil ofte være uforholdsmessig etter strpl. § 170 a.[187] Dette antas å ha vært en henvisningsfeil mellom bestemmelsene og at det antakelig skulle ha vært inntatt henvisninger enten til heleri og hvitvasking av utbytte fra grove narkotikalovbrudd eller grovt heleri og grov hvitvasking av utbytte fra grove narkotikalovbrudd.[188]

Tillatelse til dataavlesing 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. Dette er samme vilkår som gjelder ved kommunikasjonskontroll etter § 216 c første

[185] Prop. 147 L (2012-2013) side 177.
[186] Prop. 68 L (2015-2016) side 267-268.
[187] Bruce og Haugland (2018) side 260.
[188] Bruce og Haugland (2018) side 260.

ledd, og skal forstås på samme måte.[189] Kravet om særlige grunner i § 216 c annet ledd, gjelder også ved dataavlesing i angitt situasjoner jf. § 216 o tredje ledd annet punktum.

3.3.3 Felles vilkår

Både ved dataavlesing og kommunikasjonskontroll er det krav om at personen med «skjellig grunn» mistenkes for en straffbar handling eller forsøk på handling i bokstav a eller b. Uttrykket «skjellig grunn» har samme innhold som når det brukes ellers i straffeprosessloven. I straffeprosessloven er det tolket som sannsynlighetsovervekt for at vedkommende har begått en handling som objektivt sett svarer til straffebudet.[190] Bestemmelsene forutsetter også at grensen for straffri forberedelse er passert.[191]

Adgangen til iverksetting av kommunikasjonskontroll og dataavlesing er uavhengig av om straff kan idømmes etter straffeloven § 20, enten fordi mistenkte er utilregnelig eller under kriminell lavalder. Samme gjelder dersom tilstanden har medført at mistenkte ikke har utvist skyld jf. § 216 a annet ledd første og annet punktum jf. § 216 b annet ledd. For dataavlesing følger dette av § 216 o annet ledd første og annet punktum.
Dataavlesing og kommunikasjonskontroll, må i likhet mellom andre tvangsmidler, alltid oppfylle kravene til forholdsmessighet i strpl. § 170 a.

[189] Haugland (2021) note til straffeprosessloven 216 o.
[190] Haugland (2021) note til straffeprosessloven 216 a.
[191] Ot.prp. nr. 40 (1991-1992) side 38.

3.4 Prosessuelle vilkår

Ved innføringen av dataavlesing som politimetode, ble mange av de prosessuelle vilkårene for kommunikasjonskontroll, gitt samme anvendelsesområde under dataavlesing. Jeg starter derfor med å gi en fremstilling av de prosessuelle vilkårene for kommunikasjonskontroll i kapittel 16 a i straffeprosessloven.

3.4.1 Kommunikasjonskontroll

Påtalemyndigheten må sende begjæring og få rettens kjennelse for å iverksette bruk av skjulte tvangsmidler. Dette fremgår av bestemmelsene for kommunikasjonskontroll i strpl. §§ 216 a, 216 b og for dataavlesing i § 216 o. Dersom det ved opphold er stor fare for at etterforskningen vil lide i påvente av rettens kjennelse, kan påtalemyndighetens ordre inntre jf. § 216 d. Påtalemyndigheten er gitt hastekompetanse i saker om kommunikasjonskontroll. Beslutningen fra påtalemyndigheten må «snarest mulig» og senest innen 24 timer etter påbegynt kontroll, sendes retten for godkjennelse jf. § 216 d første ledd annet punktum. Her foretar retten en «etterkontroll» av beslutningen. Saken må videre fremlegges for retten der det er mest praktisk jf. § 216 e.

Ved kommunikasjonskontroll kan det gis tillatelse for opp til 4 uker jf. § 216 f. Tillatelsen skal ikke være lenger enn «strengt nødvendig», og kan derfor også vare mindre dersom behovet tilsier det i en sak. Videre er det gitt regler for oppbevaring av data i § 216 g, om kontrollutvalget i § 216 h og taushetsplikt etter § 216 i.

I utgangspunktet skal mistenkte og den som har rådighet over kommunikasjonsanlegget underrettes når kommunikasjonskontrollen er avsluttet jf. § 216 j første ledd.
Det kan likevel ved kjennelse besluttes at underretning kan utsettes dersom dette vil være til vesentlig skade for etterforskningen i saken eller annen verserende sak hvor det kan besluttes underretning eller dersom hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig jf. § 216 j første ledd annet punktum.
Underretningen skal gis senest når tiltale tas ut eller fristen for omgjøring av påtalemyndighetens beslutninger om påtaleunnlatelse er utløpt etter strpl. § 75 annet ledd første punktum. jf. § 216 j tredje ledd.

Retten kan også beslutte at underretning kan unnlates dersom saken henlegges og underretning vil være til vesentlig skade for fremtidig oppklaring av saken eller etterforskning av en annen sak hvor det kan besluttes utsatt underretning eller dersom hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig jf. § 216 j tredje ledd annet punktum.

3.4.2 Dataavlesing

Det fremgår av § 216 o femte ledd at reglene fra §§ 216 d til 216 k gjelder tilsvarende for dataavlesing, med forbehold om at rettens tillatelse ikke kan gjelde for mer enn 2 uker om gangen for dataavlesing.

3.4.2.1 Særlige vilkår ved dataavlesing

Dataavlesing stiller i tillegg noen prosessuelle og personelle krav til gjennomføringen av metoden, som er ment å minimere sikkerhetsrisikoer som kas tenkes å oppstå ved gjennomføring av dataavlesing. Disse kan fungere som rettsikkerhetsgarantier.

Etter § 216 p første ledd er det kun personell som er «særlig» skikket til det, som kan foreta dataavlesing etter § 216 o. For å understreke viktigheten av at det ikke gjøres større inngrep i noens privatliv enn nødvendig, er det stilt opp et ekstra vilkår i § 216 p annet ledd.[192] Dataavlesingen skal innrettes slik at det ikke «unødig» fanges opp opplysninger om andre enn mistenktes bruk av datasystemet. Avlesingen skal være målrettet og er praktisk i tilfeller der den mistenkte deler datasystemet med andre.[193]

Avlesingen skal videre utføres forsiktig slik at det ikke «unødig» voldes fare for driftshindring eller skade på utrustning eller data jf. § 216 p annet ledd annet punktum. Noe skade må likevel aksepteres ettersom det er den «unødige» faren som bør unngås. Dersom politiet står overfor flere alternativer, kan dette innebære en plikt til å velge mer omstendelige fremgangsmåter, for at det ikke «unødig» voldes fare for skade på utrustning eller data.[194]

Politiet skal også passe på sikkerheten ved «så vidt mulig» avverge at noen som følge av gjennomføringen skaffer seg uberettiget tilgang til datasystemet, vernet informasjon eller til å begå andre straffbare handlinger § 216 p annet ledd tredje punktum. Det kreves nøyaktig registrering av hva politiet har foretatt seg ved dataavlesing ved protokollføring.[195] Hjemmelen for dette er i dag kommunikasjonskontrollforskriften § 7 første ledd, som stiller krav til politiets protokoll ved bruk av kommunikasjonskontroll, romavlytting og dataavlesing. Ved tvangsmiddelbruk i nevnte saker, skal politiet føre en «protokoll» med oversikt over en rekke opplysninger om tvangsmiddelbruken, for eksempel når tvangsmiddelbruken startet jf. § 7 første ledd nr. 6, hvilke kommunikasjonsanlegg/datasystem tvangsmiddelbruken er rettet mot jf. § 7

[192] Prop. 68 L (2015-2016) side 272.
[193] Prop. 68 L (2015-2016) side 272.
[194] Prop. 68 L (2015-2016) side 272.
[195] Prop. 68 L (2015-2016) side 272.

første ledd nr. 5 samt opplysninger om opphør, sletting og sperring. Det stilles i § 7 annet ledd noen tilleggskrav ved dataavlesing. Kravet til protokollføring vil sikre notoritet med politiets tvangsmiddelbruk.

Utstyr som er benyttet i forbindelse med gjennomføringen av dataavlesing skal fjernes «snarest mulig», etter periodens utløp jf. § 216 o femte ledd annet punktum.

3.5 Kontrollsystem

Det må føres kontroll med politiets bruk av kommunikasjonskontroll og dataavlesing som skjulte tvangsmidler, for å sikre at det ikke gis tillatelse til innhenting av informasjon som faller utenom hjemmelsgrunnlaget.[196] Kontrollsystemet for kommunikasjonskontroll og dataavlesing består av de samme kontrollmekanismene som presenteres nedenfor.

3.5.1 Intern kontroll

Kontrollsystemet består av både interne kontrollmekanismer, som politiets og påtalemyndighetens organinterne kontroll og eksterne kontrollmekanismer, som advokater, domstolskontroll eller kontroll gjennom utvalg. En forutsetning for at den eksterne kontrollen skal være effektiv, vil ofte være at den interne kontrollen, særlig i form av rapporteringer fungerer tilfredsstillende.[197]

Intern kontroll består av de organinterne kontrollmekanismer som finnes innad i for eksempel et politidistrikt eller særorgan.[198] Påtalemyndigheten er organisert på tre nivå, og består av politiadvokater, statsadvokatene og riksadvokaten med overordnet ansvaret for ledelsen av påtalemyndigheten jf. strpl. § 56 annet ledd. Overordnet påtalemyndighet utøver kontroll med utførelsen av de påtalemessige oppgavene i politiet, blant annet gjennom sin instruksjonsmyndighet.[199] Etter strpl § 59 vil en overordnet ha instruksmyndighet overfor underordnet, og alltid kunne overta sak fra underordnet. Statsadvokatene skal føre tilsyn med straffesaksbehandlingen i politiet og gi faglig veiledning til påtalemyndigheten i politiet strpl. § 57 sjette ledd. Riksadvokatens rundskriv legger føringer for hvordan saker om skjult tvangsmiddelbruk skal behandles hos politi og påtalemyndigheten.[200]

[196] Prop. 68 L (2015-2016) side 243.
[197] Bruce og Haugland (2018) side 131.
[198] Bruce og Haugland (2018) side 132.
[199] Bruce og Haugland (2018) side 132.
[200] Kontrollutvalget for kommunikasjonskontroll årsrapport for 2016 side 6.

Videre har politiet en rapporteringsplikt til riksadvokaten i saker om kommunikasjonskontroll og dataavlesing (samt romavlytting), ved at kopi av begjæring med rettens kjennelse og sakens underlagsdokumenter må sendes til riksadvokaten uten opphold jf. kommunikasjonskontrollforskriften § 3. Det påpekes at kontrollen fra riksadvokaten er reell og verdien er meget stor.[201] Politiets omfattende rapporteringsplikt til riksadvokaten antas å ha en disiplinerende effekt.[202]

3.5.2 Ekstern kontroll

Ekstern kontroll dreier seg om den delen av kontrollen som utøves av andre utenfor politietaten. Eksterne kontrollmekanismer kan være kontroll fra offentlig oppnevnt advokat, domstolskontroll og tilsyn av Kommunikasjonsutvalget for kommunikasjonskontroll (KK-utvalget)

3.5.2.1 Offentlig oppnevnt advokat

Etter strpl. § 100 a skal retten ved behandling av begjæringer i saker om blant annet kommunikasjonskontroll og dataavlesing, oppnevne en offentlig advokat for mistenkte.
Ordningen er ment å kompensere for at mistenkte ikke gis underretning ved skjult tvangsmiddelbruk og dermed ikke kan forsvare sine interesser eller utfordre politiets tvangsmiddelbruk.[203]Advokaten opptrer på vegne av den mistenkte og skal ivareta mistenktes rettigheter, eventuelt tredjepersoners, interesser ved rettens begjæring jf. § 100 annet ledd første punktum. Primæroppgaven vil være å sørge for at faktum blir grundigere og mer allsidig belyst, samt at vilkårene for tvangsmiddelbruk og proporsjonalitet er oppfylt.[204]

Advokaten kan ikke sette seg i forbindelse med mistenkte jf. § 100 a tredje ledd første punktum. Videre har advokaten taushetsplikt om begjæringen, rettens behandling og opplysninger som fremskaffes under metodebruken jf. 100 tredje ledd annet punktum og tredje punktum. Advokaten skal være til stede under rettsmøte til behandling av begjæringen og kan uttale seg før retten treffer beslutning. jf. § 100 a annet ledd tredje punktum. Advokatens tilstedeværelse på et så tidlig stadium før rettens beslutning er tatt, gir advokaten en reell mulighet til å påvirke utfallet. Videre har advokaten ankerett i kjennelser jf. § 100 a annet ledd femte punktum.

[201] Kontrollutvalget for kommunikasjonskontroll årsrapport for 2016 side 6.
[202] Bruce og Haugland (2018) side 135.
[203] Ot.prp. nr. 64 (1998-1999) side 81.
[204] Ot.prp. nr. 64 (1998-1999) side 83.

3.5.2.2 Domstolskontroll (forutgående)

I tillegg til ordningen med offentlig oppnevnt advokat, skal også domstolene før en forhåndskontroll med politiet og påtalemyndighetens bruk av skjult tvangsmiddelbruk.
Høyesterett skal begrunne sine kjennelser jf. strpl § 52. Begrunnelsesplikten kan gjøre det enklere for advokaten å etterprøve om vilkårene for skjult tvangsmiddelbruk er oppfylt, og også være nødvendig for at kontrollutvalgene skal kunne føre en betryggende kontroll. [205]

3.5.2.3 Kommunikasjonskontroll utvalget (etterfølgende kontroll)

Kommunikasjonskontrollutvalget fører etterfølgende kontroll med politiets skjult tvangsmiddelbruk i saker om kommunikasjonskontroll, dataavlesing og romavlytting.

Kommunikasjonskontrollutvalget har som oppgave å føre kontroll med politiets og påtalemyndighetens saker om kommunikasjonskontroll jf. strpl § 216 h første ledd.
KK-utvalget kan behandle saker i avvergende øyemed jf. strpl. §222 d siste ledd der det understrekes at bestemmelsene i kapittel 16a gjelder tilsvarende.

Deres kontrollområde er regulert i kommunikasjonskontrollforskriften kapittel 2 § 14 første ledd. KK-utvalget skal kontrollere at politiets bruk av kommunikasjonskontroll, romavlytting og dataavlesing skjer innenfor rammen av lov og instrukser, der tvangsmiddelbruken begrenses mest mulig, og ikke skjer i andre saker enn nevnt i strpl. §§ 216 a og § 216 b, § 216 m og § 216 o. Utvalget har fått et særskilt ansvar for å ivareta borgernes rettssikkerhet ved å ha «særlig øye for den enkeltes rettssikkerhet» jf. § 14 første ledd annet punktum. Utvalget skal også kontrollere om de opplysningene politiet har fått ved bruk av tvangsmidler i disse sakene blir brukt på lovlig måte, samt at politiet følger lovens regler om oppbevaring, sperring og sletting og opprettholder taushetsplikten jf. § 14 annet ledd. Politiet har en rapporteringsplikt og plikter å gi opplysninger som utvalget finner nødvendig av hensyn til sine kontrollfunksjoner jf. § 216 h.

Etter kommunikasjonskontrollforskriften § 18 er utvalget et uavhengig kontrollorgan, som ikke kan instrueres eller overprøves av andre. Dette gir bra rettsikkerhet til borgerne, de kan vite at en nøytral part har ivaretatt deres rettssikkerhet mens tvangsmiddelbruken har pågått skjult.

[205] Ot.prp. nr. 64 (1998-1999) side 145.

4 FORHOLDET TIL PERSONVERN OG RETTSIKKERHET

4.1 «Tankepoliti»?

Bruk av kommunikasjonskontroll og dataavlesing kan gi politiet innsikt i omfattende informasjon og opplysninger av sensitiv karakter om personene de rettes mot. I det følgende skal jeg forsøke å gi en oppsummering av utfordringer knyttet til dataavlesing og knytte bemerkninger til kommunikasjonskontroll der dette er relevant.

Ved dataavlesing har politiet både rettslig og faktisk tilgang til alt informasjon som finnes, lagres eller sendes på eller i et datasystem. Politiet kan for eksempel avlese personlige filer, notater og kontrollere kommunikasjon fra datasystemet til andre. Personlige notater og dagbøker vil kunne være gjenstand for politiets innsyn, selv om disse ikke ment å deles videre med andre.

Metodekontrollutvalget mener at politiets kontroll av innholdet i informasjonen som lagres på maskinen uten å være kommunisert til andre, utgjør et større inngrep enn kontroll av innholdet i brukerens kommunikasjon.[206] Dette har gode grunner for seg. Kommunikasjonsavlytting kan riktignok gi politiet innsikt i en persons sinnsstemning, følelser og tankegang. Tilgangen til denne informasjonen vil imidlertid være begrenset til det personen frivillig velger å dele videre. Det er problematisk at politiet kan avlese nedskrevne tanker. Personer bør kunne tenke og reflektere fritt, uten å frykte at deres «tanker» kan bli tatt ut av kontekst og brukes mot dere ved en senere anledning. Datatilsynet fryktet at dataavlesing kunne fungere som en form for «tankepoliti» der folk blir straffet for tanker de har nedskrevet, men ikke planlegger å gjennomføre. [207]

Personvernet er videre en viktig forutsetning for en opplyst og aktiv demokratisk debatt. [208] Frykten for overvåking kan medføre endret atferd hos befolkningen i bruken av tjenester eller kommunikasjon.[209] Folk kan vegre seg for å fremsette ytringer om kontroversielle tema. Dette har ikke et demokratisk samfunn godt av, ettersom et demokrati bør være mangfoldig og inkluderende og legge til rette for en åpen og fri meningsutveksling.

[206] Prop. 68 L (2015-2016) side 243.
[207] Klikk (2016).
[208] NOU 2022:11 side 32.
[209] NOU 2022:11 side 33.

4.2 Sikkerhetsutfordringer ved gjennomføringen av dataavlesing

4.2.1 Skader på drift og programvarer

Det er flere utfordringer knyttet til politiet sin fremgangsmåte under gjennomføringen av dataavlesing. Et teknologisk innbrudd kan for eksempel påføre maskinen virus og skader på drift og programvarer.

En annen konsekvens kan være at når en datamaskin er svekket, vil den også være mer sårbar for hacking fra andre. Dette er særlig praktisk ved hardware- eller softwarebaserte avlyttingsløsninger som skal kommunisere data tilbake til politiet over for eksempel kommunikasjonsnettverk som radio, Internettet eller GSMnet.[210] Politiet må sette inn tiltak for at andre ikke skal fange opp data politiet skal ha, eller å overta eller kontrollere avlyttingsløsningen.[211] Vår identitet er blitt digitalt i dag og smarttelefoner og datamaskiner håndterer store mengder av personlig informasjon. Det er en fare knyttet til at denne informasjonen fanges opp av andre utenforstående. Denne informasjonen kan brukes til å begå kriminalitet, stjele vedkommende sine verdier, misbruke identiteten eller brukes som et pressmiddel mot vedkommende.

Det kunne tenkes at det er mindre inngripende å innhente informasjon via en tredjeperson, slik det kreves ved kommunikasjonskontroll. Denne fremgangsmåten å foreta kommunikasjonskontroll anses som «mindre» inngripende både sikkerhetsmessig og i forhold til hensynet til personvern, ettersom det finnes et mellomledd mellom den mistenkte og politiet. Det er likevel viktig å påminne at behovet for dataavlesing oppsto som følge av kryptering som gjorde at dataene ikke lenger var lesbare hos teletilbyder, og dette uansett ikke var noe reelt alternativ ved dataavlesing.

4.2.2 Bruk av «trojaner»-basert på erfaringer fra Tyskland

Ved innføringen av dataavlesing kom Teknologirådet med flere innspill basert på erfaringer fra Tyskland. Det vises til tysk politi sin utvikling og bruk av en trojaner som visste seg å ha sikkerhetssvakheter, som ble varslet av den tyske hackergruppen Chaos Computer Club (CCC).

Dårlig kryptering og autentisering gjorde det mulig for CCC å få tilgang til alle maskiner som var infisert av trojaneren og ta over kontrollen av disse, både politiet og overvåkningsobjektet

[210] Prop. 68 L (2015-2016) side 266-267.
[211] NOU 2009:15 side 248.

sine systemer.[212] Det var utfordringer knyttet overvåking fra andre lands sikkerhetsmyndigheter fordi kommunikasjon mellom trojaneren og tysk politi gikk via servere i USA.[213] Videre kunne kontrolløren av trojaneren installere og kjøre hvilket som helst program på den infiserte maskinen, også funksjonaliteter som gikk utover landets lov. CCC oppdaget at det dessuten var gjort bevisste tekniske forsøk på å skjule funksjonaliteten til trojaneren.[214]

Det er risiko knyttet til at skadelige programvarer aktiverer mikrofon eller videokamera på vedkommende datamaskin.[215] Slik risiko bør kunne kontrolleres eller programvaren innrettes på en slik måte at dette ikke skjer. Metodekontrollutvalget påpeker at skjult overvåking, som aktivering av mikrofon eller webkamera, vil være i strid med norsk lov. Det er likevel ikke gitt garantier mot misbruk av disse mulighetene. Proposisjonen om dataavlesing mangler en redegjørelse i forhold til disse sikkerhetsutfordringene. Proposisjonen kunne med fordel hatt mer søkelys på verktøy som brukes, funksjonaliteten og hvordan disse bør innrettes for å ivareta samfunnet og borgernes rettsikkerhet.

4.3 Legalitetsprinsippet

Videre er det en klar utfordring at bestemmelsen om dataavlesing er teknologinøytral. Lovgiver har valgt en generell utforming, ut fra et ønske om at dataavlesingen skal kunne gjennomføres uavhengig av ny teknologisk utvikling.[216] Det er bra at bestemmelsen er teknologinøytral for at den skal ha et dynamisk innhold og anvendes med den stadige utviklingen i samfunnet.

Den vage definisjonen av dataavlesing, kan imidlertid stille metodebruken i dårlig lys i forhold til legalitetsprinsippet i Grunnloven § 113. Legalitetsprinsippet står særlig sterkt ved ileggelse av straff jf. Grunnloven § 96. Lovhjemmelen skal ivareta hensynet til forutberegnelighet og hindre vilkårlig maktmisbruk. Gode grunner taler for at politiets bruk av dataavlesing burde vært underlagt skranker gjennom beskrivelser av fremgangsmåter for å hindre maktmisbruk.

På den annen side ville en spesifikk angivelse av fremgangsmåtene medføre at politiets fremgangsmåter kunne kommet utenfor lovens anvendelsesområde. Legalitetsprinsippet stiller strenge krav til tolkning av straffebestemmelser. Baksiden ved en teknologinøytral

[212] Teknologirådet, Innspill til Prop. 68 L (2015-2016) side 2.
[213] Teknologirådet, Innspill til Prop. 68 L (2015-2016) side 2.
[214] Teknologirådet, Innspill til Prop. 68 L (2015-2016) side 3.
[215] NOU 2009:1 side 83.
[216] Prop. 68 L (2015-2016) side 270.

lovbestemmelse er at politiet kan benytte seg av nyere og mer avanserte dataprogrammer, som kanskje åpner for mer enn det lovhjemmelen gir tillatelse til.

4.4 Kontrollutfordringer

4.4.1 Teknologinøytral lovhjemmel

Begrensningene ved dataavlesing følger teknisk sett bare av hva slags informasjonssystem det dreier seg om og funksjonaliteten til program eller maskinvaren som benyttes.[217]

Det er enklere å kontrollere metodebruken ved kommunikasjonskontroll, fordi lovbestemmelsene har flere «begrensninger». Når politiet for eksempel skal lokalisere kommunikasjonsanlegg må dette skje «ved hjelp av teknisk utstyr» som politiet benytter og kan ikke innhente lagrede samtaledata fra tilbydernes basestasjon.[218] Kontroll av kommunikasjon må også knytte seg til identifisering av anlegg, og ikke personer.

Ved kommunikasjonskontroll, varer metodebruken mens samtalen pågår. Dataavlesing krever en «kontinuerlig» tilstedeværelse over tid i datasystemet. [219] Tidsaspektet og omfanget av metodebruken gjør det vanskelig å kontrollere metodebruken i praksis.

4.4.2 «Reell» kontroll med politiets skjulte etterforskningsmetoder?

Den manglende kontakten med mistenkte i saker om skjult tvangsmiddelbruk kan gjøre det vanskelig for advokaten å forberede et godt forsvar uten å høre siktedes versjon av saken. Da er det viktig at andre tilsynsmyndigheter kan ivareta siktedes rettssikkerhet ved å kontrollere politiets metodebruk.

Utvalget for kommunikasjonskontroll har i år, 2023, meddelt Justisdepartementet det utvalget ser på som «alvorlig rutinesvikt» og «bakenforliggende mangler ved dagens regelverk og kontrollsystem».[220] KK-utvalget påpeker blant annet at de mangler verktøy for å etterprøve politiets rapporteringer. Deres etterkontroll av politiets metodebruk er i dag begrenset til dokumentgjennomgang og tilsyn.

[217] Prop. 68 L (2015-2016) side 225.
[218] Se punkt 3.2.2.2 ovenfor.
[219] Prop. 68 L (2015-2016) side 265.
[220] Kontrollutvalget for kommunikasjonskontrolls særskilte innberetninger for 2023 side 2.

Det er bare politiet som har innsikt i metodebruken under dataavlesing. Utenforstående vil ikke ha mulighet til å vurdere om gjennomføringen av dataavlesingen har ivaretatt hensynet til privatliv og personvern. Da vil også informasjon om misbruk og svakheter ved gjennomføringsmåten heller ikke oppdages. Det kan være fare for at politiet vil unngå å rapportere om «mangler» eller at opplysningene ikke behandles etter gjeldende regelverk eller brukes til etterforskning i andre saker enn innhentet formål. I en sak fra Spesialenheten ble det avdekket at KK-utvalgets kritikk og pålegg om sletting av nærståendesamtaler ikke ble fulgt opp av Agder politidistrikt.[221] Dette understreker viktigheten av at kontrollorganer bør kunne føre en reell kontroll med politiets bruk av skjulte etterforskningsmetoder.

Etter EMDs rettspraksis vil eksistensen av gode kontrollordninger være relevant i en vurdering av om inngrep er forholdsmessig.[222] KK-utvalget bør økes med mer teknologisk kompetanse for å ha bedre forutsetninger for å vurdere om fremgangsmåtene er innenfor «rammene av lov og instrukser» jf. kommunikasjonskontrollforskriften § 14 første ledd. Da vil KK-utvalget ha bedre grunnlag for å vurdere om de tekniske fremgangsmåtene som er benyttet, ligger innenfor rammene i strpl. § 216 p første ledd annet punktum og fjerde punktum.

[221] Kontrollutvalget for kommunikasjonskontrolls særskilte innberetninger for 2023 side 1.

[222] Roman Zakharov v. Russia avsnitt 232.

5 OPPSUMMERING AV OPPGAVEN

Tema for avhandlingen er politiets bruk av skjulte tvangsmidler under etterforskning og deres forhold til personvern og rettsikkerhet. Jeg har belyst dette temaet gjennom en analyse av lovbestemmelsene om kommunikasjonskontroll og dataavlesing. Analysen har særlig påpekt hva som skiller disse metodene fra hverandre. I kapittel 3.1 har jeg forklart den historiske bakgrunnen for lovbestemmelsene. Jeg har gjort rede for hva kommunikasjonskontroll og dataavlesing innebærer som skjulte etterforskningsmetoder og deres fremgangsmåter for innhenting av informasjon i kapittel 3.2. Deres materielle og prosessuelle vilkår er presentert i kapittel 3.3 og 3.4. Kontrollsystemet for begge regelsettene er felles og er presentert generelt i kapittel 3.5.

Et siktemål med oppgaven var også å vurdere kommunikasjonskontroll og dataavlesing i lys av hensynet til personvern og rettsikkerhet. Dette er gjort i kapittel 4 der jeg har sett på en rekke personvern og rettssikkerhetsutfordringer. Dataavlesing byr på større personvern og rettssikkerhetsproblemer fordi det følger få begrensninger av lovbestemmelsen siden den er teknologinøytral og objektet for avlesing «datasystem» favner vidt. Metodebruken gir «kontinuerlig» overvåking av et datasystem og kan fordre «innbrudd» dersom det er nødvendig for å skaffe tilgang. I tillegg er det vanskelig å kontrollere metodebruken i praksis, fordi teknologiens funksjonalitet er bredt og det stilles få krav til denne måten å innhente informasjon på. Dette er momenter som samlet taler for at dataavlesing er mer inngripende enn kommunikasjonskontroll som skjult tvangsmiddel.

6 Litteraturliste

Lover, forskrifter og konvensjoner

Grunnloven	Lov 17.mai 1814. Kongenrikets Norges Grunnlov.
Den Europeiske menneskerettighetskonvensjonen	Europarådets konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter 4.november 1950.
Menneskerettsloven	Lov. 21.mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett.
SP-konvensjonen	Den internasjonale konvensjonen om sivile og politiske rettigheter 16. desember 1966.
Straffeprosessloven	Lov 22.mai 1981 nr. 25 om rettergangsmåten i straffesaker.
Straffeloven	Lov. 20 mai. 2005 nr. 28 om straff.
Politiloven	Lov 4. august 1995 nr. 53 om politiet.
Kommunikasjonskontrollforskriften	Forskrift 09.september 2016 nr. 1047 om kommunikasjonskontroll, romavlytting og dataavlesing.

Forarbeider og stortingsdokumenter

NOU 1997: 15	Etterforskingsmetoder for bekjempelse av kriminalitet Delutredning II.
NOU 2003: 18	Rikets sikkerhet straffelovkommisjonens delutredning VIII (Lund-utvalget).
NOU 2013:9	Ett politi-rustet til å møte fremtidens utfordringer (Politianalysen)
NOU 2004: 6	Mellom effektivitet og personvern – Politimetoder i forebyggende øyemed (Politimetodeutvalget).
NOU 2007: 2	Lovtiltak mot datakriminalitet- Delutredning II (Datakrimutvalget).

NOU 2009: 15	Skjult informasjon – åpen kontroll. Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker.
NOU 2009: 1	Individ og integritet- Personvern i det digitale samfunnet.
NOU 2016: 24	Ny straffeprosesslov
NOU 2022: 11	Ditt personvern- vårt felles ansvar. Tid for en personvernpolitikk
Ot. prp. nr. 64 (1998-1999)	Endringer i straffeprosessloven og straffeloven m v (etterforskningsmetoder m v).
Ot.prp.nr. 60 (2004-2005)	Endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet).
Ot.prp.nr. 40 (1991-1992)	Endringer i straffeprosessloven (telefonavlytting i narkotikasaker).
Prop. 68 L (2015-2016)	Endringer i straffeprosessloven mv. (skjulte tvangsmidler).
Prop. 147 L (2012-2013)	Endringer i straffeprosessloven mv. (behandling og beskyttelse av informasjon).
Innstil. 343 L (2015-2016)	Innstilling fra justiskomiteen om Endringer i straffeprosessloven mv. (skjulte tvangsmidler).

Rettspraksis

Rt. 1984- 1076 (307-84)

HR- 2013- 00881-A

Rt. 2009 s. 394

Rt. 2010 s. 1232

KK-2002-2-Rt. 2005-199

Avgjørelser fra Den Europeiske Menneskerettighetsdomstolen

47143/06	Roman Zakharov v. Russia 4. desember 2015.
62498/11	R.E v. The United Kingdom 27. oktober 2015.

8691/79 Malone v. The United Kingdom 02. august 1984

9063/80 Gillow v. The United Kingdom 14. september 1987

6538/74 Sunday times v. The United Kingdom 6. november 1980

58170/13
62322/14
24960/15 Big Brother Watch and others v. The United Kingdom 25. mai 2021.

Juridisk litteratur

Aall (2018) Aall, Jørgen. Rettsstat og menneskerettigheter: *en innføring i vernet om individets sivile og politiske rettigheter etter den norske forfatning og etter den europeiske menneskerettighetskonvensjonen*. 5. utgave, Bergen: Fagbokforlaget, 2018.

Bruce (2018) Bruce, Ingvild og Geir Sunde Haugland. *Skjulte tvangsmidler.* 2. utgave, Oslo: Universitetsforlaget, 2018.

Graver (2003) Graver, Hans Petter. «Internasjonale konvensjoner som rettskilde». *Lov og rett*. Vol. 42, hefte 8 (2003) s. 468- 489. [Lest i Idunn.no].

Skoghøy (2002) Skoghøy, Jens Edvin A. «Norske domstolers lovkontroll i forhold til inkorporerte menneskerettigheter» *Lov og rett*. Vol. 41, hefte 6 (2002). s. 337- 354. [Lest i Idunn.no].

Andre kilder

Teknologirådet. *Innspill til Prop. 68 L – skjulte tvangsmidler.* 2016. https://cdn.innocode.digital/teknologiradet/uploads/2018/05/Innspill_Prop68L_250516.pdf

Kontrollutvalget for kommunikasjonskontroll. *Årsrapport 2016.* https://d71tvbqpkyamo.cloudfront.net/KK-utvalget/Publikasjoner/Årsrapporter/rsrapport2016.pdf

Kontrollutvalget for kommunikasjonskontroll. *Årsrapport 2021.* https://d71tvbqpkyamo.cloudfront.net/KK-utvalget/Publikasjoner/Årsrapporter/KKutvalget_årsrapport_2021-3.pdf

Kontrollutvalget for kommunikasjonskontroll. *Kontrollutvalget for kommunikasjonskontroll må sikres reell kontrollmulighet av politiets skjulte metodebruk*. 2023. https://d71tvbqpkyamo.cloudfront.net/KK-utvalget/Publikasjoner/Særskilte-innberetninger/Særskilt-innberetning-2023-02-17.pdf

Datatilsynet. *Hva er personvern?* 2019.
https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/

Regjeringen. Hva er *personvern?* 2019.
https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/hva-er-person-vern/id448290/

Klikk.no. *Det er ikke forbudt å tenke onde tanker*. 2016
https://www.klikk.no/teknologi/det-er-ikke-forbudt-a-tenke-onde-tanker-4362093