Kontroll med politiets bruk av dataavlesing

- *Særlig med inngrepets forholdsmessighet*

Kandidatnummer: 20

Antall ord: 14 921

JUS399 Masteroppgave

Det juridiske fakultet

UNIVERSITETET I BERGEN

8. juni 2020

Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstilling

Temaet for avhandlingen er kontroll med politiets bruk av dataavlesing for å etterforske alvorlig kriminalitet. Den overordnede problemstillingen er hvorvidt kontrollen med politiets bruk av dataavlesing tilstrekkelig effektivt sikrer at slike inngrep i privatlivet ikke er uforholdsmessige, jf. Grunnloven (Grl.) § 102 første ledd og Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 8.[1]

Dataavlesing er et skjult tvangsmiddel som ble innført i norsk rett ved lov nr. 54/2016, i straffeprosessloven (strpl.) kapittel 16 d.[2] Metoden *dataavlesing* omfatter en rekke ulike fremgangsmåter for å skaffe tilgang til informasjon som produseres, lagres eller kommuniseres i eller mellom elektroniske informasjonssystem.[3] *Tvangsmidler* er «offentlige myndigheters virkemidler som innebærer at borgerne tvinges til å gjøre eller tåle noe som medfører et kvalifisert inngrep i deres personlige integritet».[4] Videre kan *skjulte tvangsmidler* defineres som «lovregulerte politimetoder som brukes uten at den metodebruken retter seg mot kjenner til det, og som det også i ettertid kan besluttes utsatt eller unnlatt underretning om».[5] Politiet og Politiets sikkerhetstjeneste (PST) har adgang til å bruke dataavlesing både som ledd i alminnelig etterforskning etter strpl. §§ 216 o og 216 p, og i avvergende øyemed etter strpl. § 222 d. I tillegg kan PST, som eneste politimyndighet, benytte dataavlesing for å forebygge visse typer straffbare handlinger etter politiloven § 17 d.[6]

Reglene om dataavlesing må forstås i lys av og praktiseres i tråd med grunnleggende verdier, slik disse kommer til uttrykk i våre konstitusjonelle rammer og internasjonale forpliktelser.[7] Ifølge Grl. § 102 første ledd og EMK artikkel (art.) 8 nr. 1 har enhver *rett til respekt for sitt privatliv*. Statens myndigheter har etter Grl. § 92 og EMK art. 1 en plikt til å *respektere* og *sikre* denne og andre menneskerettigheter. At staten skal respektere rettigheten innebærer

[1] Lov 17. mai 1814 Kongerikets Norges Grunnlov; Europarådets konvensjon 4. november 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter
[2] Lov 22. mai 1981 nr. 30 om rettergangsmåten i straffesaker
[3] Prop. 68 L (2015-2016) s. 224
[4] Bruce og Haugland (2018) s. 16
[5] Bruce og Haugland (2018) s. 15
[6] Lov 4. august 1995 nr. 53 om politiet
[7] Bruce og Haugland (2018) s. 20

blant annet at den selv ikke skal foreta uberettigede inngrep i borgernes rett til privatliv, for eksempel ulovlig overvåking. Samtidig plikter staten å sikre at enkeltpersoners rettigheter og interesser gis en effektiv beskyttelse, eksempelvis ved å etablere et system for avdekking, oppklaring og straffeforfølgning av kriminelle handlinger.[8] Det er dette staten tar sikte på ved å tillate dataavlesing og andre skjulte tvangsmidler for å bekjempe alvorlig kriminalitet. For å sikre enkeltes rettigheter kan det imidlertid være nødvendig å gjøre inngrep i andres rettigheter. Ved bruk av skjulte tvangsmidler vil staten selv gripe inn i den eller de tvangsmiddelbruken går utover sin rett til respekt for privatliv. Retten til respekt for privatlivet kan derfor ikke være – og er heller ikke – absolutt.[9]

Interessen av å få oppklart kriminelle handlinger kan imidlertid ikke rettferdiggjøre ethvert inngrep.[10] I bestrebelsene for å beskytte borgerne mot kriminalitet må staten holde seg innenfor visse rammer. Høyesterett har lagt til grunn at det kan gripes inn i retten til privatliv dersom tiltaket har tilstrekkelig *hjemmel*, forfølger et legitimt *formål* og er *forholdsmessig*.[11] De samme vilkårene følger av EMK art. 8 nr. 2. For at bruken av dataavlesing skal være rettmessig, må disse vilkårene være oppfylt.[12]

1.2 Aktualitet

Den 4. februar i år kom PST med den nasjonale trusselvurderingen for 2020. De mest alvorlige truslene er spionasje mot regjeringen, Stortinget og Forsvaret, digital kartlegging og sabotasje av kritisk infrastruktur, samt terrorangrep utført av enkeltpersoner. Det ble i vurderingen påpekt at stadig mer av trusselaktiviteten rettet mot grunnleggende nasjonale interesser foregår i det digitale rom.[13] Skjult tilstedeværelse på digitale arenaer kan være avgjørende for politiets evne til å drive tilfredsstillende kriminalitetsbekjempelse, og dermed også for opprettholdelsen av en stabil samfunnsorden.[14] For norsk politi er det krevende å møte denne trusselen effektivt, samtidig som de rettsstatlige krav og begrensninger respekteres.

[8] *X og Y mot Nederland* [J], no. 8978/80, ECHR:1985 avsnitt 23; Bruce og Haugland (2018) s. 39
[9] Dok.nr. 16 (2011-2012) s. 178; Rt. 2015 s. 93 A avsnitt 60
[10] NOU 2016: 24 s. 121
[11] Rt. 2014 s. 1105 A avsnitt 28
[12] Bruce og Haugland (2018) s. 35
[13] PST (2020) s. 3
[14] Prop. 68 L (2015-2016) s. 26; Bruce og Haugland (2018) s. 21–22

Det endrede trusselbildet i kombinasjon med den teknologiske utviklingen har medført et betydelig behov for mer inngripende tvangsmidler.[15] Politiet og påtalemyndigheten har derfor gjennom flere lovendringer de siste 20 årene fått stadig større adgang til å benytte skjulte tvangsmidler i sitt arbeid.[16] Eksempler på skjulte tvangsmidler er kommunikasjonskontroll, romavlytting, kameraovervåking, teknisk sporing, beslag, ransaking og dataavlesing.

Dataavlesing er det nyeste skjulte tvangsmiddelet politiet kan benytte seg av for å bekjempe kriminalitet. Metoden brukes for å innhente informasjon fra informasjonssystemer som brukes av mistenkte. Det er nyttig både når den kriminelle handlingen er gjort *i* det digitale rom og når den er gjort *ved hjelp av* det digitale rom. Med andre ord kan dataavlesing bidra til å fremskaffe bevis i de tilfeller der den mistenkte har benyttet seg av et informasjonssystem ved planleggingen eller gjennomføringen av en forbrytelse. Metoden kan for eksempel fange opp elektroniske spor der en mobiltelefon har blitt brukt til å kjøpe utstyr for å begå en terrorhandling, eller der en datamaskin har blitt brukt til å laste ned overgrepsbilder av barn.

Behovet for å bekjempe slik og annen alvorlig kriminalitet står, som alt antydet, i et spenningsforhold til den mistenktes rett til respekt for sitt privatliv etter Grl. § 102 og EMK art. 8. Feilaktig bruk av skjulte tvangsmidler kan få alvorlige konsekvenser, både for den inngrepet går utover og for et demokratisk samfunn som helhet. Til tross for dette har Den europeiske menneskerettighetsdomstolen (EMD) gitt medlemsstatene stor grad av frihet til selv å bestemme hvilke skjulte tvangsmidler de ønsker å tillate.[17] Samtidig stiller EMD strenge krav til forholdsmessigheten av de konkrete inngrep som gjøres, blant annet ved krav om rettssikkerhetsgarantier som er egnet til å verne borgerne mot vilkårlige inngrep og maktmisbruk.[18] Behovet for vern mot vilkårlighet og misbruk er særlig sterkt i tilfeller der politiet kan foreta inngrep i kommunikasjon direkte, uten å måtte gå veien om en teletilbyder, slik som ved dataavlesing.[19]

EMD vektlegger særlig eksistensen av et effektivt kontrollsystem.[20] Med «kontrollsystem» menes alle enkeltmomenter og kontrollmekanismer som fører kontroll med politiets bruk av skjulte tvangsmidler.[21] I Norge finnes det et helt sikkerhetsnett som skal sørge for kontroll

[15] NOU 2016: 24 s. 203–204 med videre henvisning
[16] Bruce og Haugland (2018) avsnitt 1.2
[17] *Roman Zakharov mot Russland* [GC], no. 47143/06, ECHR:2015 avsnitt 232
[18] *Klass mfl. mot Tyskland* [P], no. 5029/716, ECHR:1978 avsnitt 49; Bruce og Haugland (2018) s. 48
[19] *Roman Zakharov* avsnitt 270
[20] *Roman Zakharov* avsnitt 165
[21] NOU 2009: 15 s. 130

med politiets bruk av dataavlesing, men de viktigste er domstolene og Kontrollutvalget for kommunikasjonskontroll (KK-utvalget).[22]

Det fremgår av KK-utvalgets årsrapport fra 2018 at politiet, Kripos og Økokrim benyttet dataavlesing i én sak i 2017 og i syv saker i 2018.[23] Tallene for 2019 er i skrivende stund ikke publisert. Statistikken gir imidlertid inntrykk av at bruk av dataavlesing vil øke vesentlig de neste årene.

I juni 2019 sendte KK-utvalget et brev til Riksadvokaten som forklarte at det har vært vanskelig for dem å kontrollere hvorvidt politiets bruk av dataavlesing skjer i samsvar med loven.[24] Bakgrunnen for dette er at politiets protokollføring ikke omfatter de elementer som KK-utvalget anser nødvendige for en tilfredsstillende kontroll. Dette er problematisk, ettersom et velfungerende og grundig kontrollsystem må betraktes som en forutsetning for en målrettet og riktig bruk av de skjulte tvangsmidlene.[25]

1.3 Presisering og avgrensing av temaet

Ettersom dataavlesing er en relativt ny og omdiskutert metode, inviterer temaet til mange spennende problemstillinger. Det er derfor nødvendig å presisere og avgrense oppgavens rammer nærmere.

Formålet med avhandlingen er å vurdere om kontrollen med måten dataavlesing gjennomføres på, den *fremgangsmåten* politiet benytter, i tilstrekkelig grad sikrer at slike inngrep i privatlivet ikke er uforholdsmessige. Det avgrenses mot kontroll med politiets etterfølgende behandling av opplysningene som innhentes ved dataavlesingen, herunder taushetsplikt, bruk, oppbevaring, sperring og sletting av informasjon. Avgrensingen foretas da feilbehandling her kan utgjøre egne typer inngrep i privatlivet, som det av formatmessige grunner ikke er rom for å behandle.[26]

[22] Prop. 68 L (2015–2016) s. 18
[23] KK-utvalgets årsrapport 2018 s. 12
[24] KK-utvalget (2019)
[25] Bruce og Haugland (2018) s. 132
[26] NOU 2009: 15 s. 52; Behandling av opplysninger fra skjult tvangsmiddelbruk er dessuten behandlet av Bruce og Haugland (2018)

Det er kontrollen med politiets fremgangsmåte ved bruk av *dataavlesing* KK-utvalget nylig har fremhevet som særlig utfordrende.[27] Av denne grunn avgrenses det mot redegjørelse av andre og nærliggende skjulte tvangsmidler, som kommunikasjonskontroll, hemmelig ransaking og beslag.

At avhandlingen skal ta for seg kontrollen med *politiets* bruk av dataavlesing i etterforskningssporet, innebærer videre at det avgrenses mot kontroll med etterretnings-, overvåkings- og sikkerhetstjenestene (EOS-tjenestene). I dag er disse tjenestene hovedsakelig lagt til Etterretningstjenesten, PST, Nasjonal sikkerhetsmyndighet og Forsvarets sikkerhetsavdeling.[28] Kontrollen med disse tjenestene er tillagt EOS-utvalget, og er regulert i EOS-kontrolloven.[29] Avgrensingen foretas da kontrollen med disse tjenestene har syntes å fungere tilfredsstillende.[30] Det vil likevel rettes et sideblikk mot EOS-utvalget der det er relevant.

1.4 Metodiske spørsmål og fremstillingen videre

I avhandlingen redegjør jeg for, analyserer og vurderer gjeldende rett på området. Det foretas dermed en rettsdogmatisk analyse. Et naturlig utgangspunkt er å redegjøre for hva metoden dataavlesing innebærer, slik den kommer til uttrykk i strpl. §§ 216 o og 216 p. Dette gjøres i kapittel 2.

Straffeprosesslovens regler gjelder bare «med de begrensninger som er anerkjent i folkeretten eller følger av overenskomst med fremmed stat», jf. strpl. § 4 første ledd. EMK gjelder som norsk lov etter menneskerettsloven (mrl.) § 2 nr. 1.[31] Det innebærer at EMK ved motstrid går foran bestemmelser i annen lovgivning, jf. mrl. § 3. Den internasjonale konvensjonen om sivile og politiske rettigheter (SP) art. 17 spiller også en rolle i denne sammenheng, men kravene samsvarer med eller er mildere enn kravene etter EMK art. 8.[32] I det videre tar jeg derfor utgangspunkt i EMK.

[27] KK-utvalgets årsrapport 2018; KK-utvalget (2019)
[28] EOS-utvalgets årsrapport 2018 s. 3
[29] Lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste
[30] NOU 2009: 15 underavsnitt 11.12.2; Prop. 68 L (2015–2016) s. 18
[31] Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett
[32] Bruce og Haugland (2018) s. 39

Da menneskerettighetene ble grunnlovsfestet i 2014 var EMK en inspirasjonskilde. Konstitusjonskomiteen påpekte derfor at EMDs fortolkning av konvensjonen ville få betydning for tolkningen av menneskerettighetsbestemmelsene i Grunnloven.[33] I ettertid har Høyesterett flere ganger uttalt at Grl. § 102 skal tolkes i lys av den tilsvarende bestemmelsen i EMK art. 8.[34] Det opereres imidlertid med et skille mellom rettspraksis før og etter 2014.[35] EMD-praksis før 2014 vil ha større prejudikatsverdi ved grunnlovstolkningen nettopp fordi Grunnloven kapittel E er inspirert av EMKs rettighetsbestemmelser slik disse da fremsto. Etter 2014 vil ikke praksisen ha samme prejudikatsverdi, fordi det er Høyesterett som etter vår forfatning har ansvaret for å tolke, avklare og utvikle Grunnlovens menneskerettsbestemmelser.[36] Det er likevel ikke tvil om at så lenge Norge er bundet av EMK, vil EMDs tolkning av bestemmelsene spille en viktig rolle.[37] I avhandlingens kapittel 3 rettes det dermed stort fokus på EMD-praksis for å se hvilke materielle og prosessuelle krav domstolen stiller til skjult tvangsmiddelbruk.

I kapittel 4 ser jeg på hvordan de materielle forholdsmessighetskravene er gjennomført i straffeprosessloven, mens det i kapittel 5 rettes et særlig fokus på de prosessuelle garantier som er gitt for å sikre at slike inngrep i privatlivet ikke er uforholdsmessige. Kapittel 5 fokuserer særlig på kontrollsystemet, og eventuelle svakheter ved dette. En viktig oppfølgning av å konstatere mangler er å komme med forslag til en løsning. I kapittel 6 vil jeg derfor foreta en rettspolitisk analyse, der jeg forsøker å komme med forslag til hvordan de ulike aktørene i kontrollsystemet kan føre tilsyn med inngrepets forholdsmessighet på en mer effektiv og tilfredsstillende måte.

Det som særpreger rettskildebildet innenfor det valgte emnet, er blant annet at forrige evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler er fra 2009.[38] Da var ikke dataavlesing et tillatt tvangsmiddel etter norsk rett, og mye kan ha forandret seg siden dette. På tidspunktet var Metodekontrollutvalget av den oppfatning at det var grunn til å gjøre grep for å forbedre kontrollen i slike saker, men kom i liten grad med konkrete lovforslag for

[33] Dok.nr. 16 (2011–2012) s. 90; Innst. 186 S (2013–2014) s. 20
[34] HR-2017-2015-A (46) med videre henvisninger
[35] Rt. 2015 s. 93 A avsnitt 57; HR-2016-2554-P; Aall (2018) s. 48
[36] Grl. § 88; Rt. 2015 s. 93 A avsnitt 57
[37] Aall (2018) s. 50
[38] NOU 2009: 15

å gjøre dette. Justis- og beredskapsdepartementet fant det dermed ikke naturlig å behandle temaet i Prop. 68 L (2015–2016).

Det finnes heller ikke praksis fra verken EMD eller Høyesterett som direkte gjelder dataavlesing. EMD-praksis utgjør likevel en viktig kilde ved besvarelsen av problemstillingen ettersom prinsippene og uttalelsene som fremgår av praksisen i stor grad må anses sammenfallende, uavhengig av hvilket skjult tvangsmiddel det dreier seg om.[39] Den rettspraksis som gjennomgås vil dermed gjelde slike tilgrensende tvangsmidler.

En gjennomgående metodisk utfordring er også at problemstillingen er lite behandlet i juridisk teori. For å forstå hvilke problemer som oppstår i praksis, benyttes det i stor grad uttalelser og årsrapporter fra forskjellige ekspertorganer. Tilgangen til slik informasjon forutsetter imidlertid at den er offentliggjort, noe som blant annet KK-utvalgets siste årsrapport ikke er før innleveringen av avhandlingen.

[39] Prop. 68 L (2015–2016) s. 238; *Klass mfl*. avsnitt 50

2 Nærmere om dataavlesing

2.1 Bakgrunn

Behovet for dataavlesing oppsto særlig som følge av fremveksten av krypteringsløsninger.[40] Kryptering er en matematisk metode som går ut på å omforme data slik at den elektroniske informasjonen blir uforståelig for utenforstående, enten det gjelder skrift, bilder eller lyd.[41] Aktører som Google, Apple og WhatsApp krypterer store deler av sine tjenester automatisk.[42] Denne trenden er et svar på høyst reelle sikkerhetsproblemer, som overvåking, hacking, identitetstyveri og spionasje.[43] Bruk av kryptering skyldes derfor i hovedsak et legitimt ønske hos tilbydere av nett- og kommunikasjonstjenester og deres brukere om å beskytte informasjon.[44] Kryptering kan for eksempel være helt nødvendig for å sikre konfidensialiteten til helseinformasjon, banktransaksjoner, personlige bilder og meldinger.

Kryptering kan imidlertid også være et nyttig verktøy for kriminelle.[45] Ettersom krypteringen vanligvis skjer idet informasjon sendes eller lagres, er informasjonen uforståelig for politiet ved bruk av kommunikasjonskontroll eller ransaking og beslag.[46] Forsøk på å finne krypteringsnøkkelen krever betydelige ressurser i form av tid, datakraft og kompetanse, og det er beskjedne muligheter til å lykkes innenfor et så kort tidsrom at informasjonen forblir etterforskningsmessig relevant.[47] Den teknologiske utviklingen har dermed medført at elektroniske bevis blir mindre tilgjengelig enn før.[48]

Dataavlesing bidrar til å løse dette problemet fordi metoden gjør at politiet kan avlese informasjonen mens den befinner seg i datasystemet og før den krypteres.[49] Fremgangsmåten beskrives nærmere i avsnitt 2.4. Det foretas først en gjennomgang av objektet for dataavlesing og hvilke opplysninger som kan avleses.

[40] Prop. 68 L (2015–2016) s. 259–260
[41] Datatilsynet (2012)
[42] Teknologirådet (2016) s. 1
[43] Teknologirådet (2016) s. 2
[44] Bruce og Haugland (2018) s. 248
[45] Bruce og Haugland (2018) s. 248
[46] Prop. 68 L (2015–2016) s. 259
[47] Prop. 68 L (2015–2016) s. 260; Bruce og Haugland (2018) s. 248
[48] Prop. 68 L (2015–2016) s. 249 (Kripos' uttalelse)
[49] Bruce og Haugland (2018) s. 248

2.2 Objektet

Objektet for dataavlesing er et «datasystem», jf. strpl. § 216 o første ledd første punktum. Det tilsier at systemet som avleses må være basert på informasjonsteknologi. Ifølge forarbeidene skal «datasystem» forstås som enhver innretning, bestående av maskinvare og data, som foretar behandling av data ved hjelp av dataprogrammer.[50] Uttrykket er teknologinøytralt, i den forstand at også innretninger for databehandling som ikke brukes til kommunikasjon omfattes.[51] Presiseringen i forarbeidene tilsier at det som kan avleses, må være et fysisk objekt (maskinvare) som har et digitalt element knyttet til seg (programvare), og at det kan brukes til å foreta behandling av data.[52] Datasystemer som kan avleses er for eksempel smarttelefoner, datamaskiner, digitale klokker, kopimaskiner og GPS-utstyr.

I tillegg til datasystemer kan også «brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester» avleses, jf. strpl. § 216 o fjerde ledd. Det tilsier at politiet kan avlese informasjon som fremgår av kontoer mistenkte har på internett, for eksempel Facebook, Google og iCloud. Ifølge forarbeidene innebærer det at e-posttjenester og skylagringstjenester kan avleses.[53] Ved å åpne for avlesing av brukerkontoer unngår politiet å være avskåret fra effektiv kontroll dersom mistenkte bruker slike tjenester via mange ulike nettverkstilkoblinger og flere forskjellige datasystemer.[54]

2.3 Opplysningene

Dataavlesing kan brukes til å avlese «ikke offentlig tilgjengelige opplysninger» i et datasystem, jf. strpl. § 216 o første ledd første punktum. Ordlyden tilsier at metoden retter seg mot digital informasjon som ikke enhver har tilgang til. Av § 216 o fjerde ledd andre punktum fremgår det at avlesingen kan omfatte kommunikasjon, elektronisk lagrede data og «andre opplysninger om bruk av datasystemet eller brukerkontoen». Henvisningen til «andre opplysninger» gjør at ordlyder favner vidt. En naturlig språklig forståelse av ordlyden tilsier at politiet er gitt anledning til å avlese alle typer opplysninger om hva som for eksempel har blitt skrevet, søkt på, sendt eller mottatt i datasystemet eller brukerkontoen. Forarbeidene

[50] Prop. 68 L (2015–2016) s. 270
[51] Prop. 68 L (2015–2016) s. 270
[52] Bruce og Haugland (2018) s. 252
[53] Prop. 68 L (2015–2016) s. 270
[54] Prop. 68 L (2015–2016) s. 270

inneholder en oppregning av hvilke opplysninger som kan avleses.[55] Her nevnes blant annet lydstrømmer, bilder- og videostrømmer, tastetrykk, innholdet på lagringsmedium og data som genereres på internett. De opplysninger politiet kan få tilgang til, begrenses kun av hva slags informasjonssystem det dreier seg om og funksjonaliteten til program- eller maskinvaren som benyttes.[56]

Ved dataavlesing har det ingen betydning hvorvidt informasjonen er lagret eller om den er under overføring mellom en avsender og en mottaker.[57] Det er fordi informasjonen avleses *i datasystemet*, i motsetning til kommunikasjonskontroll hvor den innhentes hos teletilbyder.[58] Metoden skiller seg også fra hemmelig ransaking og beslag av elektroniske opplysninger, ved at den åpner for å samle inn den informasjonen som genereres i datasystemet fortløpende og over tid.[59] Dette inkluderer også opplysninger som verken lagres eller kommuniseres i datasystemet, for eksempel inntastinger som brukeren foretar og tekster som opprettes uten at de lagres.[60] Slik informasjon får ikke politiet tilgang til gjennom andre skjulte metoder. Dataavlesing er dermed ment å kompensere for disse metodenes reduserte effektivitet.[61]

2.4 Fremgangsmåten

Straffeprosessloven inneholder ingen forklaring på hva som menes med «avlesing». Av forarbeidene fremgår det at dataavlesing ikke er et entydig juridisk begrep, og at det heller ikke betegner noen klart avgrenset teknologisk fremgangsmåte.[62] Det er dermed uklart hvilke fremgangsmåter som kan brukes for å få tilgang til opplysningene.

Det følger av strpl. § 216 p første ledd andre punktum at avlesingen kan foretas «ved hjelp av tekniske innretninger, dataprogram eller på annen måte». Den tekniske innretningen eller dataprogrammet kan installeres «i datasystemet og i annen maskinvare som kan knyttes til datasystemet», jf. femte punktum. Eksempler på annen maskinvare er tilbehør som tastaturer, hodetelefoner og minnepinner.[63] I forarbeidene presiseres det at det kan tilrettelegges for

[55] Prop. 68 L (2015–2016) s. 224
[56] Bruce og Haugland (2018) s. 257
[57] Bruce og Haugland (2018) s. 256–257
[58] Bruce og Haugland (2018) s. 248
[59] Prop. 68 L (2015–2016) s. 264
[60] Fredriksen (2018) s. 252
[61] Prop. 68 L (2015–2016) s. 267
[62] Prop. 68 L (2015–2016) s. 224
[63] Prop. 68 L (2015–2016) s. 271

innhenting av informasjon gjennom dataavlesing ved at det installeres *maskinvare* eller *programvare på* eller *i* et elektronisk informasjonssystem.[64]

Maskinvare er fysiske komponenter som installeres på eller i mistenktes datasystem.[65] Forarbeidene nevner key-logging som eksempel, som innebærer at det monteres et utstyr i tastaturet som avleser tastetrykkene.[66] Politiet kan også montere utstyr i hodetelefoner eller mikrofoner som benyttes av mistenkte for å kommunisere over internett, slik at de kan fange opp lydsignaler.[67] En tillatelse til dataavlesing gir imidlertid ikke politiet adgang til å manipulere datasystemet for å drive andre former for skjult overvåking.[68] Det er for eksempel ikke tillat å aktivere mikrofon eller kamera tilknyttet datasystemet for å fange opp lyd og bilder.[69] Slik overvåking må hjemles i reglene for romavlytting og skjult kameraovervåking.

Med programvare menes her et program som politiet installerer i datasystemet, og som gjør dem i stand til å hente ut informasjon.[70] Dette gjøres typisk ved at politiet utnytter et sikkerhetshull i datasystemet eller sender en e-post som inneholder et skjult vedlegg med det aktuelle programmet (ofte kalt en *trojaner*).[71] Programvare kan installeres i informasjonssystemet ved elektronisk innbrudd, mens plassering av maskinvare forutsetter fysisk tilgang.

Dataavlesing er en form for *overvåking*, da det uansett fremgangsmåte er tale om systematisk innsamling, oppbevaring og anvendelse av opplysninger.[72] Det går imidlertid et skille mellom skjulte tvangsmidler som benyttes som ledd i strategisk og målrettet overvåking, og de som brukes som ledd i generell masseovervåking. Førstnevnte vil være rettet mot bestemte enkeltpersoner eller kommunikasjonsmidler, for eksempel som ledd i strafferettslig etterforskning.[73] Masseovervåking er derimot overvåking av tilfeldige og ubestemte personer. Dataavlesing faller inn under førstnevnte kategori.

[64] Prop. 68 L (2015–2016) s. 224
[65] NOU 2009: 15 s. 248
[66] Prop. 68 L (2015–2016) s. 247
[67] NOU 2009: 15 s. 248
[68] Prop. 68 L (2015–2016) s. 264
[69] Prop. 68 L (2015–2016) s. 264
[70] NOU 2009: 15 s. 247
[71] NOU 2009: 15 s. 247
[72] *Uzun mot Tyskland* [J], no. 35623/05, ECHR:2019 avsnitt 49–53
[73] Kjølbro (2020) s. 979

Selv om straffeprosessloven setter noen rammer for gjennomføringen, styres rammene i stor grad også av teknologiutviklingen, herunder hva som er mulig å få til teknologisk og operativt med de ressurser som er tilgjengelig.[74] Lovgiver har med dette gitt politiet et vidt teknologisk og skjønnsmessig spillerom hva gjelder metodens fremgangsmåte. Dette er uvanlig for skjult tvangsmiddelbruk, på grunn av det strenge legalitetsprinsippet på området.[75] Det var imidlertid et bevisst valg fra lovgivers side, da det ikke var ønskelig at loven skulle hindre politiet i å møte utfordringene som den teknologiske utviklingen medfører.[76]

Spørsmålet i det videre er hvilke krav og begrensninger Grunnloven og EMK stiller til skjult tvangsmiddelbruk.

[74] KK-utvalgets årsrapport 2018 s. 17
[75] Bruce og Haugland (2018) kap. 1; se avhandlingens avsnitt 3.3
[76] Prop. 68 L (2015–2016) s. 264

3 Krav og begrensninger etter Grunnloven og EMK

3.1 Retten til respekt for sitt privatliv

For at dataavlesing skal utgjøre en krenkelse av retten til respekt for privatliv, må det først påvises at myndighetene har foretatt et inngrep i det vernet av privatlivet som Grl. § 102 og EMK art. 8 tilbyr.[77] Spørsmålet er dermed om dataavlesing er å anse som et inngrep i retten til privatliv, slik at vilkårene for inngrep må overholdes om krenkelse skal unngås.

Det følger av Grl. § 102 første ledd første punktum at enhver har «rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon». Etter EMK art. 8 nr. 1 har enhver «rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse». Bestemmelsene har et sammenfallende innhold, og som nevnt innledningsvis må Grl. § 102 forstås i lys av EMK art. 8.[78] I det følgende vil det dermed tas utgangspunkt i EMK art. 8. Tilsvarende krav vil gjelde etter Grl. § 102, dersom ikke annet er sagt.

«Privatliv» er bestemmelsens hovedbegrep, og er vidt nok til å konsumere begrepene familieliv, hjem og korrespondanse.[79] Rekkevidden av begrepet «privatliv» lar seg ikke definere helt presist, og EMD har heller ikke funnet det nødvendig å prøve.[80] Det vanlige er å avklare rekkevidden ved å se på hva som har blitt omfattet i praksis, heller enn å finne en løsning gjennom ordlydstolkning.[81]

Kjernen i rettigheten er at alle skal ha en privat sfære der de er beskyttet mot innblanding fra det offentlige eller andre utenforstående. Bestemmelsen reflekterer ulike personvern- og rettssikkerhetshensyn. Behovet for en privat sfære er en del av kjernen i den personlige integritet, og den sentrale begrunnelsen for *personvernet*.[82] Personvern innebærer en frihet fra

[77] Bruce og Haugland (2018) s. 40
[78] Innst. 186 S (2013–2014) s. 20; Dok.nr. 16 (2011–2012) s. 90; HR-2017-2015-A avsnitt 46 med videre henvisninger
[79] Aall (2018) s. 214
[80] *Niemietz mot Tyskland* [J], no. 13710/8816, ECHR:1992 avsnitt 29
[81] Høstmælingen (2012) s. 223
[82] Bruce og Haugland (2018) s. 23

å bli observert eller overvåket i den private sfæren, og til å ha kontroll over opplysninger om en selv.[83] *Rettssikkerhet* knytter seg til beskyttelse av den personlige integritet og selvbestemmelsesrett mot overgrep og vilkårlighet fra myndighetenes side, samt krav til å kunne forutberegne sin rettsstilling og forsvare sine rettslige interesser.[84]

I *Klass mfl. mot Tyskland* uttalte EMD at hemmelig overvåking av borgere karakteriserer en politistat, og at slike tiltak kun er lovlige i den grad de skjer i tråd med vilkårene i EMK art. 8 nr. 2.[85] Det er nettopp på grunn av det kvalifiserte inngrepet dataavlesing utgjør i mistenktes personlige integritet, at metoden er å anse som et tvangsmiddel.[86] Det kan dermed ikke være tvil om at dataavlesing utgjør en krenkelse av retten til respekt for privatliv, slik at vilkårene for inngrep må overholdes om krenkelse skal unngås.

Det primære formålet med EMK art. 8 er å beskytte individet mot *uberettigede* inngrep fra offentlige myndigheter, ikke å tvinge staten til å avstå fra inngrep i sin helhet.[87] Inngrep må med andre ord skje innenfor visse rammer. Inngrepet – her dataavlesingen – må være «i samsvar med loven», den må være «nødvendig i et demokratisk samfunn» og den må ivareta et eller flere av nevnte anerkjennelsesverdige formål, jf. EMK art. 8 nr. 2.

3.2 Formål

Formålet med dataavlesingen må være av «hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter», jf. EMK art. 8 nr. 2. I alminnelig etterforskning benyttes dataavlesing særlig «for å forebygge [...] kriminalitet». Formålene er uansett formulert tilstrekkelig bredt til å dekke de fleste tilfeller der staten har behov for å foreta inngrep i de beskyttede rettigheter, noe som gjør at dette vilkåret sjeldent skaper problemer i praksis.[88] De vage formålsbegrensingene gjør imidlertid siste skanse – kravet til forholdsmessighet – desto viktigere.[89]

[83] Bruce og Haugland (2018) s. 23 med videre henvisninger
[84] Bruce og Haugland (2018) s. 26
[85] *Klass mfl.* avsnitt 42–43
[86] Se definisjonen av «tvangsmidler» i avsnitt 1.1
[87] *X og Y* avsnitt 23; Kjølbro (2020) s. 887
[88] Kjølbro (2020) s. 850
[89] Aall (2018) s. 151

3.3 Lov

Dataavlesingen må være «i samsvar med loven», jf. EMK art. 8 nr. 2. Vilkåret gir uttrykk for legalitetsprinsippet, som innebærer at staten ikke kan gjøre inngrep i borgernes rettigheter uten grunnlag i lov. Konvensjonens lovbegrep omfatter både formell lov, ulovfestet rett og alminnelige rettsprinsipper.[90] For norsk retts vedkommende følger lovskravet av Grl. § 113. Det norske lovskravet er strengere, ettersom inngrep må ha grunnlag i formell lov eller provisorisk anordning.[91]

Legalitetskravet medfører i denne sammenhengen at inngrepet må ha tilstrekkelig hjemmel i nasjonal lovgivning og at hjemmelen må være forenlig med «the rule of law».[92] «The rule of law» innebærer at loven må tilfredsstille visse kvalitetskrav: Den må være tilgjengelig og forutsigbar.[93] I *Roman Zakharov mot Russland* påpekte EMD at henvisningen til forutsigbarhet naturligvis ikke betyr at en person skal kunne forutse når myndighetene sannsynligvis vil overvåke ham, slik at han kan tilpasse sin oppførsel deretter.[94] Kravet må forstås slik at den nasjonale loven må være tilstrekkelig klar til å gi innbyggerne en adekvat indikasjon på under hvilke omstendigheter offentlige myndigheter kan foreta slike tiltak.[95] Utover dette trer individets innrettelsesbehov i bakgrunnen til fordel for et maktfordelings- og kontrollhensyn.[96] Reglene må være tilstrekkelig klare til å sikre kontrollmulighet og slik forebygge myndighetsmisbruk.[97]

EMD har flere ganger uttalt at det er nær sammenheng mellom lovskravet og nødvendighetskravet, ettersom loven må sikre at hemmelige overvåkingstiltak kun foregår når det er «nødvendig i et demokratisk samfunn», og da særlig ved at loven sørger for adekvate og effektive garantier mot misbruk.[98]

[90] *Kruslin mot Frankrike* [J], no. 11801/85, ECHR:1990 avsnitt 29
[91] Aall (2018) s. 115
[92] *Roman Zakharov* avsnitt 228
[93] *Roman Zakharov* avsnitt 228
[94] *Roman Zakharov* avsnitt 229
[95] *Roman Zakharov* avsnitt 229
[96] Aall (2018) s. 117
[97] *Roman Zakharov* avsnitt 230
[98] *Roman Zakharov* avsnitt 236

3.4 Forholdsmessighet

3.4.1 Innledning

Inngrepet må være «nødvendig i et demokratisk samfunn», jf. EMK art. 8 nr. 2. Ordlyden tilsier at dataavlesingen må være tiltrengt for å ivareta demokratiske verdier. Domstolen deler kravet til nødvendighet i to kumulative undervilkår: Inngrepet må motsvare et presserende samfunnsbehov («a pressing social need») *og* det må være proporsjonalt i forhold til det legitime formålet som forfølges («proportionate to the legitimate aim pursued»).[99] Ifølge EMD må hemmelig overvåking av borgerne være strengt nødvendig («strictly necessary»).[100] At inngrepet må være proporsjonalt innebærer et krav om *forholdsmessighet* mellom tjenestehandlingens mål og midlene som tas i bruk for å nå dette målet. Det som må vurderes er det samfunnsmessige eller individuelle behovet for inngrepet målt opp mot inngrepets styrke for den som rammes.[101]

3.4.2 Statens skjønnsmargin

I vurderingen av om et inngrep er nødvendig i et demokratisk samfunn, har medlemsstatene en viss *skjønnsmargin* («margin of appreciation»).[102] At staten har en skjønnsmargin innebærer at EMD i større eller mindre grad vil lytte til statens egen vurdering av nødvendigheten.[103] Medlemsstatene har også en skjønnsmargin ved valget av den spesifikke metoden som benyttes for å oppnå det legitime formålet.[104] Likevel er det EMDs oppgave å føre tilsyn med både lovgivningen og begrunnelsen for å anvende den. I *Roman Zakharov mot Russland* uttalte EMD følgende:

> *In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse.*[105]

[99] *Olsson mot Sverige* [P], no. 10465/83, ECHR:1988 avsnitt 67; Kjølbro (2020) s. 851
[100] *Klass mfl.* avsnitt 42
[101] Aall (2018) s. 153
[102] *Roman Zakharov* avsnitt 232
[103] *The Sunday Times mot Storbritannia* [P], no. 6538/74, ECHR:1979 avsnitt 59; Aall (2018) s. 154
[104] *Roman Zakharov* avsnitt 232
[105] *Roman Zakharov* avsnitt 232

Kravet til forholdsmessighet operasjonaliseres ved visse materielle forholdsmessighetskrav og prosessuelle garantier.[106]

3.4.3 Materielle forholdsmessighetskrav og prosessuelle garantier

3.4.3.1 Adekvate og effektive

EMD vurderer hvorvidt nasjonal lovgivning inneholder adekvate og effektive garantier, i motsetning til teoretiske og illusoriske, for å oppfylle kravet til at inngrep kun gjøres i den grad det er «nødvendig i et demokratisk samfunn».[107] Domstolen må være tilfreds med at det finnes slike garantier mot misbruk, «whatever system of surveillance is adopted».[108] I den forbindelse har domstolen vært opptatt av om det eksisterer effektive kontrollmekanismer på alle stadier av inngrepet.[109]

Forholdsmessigheten av inngrep i retten til privatliv avhenger dermed i stor grad av at det er etablert betryggende prosessuelle garantier – og at disse er gjennomført i praksis.[110] Hvis ikke det finnes adekvate og effektive rettssikkerhetsgarantier til beskyttelse mot misbruk, vil ikke EMD anse medlemsstaten i stand til å sikre at hemmelig overvåking kun finner sted når det er nødvendig i et demokratisk samfunn.[111] Da vil det bli statuert krenkelse av EMK art. 8.[112]

I denne vurderingen legger EMD blant annet vekt på:

> [...] *the scope and duration of the secret surveillance measures,* [...] *the authorisation procedures, the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law.*[113]

3.4.3.2 Omfanget av tiltaket

Som nevnt må nasjonal lov definere omfanget av anvendelsen av hemmelige overvåkingstiltak ved å gi innbyggerne en tilstrekkelig indikasjon på under hvilke

[106] Aall (2018) s. 152
[107] *Roman Zakharov* avsnitt 237
[108] *Klass mfl.* avsnitt 50
[109] Bruce og Haugland (2018) s. 46
[110] *Centrum för Rättvisa mot Sverige* [GC], no. 35252/0819, ECHR:2018 avsnitt 158; Aall (2018) s. 60–61
[111] *Roman Zakharov* avsnitt 302–304
[112] Kjølbro (2020) s. 961
[113] *Roman Zakharov* avsnitt 238

omstendigheter myndighetene kan ty til slike tiltak. Dette gjøres særlig ved å tydelig angi arten av lovbruddene som kan medføre slike tiltak, hvem som kan bli utsatt for det og begrunnelsen som kreves for å iverksette det.[114]

3.4.3.3 Varigheten av tiltaket

EMD har slått fast at den samlede varigheten av overvåkingstiltaket kan overlates til de relevante innenlandske myndigheters skjønn, forutsatt at det foreligger klar indikasjon i nasjonal lovgivning om hvor lenge en tillatelse kan gis for om gangen, betingelsene for å forlenge tillatelsen og under hvilke omstendigheter tiltaket ikke lenger er tillatt.[115]

3.4.3.4 Autorisering av tiltaket

EMD tar hensyn til en rekke faktorer ved vurderingen av om autorisasjonsprosedyrene er i stand til å sikre at hemmelig overvåking ikke skjer «haphazardly, irregularly or without due and proper consideration».[116] Domstolen ser særlig på myndigheten som autoriserer overvåkingen, omfanget av vurderingen og innholdet i tillatelsen.[117] Ifølge EMD er det ønskelig å overlate slik autorisering til en dommer, da det vil gi de beste garantier for uavhengighet, habilitet og en riktig prosedyre.[118] EMD har i tillegg lagt til grunn at autoriseringen normalt bør forestås av en dommer med spesiell ekspertise.[119]

Dommeren må begrunne hvorfor overvåkingen tillates.[120] Det må foreligge en rimelig mistanke mot den berørte personen, herunder at det finnes objektive holdepunkter for å mistenke personen for å planlegge, begå eller ha begått kriminelle handlinger som kan føre til hemmelige overvåkingstiltak.[121] Dommeren må også undersøke om tiltaket oppfyller kravet til «nødvendig i et demokratisk samfunn», inkludert om det står i forhold til det legitime formålet som forfølges, slik vilkåret fremgår av EMK art. 8 nr. 2.[122] Relevant i vurderingen er om formålet er mulig å oppnå med mindre restriktive midler. En slik undersøkelse forutsetter

[114] *Roman Zakharov* avsnitt 243
[115] *Roman Zakharov* avsnitt 250
[116] *Roman Zakharov* avsnitt 257
[117] *Roman Zakharov* avsnitt 257
[118] *Klass mfl.* avsnitt 55–56
[119] *Szabó og Vissy mot Ungarn* [J], no. 37138/14, ECHR:2016 avsnitt 7
[120] *Roman Zakharov* avsnitt 259
[121] *Roman Zakharov* avsnitt 160
[122] *Roman Zakharov* avsnitt 160

at domstolen får tilgang til all relevant informasjon.[123] Tillatelsen bør angi overfor hvem, hvor og hvordan inngrepet kan foregå.[124]

3.4.3.5 Tilsyn med gjennomføringen av tiltaket

Etter den nasjonale domstolen har gitt tillatelse til å foreta overvåkingen, har den ikke kompetanse til å føre tilsyn med selve gjennomføringen. Den blir heller ikke informert om resultatene av overvåkingen og har ingen mulighet til å vurdere om overvåkingen skjedde i tråd med tillatelsen. Ifølge EMD er det derfor viktig at overvåkingsmyndigheten er forpliktet til å føre journal over tiltakene, slik at tilsynsorganene som driver etterkontroll har effektiv tilgang til detaljene i tiltakene som er utført.[125] Tilsyn fra ikke-rettslige organer anses forenlig med konvensjonen, forutsatt at tilsynsorganet er uavhengig av myndighetene som utfører overvåkingen og har tilstrekkelig kompetanse til å utøve en effektiv og kontinuerlig kontroll.[126] Tilsynsorganets påvirkningskraft med hensyn til eventuelle brudd som oppdages er et viktig element for å vurdere dets effektivitet.[127] EMD vil også undersøke om tilsynsorganets virksomhet er åpen for offentlig kontroll.[128]

Tilsyn med hemmelige overvåkingstiltak kan oppstå på tre forskjellige tidspunkt: ved iverksettelse av overvåkingen, mens den utføres, og etter at den er avsluttet.[129] Når det gjelder de to første trinnene, tilsier selve arten av inngrepet at det må foregå uten den berørtes viten. Vedkommende vil derfor nødvendigvis være forhindret fra å selv kontrollere og påvirke tiltaket. Med dette gjøres det unntak fra helt sentrale rettssikkerhetsgarantier, som retten til kontradiksjon, siktedes egenkontroll og kontroll gjennom offentlighet.[130] Sjansen for at politiet og påtalemyndigheten begår feil er derfor større enn i andre sammenhenger. På bakgrunn av dette er det avgjørende at det foreligger prosedyrer som gir tilstrekkelige og likeverdige garantier for å ivareta vedkommendes rettigheter.[131] Når det gjelder det tredje og siste trinnet, etter avsluttet inngrep, er spørsmålet om effektiv kontroll tett knyttet til

[123] *Roman Zakharov* avsnitt 161
[124] *Roman Zakharov* avsnitt 264
[125] *Roman Zakharov* avsnitt 272
[126] *Roman Zakharov* avsnitt 275
[127] *Roman Zakharov* avsnitt 282
[128] *Roman Zakharov* avsnitt 283
[129] *Roman Zakharov* avsnitt 233
[130] Bruce og Haugland (2018) s. 131
[131] *Roman Zakharov* avsnitt 233

spørsmålet om underretning. Det vil selvsagt være vanskelig for vedkommende å kontrollere inngrepets lovlighet om han eller hun ikke blir gjort kjent med inngrepet.[132]

3.4.3.6 Underretning om tiltaket og tilgjengelige virkemidler

Det fremgår av *Roman Zakharov mot Russland* at *«the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers».*[133]

At vedkommende ikke blir varslet om overvåkingen så snart den er opphørt, betyr ikke i seg selv at inngrepet ikke var «nødvendig i et demokratisk samfunn». Det EMD krever er at berørte personer skal underrettes så snart det lar seg gjøre, uten å sette formålet med overvåkingen i fare etter at overvåkingstiltaket er avsluttet.[134]

Kapittelet viser at EMD har stilt krav til en rekke materielle og prosessuelle vilkår som må tilfredsstilles for at kontrollen med politiets bruk av dataavlesing tilstrekkelig effektivt skal sikre at slike inngrep i privatlivet ikke er uforholdsmessige. Spørsmålet i neste kapittel er om norsk rett har gjennomført de materielle forholdsmessighetskravene på en tilfredsstillende måte.

[132] *Roman Zakharov* avsnitt 234
[133] *Roman Zakharov* avsnitt 234
[134] *Roman Zakharov* avsnitt 287

4 Materielle forholdsmessighetskrav

4.1 Det generelle forholdsmessighetskravet

Det stilles et generelt forholdsmessighetskrav til all tvangsmiddelbruk i strpl. § 170 a. Et tvangsmiddel kan kun brukes når det er «tilstrekkelig grunn til det», jf. første punktum. Det tilsier at det må foreligge gode nok grunner for å foreta inngrepet. Politiet plikter å avstå fra avlesingen, eller avslutte den, dersom det ikke er tilstrekkelig behov for den.[135] Formuleringen innebærer med andre ord et krav til *nødvendighet.*[136] En forutsetning for at et inngrep skal være nødvendig, er også at det er *egnet* for det formål det har.[137]

Videre kan ikke tvangsmiddelet brukes når det etter «sakens art og forholdene ellers ville være et uforholdsmessig inngrep», jf. § 170 a andre punktum. Inngrepet er uforholdsmessig dersom det ikke står i forhold til det som ønskes oppnådd. Retten må dermed vurdere hvor inngripende dataavlesingen er i mistenktes privatliv. Forholdsmessigheten har betydning både for spørsmålet *om* dataavlesing kan foretas og for spørsmålet om *hvor lenge* det kan foretas.[138]

Bestemmelsen er kun et minstekrav.[139] Som vi skal se inneholder reglene om dataavlesing flere skjerpede forholdsmessighetskrav.

4.2 Mistankekravet

Straffeprosessloven § 216 o første ledd gir politiet mulighet til å foreta dataavlesing når «noen» med «skjellig grunn» mistenkes for å ha begått, eller forsøkt å begå, en straffbar handling som omfattes av bestemmelsens bokstav a og b. Dette gjelder også selv om straff ikke kan idømmes på grunn av utilregnelighet eller manglende utvist skyld, jf. § 216 o andre ledd, jf. strl. § 20 første ledd. «Noen» tilsier at politiet kan avlese enhvers datasystem.

[135] Prop. 68 L (2015–2016) s. 263
[136] NOU 2016: 24 s. 312
[137] NOU 2016: 24 s. 312
[138] Ot.prp. nr. 64 (1998–1999) s. 146
[139] Ot.prp. nr. 64 (1998–1999) s. 146

Datasystemet må imidlertid knytte seg til den personen som «mistenkes» for handlingen, og kan dermed ikke tilhøre noen som kun har informasjon om en begått kriminell handling. Mistankekravet «skjellig grunn» tilsier at det må foreligge en berettiget mistanke mot vedkommende. Det må være mer sannsynlig at den tvangsmiddelet retter seg mot har begått eller forsøkt å begå handlingen, enn at vedkommende ikke har det.[140] Med andre ord kreves det sannsynlighetsovervekt. Et slikt mistankekrav er betryggende i et forholdsmessighetsperspektiv, ettersom det hindrer at dataavlesing iverksettes ved vag mistanke.

4.3 Strafferammekravet

Den straffbare handlingen vedkommende må mistenkes for å ha begått, eller forsøkt å begå, må etter loven kunne medføre «fengsel i ti år eller mer», jf. § 216 o første ledd bokstav a. Det tilsier at bestemmelsen til den aktuelle handlingen må åpne for minst 10 års fengsel. Kravet til alvorlig kriminalitet er betryggende i et forholdsmessighetsperspektiv, da det ville virket uforholdsmessig inngripende å benytte dataavlesing på lovbrudd med lav alvorlighetsgrad. Dersom handlingen er utøvet som ledd i aktivitetene til en organisert kriminell gruppe, vil dataavlesing imidlertid kunne foretas i saker ned til fem års strafferamme. Dette fordi strafferammen i slike saker kan forhøyes med «inntil det dobbelte», jf. straffeloven (strl.) § 79 c.[141]

Straffeprosessloven § 216 o første ledd bokstav b åpner også for å tillate dataavlesing for enkelte lovbrudd som medfører særlige etterforskningsmessige utfordringer.[142] Utfordringene knytter seg gjerne til at den kriminelle virksomheten ofte er godt organisert og utført på måter som gjør den vanskelig å avdekke.[143] Dette er handlinger eller forsøk på handlinger som rammes av strl. § 121 (etterretningsvirksomhet mot statshemmeligheter), § 123 (avsløring av statshemmeligheter), § 125 (uaktsom avsløring av statshemmeligheter), § 126 (annen ulovlig etterretning), §§ 127, jf. 123 (forbund om å avsløre statshemmeligheter), § 128 første punktum (ulovlig militær virksomhet), § 129 (deltakelse mv. i voldelige sammenslutninger med politiske mål), § 136 (oppfordring, rekruttering og opplæring til terrorhandlinger), § 136a

[140] Prop. 68 L (2015–2016) s. 269; Rt. 1993 s. 1302 U
[141] Lov 20. mai 2005 nr. 28 om straff
[142] Bruce og Haugland (2018) s. 259
[143] Prop. 68 L (2015–2016) s. 268

(deltakelse mv. i en terrororganisasjon), § 232 (grov narkotikaovertredelse), § 254 (frihetsberøvelse), § 257 (menneskehandel), § 311 (fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn), § 333 (grovt heleri), §§ 337 jf. 231 eller 340 jf. 231 (hvitvasking og uaktsom hvitvasking av utbytte fra narkotikalovbrudd). I tillegg omfattes eksportkontrolloven[144] § 5 og utlendingsloven[145] § 108 femte ledd (grov menneskesmugling), jf. strpl. § 216 o første ledd bokstav b.

Det kan stilles spørsmål ved henvisningen til hvitvasking og uaktsom hvitvasking av utbytte fra simpelt narkotikalovbrudd, da slike lovbrudd kun har en strafferamme på bøter eller fengsel inntil 2 år.[146] Det følger av forarbeidene at forholdsmessighetskravet vil ha særlig betydning for adgangen til dataavlesing i saker som gjelder forbrytelser med en vesentlig lavere strafferamme enn fengsel inntil 10 år.[147] I forbindelse med kommunikasjonskontroll uttalte departementet at adgangen til å foreta skjult tvangsmiddelbruk ved mistanke om simpel narkotikaovertredelse bør beholdes som en sikkerhetsventil i de sakene det likevel er nødvendig.[148] Om tilsvarende gjelder med dataavlesing eller om dette er en redigeringsfeil, er vanskelig å si.

4.4 Indikasjonskravet

Av strpl. § 216 o tredje ledd følger det et indikasjonskrav. Kravet går ut på at tillatelse bare kan gis dersom det «må antas» at dataavlesing vil være av «vesentlig betydning for å oppklare saken». Ordlyden tilsier at metoden må forutsettes å spille en betydelig rolle for etterforskningen i saken. Vilkåret stiller krav til en viss grad av sannsynlighet for at metodebruken vil bidra med opplysninger av stor betydning for det formål som ligger til grunn for metodebruken.[149]

[144] Lov 18. desember 1987 nr. 93 om kontroll med eksport av strategiske varer, tjenester og teknologi m.v.
[145] Lov 15. mai 2008 nr. 35 om utledningers adgang til riket og deres opphold her
[146] Se Bruce og Haugland (2018) s. 260 som mener dette er en redigeringsfeil
[147] Prop. 68 L (2015–2016) s. 269
[148] Prop. 68 L (2015–2016) s. 96
[149] Ot.prp. nr. 60 (2004–2005) s. 71

Hvor stor betydning dataavlesingen har for saken spiller inn på vurderingen av hvorvidt inngrepet er nødvendig.[150] Det er rapportert om nytteverdi av dataavlesing, men antallet saker er ifølge KK-utvalget for lavt til å kunne konkludere.[151]

4.5 Subsidiaritetskravet

Det kan bare gis tillatelse til dataavlesing dersom oppklaring av saken ellers «i vesentlig grad vil bli vanskeliggjort», jf. § 216 o tredje ledd. Subsidiaritetskravet tilsier at metoden kun kan anvendes dersom andre og mindre inngripende metoder vil komme til kort. Ifølge forarbeidene er det ikke et krav at andre metoder har vært brukt uten resultat.[152] Departementet fremhever her at det kan være krevende for retten å gjøre konkrete vurderinger av hvorvidt andre tvangsmidler vil kunne gi tilfredsstillende resultater, og om dette i så fall ville vært mindre inngripende enn å benytte dataavlesing.[153] På grunn av dette understrekes viktigheten av at retten gis informasjon som er tilstrekkelig til å foreta en reell vurdering av behovet for tvangsmiddelet. Subsidiaritetskravet er en del av forholdsmessighetskravet, ved at tvangstiltakene er subsidiære til alternative, mindre inngripende tiltak.[154]

4.6 Krav til fremgangsmåten

4.6.1 Elektronisk eller fysisk innbrudd

Politiet er gitt adgang til å foreta elektronisk innbrudd i § 216 p første ledd fjerde punktum, hvor det står at de kan «bryte eller omgå beskyttelse i datasystemet dersom det er nødvendig for å kunne gjennomføre avlesingen». Adgangen til å foreta fysisk innbrudd følger av bestemmelsens sjette punktum. Her fremgår det at politiet, når retten ikke bestemmer annet, kan «foreta innbrudd for å plassere eller fjerne tekniske innretninger eller dataprogram som er nødvendig for å gjennomføre dataavlesingen». At innbruddet må være «nødvendig» viser at

[150] NOU 2016: 24 s. 312–313
[151] KK-utvalgets årsrapport 2018 s. 12
[152] Prop. 68 L (2015–2016) s. 269
[153] Prop. 68 L (2015–2016) s. 269
[154] NOU 2016: 24 s. 313

det må foretas en forholdsmessighetsvurdering. Politiet kan ikke bryte seg inn i datasystemet dersom avlesingen kan gjennomføres på annet, tilfredsstillende vis.[155]

Den tekniske gjennomføringsmåten som velges har stor betydning for hvor inngripende tvangsmiddelet er. Dette fordi det har betydning for inngrepets forholdsmessighet hvor langt inn i den private sfære tvangsmiddelet befinner seg.[156] Det vil for eksempel være mer inngripende om politiet må bryte seg inn i mistenktes hjem for å installere en maskinvare fysisk på det aktuelle informasjonssystemet, enn om de fra egne kontorer installerer en programvare i det samme systemet. Det vil også være mer inngripende om politiet får tilgang til informasjon som er lagret i et datasystem, enn informasjon som er kommunisert til andre. Informasjon som er kommunisert til andre har til en viss grad «funnet vegen ut av den personlige sfære» og er dessuten noe mottakeren av kommunikasjonen selv kunne videreformidlet til politiet.[157] På samme måte vil det nok oppleves mer inngripende om politiet avleser tastetrykk på tastaturet i sanntid, enn om de får tak i mistenktes internetthistorikk. Dette fordi man må forvente at handlinger som foretas på internett i større grad registreres og overvåkes.[158]

4.6.2 Risikoen for skade på eller misbruk av datasystemet

Krav til gjennomføringsmåten følger også av § 216 p andre ledd. Dataavlesingen skal innrettes slik at det ikke «unødig» voldes fare for driftshindring eller for skade på utrustning eller data, jf. § 216 p andre ledd andre punktum. Det er den unødvendige fare politiet plikter å unngå. Enhver fare utelukker dermed ikke dataavlesing.[159] Politiet skal også «så vidt mulig avverge fare for at noen som følge av gjennomføringen settes i stand til å skaffe seg uberettiget tilgang til datasystemet eller vernet informasjon eller til å begå andre straffbare handlinger», jf. § 216 p andre ledd siste punktum. Dette er særlig aktuelt når politiet benytter seg av sikkerhetshull i datasystemet, og utenforstående som følge av dette får tilgang til systemet.

Det er grunn til å være kritisk til at politiet benytter seg av sikkerhetshull for å skaffe innpass i systemer, ettersom det er fare for at politiet blir en betalende aktør i et omstridt

[155] Prop. 68 L (2015–2016) s. 271
[156] Bruce og Haugland (2018) s. 25
[157] NOU 2009: 15 s. 243–244
[158] Bruce og Haugland (2018) s. 24
[159] Bruce og Haugland (2018) s. 255

«gråmarked».[160] Dette fordi sikkerhetshullene i mange tilfeller vil oppdages av kommersielle aktører som tilbyr dataavlesingsteknologi. I stedet for å rapportere sikkerhetshull til programvareprodusenten, utnyttes disse sikkerhetshullene for å gi betalende aktører tilgang til andres maskiner. Det er fare for at eksterne tilbydere av programvare for dataavlesing legger inn en skjult funksjon som innhenter informasjon til andre interessenter enn norsk politi. Dette vil undergrave arbeidet med å styrke samfunnssikkerheten.[161]

Hvor stor risiko inngrepet medfører er helt sentralt for hvilke konsekvenser det har for den inngrepet går utover, og dermed også for forholdsmessighetsvurderingen.

Etter § 216 p første ledd første punktum kan dataavlesing bare utføres av personell som er «særlig skikket til det» og som utpekes av politimesteren, sjef for PST eller den som bemyndiges. At personellet som utfører avlesingen må være særlig skikket til det, tilsier at de må ha tilstrekkelig juridisk og teknologisk kompetanse til å bruke tvangsmiddelet. Dette er ifølge forarbeidene ment å forebygge og redusere risiko for skade på, eller misbruk av, datasystemene som avleses.[162]

4.6.3 Risikoen for at inngrepet rammer uskyldige

Det er kun «bestemte» datasystemer og brukerkontoer som kan avleses, jf. strpl. § 216 o fjerde ledd, noe som tilsier at gjenstanden for avlesingen må være spesifisert. I formuleringen ligger det et krav om at datasystemet eller brukerkontoen må identifiseres i politiets begjæring og rettens kjennelse.[163] Det vil begrense påtalemyndighetens skjønn til å bestemme omfanget av dataavlesingen.

Videre er det kun datasystemer eller brukerkontoer «som den mistenkte besitter eller kan antas å ville bruke» som kan avleses, jf. strpl. § 216 o fjerde ledd. Ordlyden viser viktigheten av å vurdere risikoen for at inngrepet rammer uskyldige, da dette er av stor betydning for inngrepets forholdsmessighet. Med «bruke» siktes det til den direkte bruken av for eksempel en datamaskin, og ikke serveren hos tjenesteleverandører som mistenkte bare indirekte gjør bruk av.[164] I «kan antas» ligger det ikke et krav om sannsynlighetsovervekt, men det må

[160] Teknologirådet (2016) s. 2
[161] Teknologirådet (2016) s. 2
[162] Prop. 68 L (2015–2016) s. 272
[163] Prop. 68 L (2015–2016) s. 284
[164] Prop. 68 L (2015–2016) s. 271

foreligge objektive holdepunkter for at mistenkte vil bruke det aktuelle datasystemet eller brukerkontoen.[165] At det ikke bare er den mistenktes personvern som krenkes, men også ofte utenforståendes, er en side ved dataavlesing som gjør den særlig alvorlig i et personvernperspektiv.[166] Dersom inngrepet går utover tredjepersoner, i tillegg til mistenkte, vil det gjøre at inngrepet samlet sett er desto mer inngripende. Da må det kreves forholdsvis tyngre mothensyn for å tillate avlesingen.

Forholdsmessighetskravet kommer også til uttrykk i straffeprosessloven § 216 p andre ledd første punktum. Bestemmelsen oppstiller som vilkår at dataavlesingen skal innrettes slik at det ikke «unødig» fanges opp opplysninger om andre enn mistenktes bruk av datasystemet. Kravet tilsier at politiet skal tilstrebe å ikke unødvendig fange opp informasjon om andre enn mistenkte, for eksempel familiemedlemmer eller kollegaer som bruker samme datasystem.

Dersom datasystemet som den mistenkte antas å ville bruke er tilgjengelig for «et større antall personer», kan tillatelse til dataavlesing bare gis når det foreligger «særlige grunner», jf. § 216 o tredje ledd andre punktum, jf. § 216 c andre ledd første punktum. Det tilsier at datasystemet må befinne seg på et større arbeidssted eller et offentlig sted, for eksempel et bibliotek.[167] «Særlige grunner» tilsier at det må være en spesiell grunn for å tillate dataavlesing i slike tilfeller. Kravet til «særlige grunner» skal ikke forstås så strengt at politiet ikke kan iverksette avlesingen fordi mistenkte benytter seg av et datasystem i et område hvor det oppholder seg mange utenforstående.[168] Et skjerpet krav i slike saker reduserer risikoen for at flere enn mistenkte skal bli utsatt for dataavlesingen.

Det kreves også «særlige grunner» ved kontroll av datasystemer som tilhører advokat, lege, prest eller andre som erfaringsmessig fører samtaler av svært fortrolig art, jf. § 216 c andre ledd andre punktum. Et skjerpet forholdsmessighetskrav i slike tilfeller bidrar til å opprettholde tilliten mellom borgerne og de som jobber i slike yrker.

Etter gjennomgangen i dette kapittelet kan det ikke være tvil om at Norge på tilfredsstillende vis har gjennomført de materielle forholdsmessighetskravene EMD stiller til nasjonal

[165] Prop. 68 L (2015–2016) s. 271
[166] Fredriksen (2018) s. 229
[167] Rt. 2005 s. 199 U
[168] Ot.prp. nr. 60 (2004–2005) s. 146

lovgivning. Det trekker i retning av at kontrollen med politiets bruk av dataavlesing tilstrekkelig effektivt sikrer at slike inngrep i privatlivet ikke er uforholdsmessige. Spørsmålet videre er hvorvidt det er etablert betryggende prosessuelle garantier – og om disse er tilstrekkelig effektive i praksis.[169]

[169] *Roman Zakharov* avsnitt 233

5 Prosessuelle garantier

5.1 Innledning

Som tidligere påpekt er politiets bruk av dataavlesing svært invaderende i borgernes privatliv. Den inngrepet berører skal dermed ha adgang til en effektiv kontroll, der det sikres at inngrepet begrenses til hva som er nødvendig i et demokratisk samfunn.[170] For at inngrepet skal være rettmessig må samfunnets behov for beskyttelse i form av politiets kriminalitetsbekjempelse veie tyngre enn mistenktes rett til respekt for privatliv, herunder personvern og rettssikkerhet. Hvorvidt hensynet til personvern og rettssikkerhet blir ivaretatt på en tilstrekkelig god måte, avhenger av summen av alle kontrollsystemets enkeltelementer og hvor godt disse fungerer i praksis.[171] Et effektivt kontrollsystem er nødvendig for å opprettholde rettssikkerheten og ivareta borgernes tillit til politiet og påtalemyndigheten.[172]

Det kontrollsystemet vi har for skjult tvangsmiddelbruk i Norge i dag, har vokst frem som følge av en avsløring som viste at politiets overvåkingstjeneste fra 1940–1960 drev omfattende ulovlig romavlytting og telefonavlytting.[173] I den forbindelse ble det rettet sterk kritikk mot domstolens og kontrollutvalgets kontroll med tjenesten. Heldigvis er den rettslige reguleringen og kontrollen med politiets skjulte tvangsmiddelbruk noe helt annet i dag. Det betyr imidlertid ikke at det ikke foregår regelverksbrudd i politiet.

Kontrollsystemet består av interne mekanismer og tiltak i politiet og påtalemyndigheten, samt ekstern kontroll på ulike steg i prosessen.[174] Metodekontrollutvalget har påpekt at ethvert kontrollsystem bør fange opp og sikre mot svikt eller mangler på et så tidlig stadie som mulig.[175] Intern kontroll innad i politiet og påtalemyndigheten er dermed viktig for å sikre at inngrepene ikke er uforholdsmessige. En viktig del av kontrollsystemet er også at gjeldende regulering underlegges jevnlig og kontinuerlig etterkontroll.[176] Etter Justisdepartementets syn bør det regelmessig foretas kontroll av hvordan de nye reglene praktiseres – første gang tre til

[170] *Roman Zakharov* avsnitt 232
[171] NOU 2009: 15 s. 131
[172] Teknologirådet (2016) s. 1
[173] Dok.nr. 15 (1995–1996) s. 630–689; Bruce og Haugland (2018) s. 131
[174] KK-utvalgets årsrapport 2018 s. 8
[175] NOU 2009: 15 s. 135
[176] Bruce og Haugland (2018) s. 153

fire år etter lovendringen.[177] Dette var bakgrunnen for Metodekontrollutvalgets arbeid i 2009, og en lignende gjennomgang er dermed å forvente innen kort tid. I tillegg kan spesialenheten for politisaker, Datatilsynet, Sivilombudsmannen, likestillings- og diskrimineringsombudet, kommisjonen for gjenopptakelse av straffesaker og mediene nevnes.[178] Alle vil i varierende grad kunne kontrollere politiets bruk av dataavlesing. De viktigste kontrollorganene er imidlertid domstolene, den offentlig oppnevnte advokaten, forsvareren og KK-utvalget. Derfor er det disse jeg vil fokusere på i det følgende.

I tillegg til de store personverninngrep bruk av dataavlesing utgjør, er mistenktes begrensede kontrollmulighet hovedbegrunnelsen for at det stilles strenge krav til kontrollsystemet.[179]

5.2 Mistenktes egen påvirkningsmulighet er begrenset

Dataavlesingens effektivitet er åpenbart avhengig av at mistenkte ikke er klar over bruken. Avgjørelsen om å tillate dataavlesing treffes derfor uten at den mistenkte eller andre som rammes av avgjørelsen gis adgang til å uttale seg, og kjennelsen blir heller ikke meddelt dem, jf. strpl. § 216 e andre ledd, jf. § 216 o siste ledd. Mistenkte har dermed ikke mulighet til å ta til motmæle mot politiets bruk av tvangsmiddelet, verken i forkant eller underveis i inngrepet. Med dette fratas mistenkte en av de viktigste rettssikkerhetsgarantiene: muligheten til selv å føre kontroll med at egne rettssikkerhetskrav oppfylles.[180]

Mistenkte og den som har rådighet over datasystemet har først rett på underretning når tvangsmiddelbruken er avsluttet, jf. § 216 j første ledd første punktum, jf. § 216 o siste ledd. På grunn av metodens inngripende karakter er underretningsplikten den klare hovedregel.[181] Underretning kan likevel utsettes ved rettens kjennelse dersom underretning vil være til «vesentlig skade» for etterforskningen i saken, eller en annen verserende sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller dersom hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det «strengt nødvendig», jf. § 216 j første ledd andre punktum, jf. § 216 o siste ledd. Ordlyden tilsier en høy terskel før underretning kan utsettes. Etter § 216 j første ledd fjerde punktum, jf. § 216 o siste ledd kan

[177] Ot.prp. nr. 64 (1998–1999) s. 141
[178] Bruce og Haugland (2018) avsnitt 6.7
[179] NOU 2009: 15 s. 133
[180] Bruce og Haugland (2018) s. 28
[181] Prop. 68 L (2015–2016) s. 71

retten vanligvis beslutte utsettelse for inntil 8 uker om gangen. Retten kan likevel bestemme at underretning kan unnlates helt, for eksempel dersom saken henlegges og underretning vil være til vesentlig skade for fremtidig oppklaring av saken, jf. § 216 j tredje ledd, jf. § 216 o siste ledd.

Dersom mistenkte i ettertid blir underrettet om gjennomføringen av dataavlesingen, kan vedkommende ta skritt for å få inngrepet kjent ulovlig og kreve eventuell skade gjenopprettet.[182] Er det besluttet at underretning skal utsettes eller unnlates, kan enhver uansett begjære underretning om hvorvidt han eller hun har vært undergitt dataavlesing, jf. strpl. § 216 j sjette ledd, jf. § 216 o siste ledd. Underretning skal da gis med mindre det vil være til vesentlig skade for etterforskningen i saken eller en annen verserende sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig, jf. strpl. § 216 j sjette ledd, jf. første ledd. Mistenkte har dermed en viss mulighet til selv å drive etterkontroll av inngrepet.

De prosessuelle garantiene som vil gjennomgås i dette kapittelet, er satt opp for å kompensere for den rettssikkerhetsmessige utfordringen som ligger i at mistenkte fratas muligheten til kontradiksjon og i stor grad også etterfølgende kontroll. Med dette vil jeg gjennomgå de ulike kontrollmekanismene som er satt til å føre tilsyn med politiets bruk av dataavlesing. Herunder vil det vurderes hvor effektivt og velfungerende de ulike mekanismene er i praksis.

5.3 Domstolene

5.3.1 Beslutningskompetansen

Tillatelse til dataavlesing skal gis av retten ved kjennelse, jf. strpl. § 216 o første ledd. Den klare hovedregelen er dermed at domstolen skal fatte beslutningen om hvorvidt dataavlesing skal iverksettes eller ikke. Rettens samtykke har tradisjonelt vært ansett som den viktigste rettssikkerhetsgarantien for at politiets innsamling av materiale under etterforskningen er rettmessig.[183] Dersom det «ved opphold er stor fare for at etterforskningen vil lide», kan

[182] NOU 2009: 15 s. 133
[183] Ot.prp. nr. 60 (1984–1985) s. 4

imidlertid ordre fra påtalemyndigheten tre istedenfor kjennelse av retten, jf. § 216 d første ledd første punktum, jf. § 216 o siste ledd. Påtalemyndigheten er med dette gitt hastekompetanse til å beslutte dataavlesing dersom det med høy grad av sannsynlighet vil ødelegge for etterforskningen å måtte vente på rettens tillatelse. Det er ikke tilstrekkelig at det er mest praktisk for politiet å sette i gang dataavlesingen uten først å skaffe tillatelsen.[184] Dersom påtalemyndigheten har hastekompetanse foretar retten etterkontroll så snart som mulig og senest innen 24 timer, jf. § 216 d første ledd andre punktum, jf. § 216 o siste ledd.

Domstolen fører også etterkontroll under pådømmelsen av straffesaker, der bevis innhentet gjennom skjulte tvangsmidler kan tillates eller avskjæres.[185] Det dynamiske ved domstolskontrollen gjør domstolen til en svært viktig rettssikkerhetsgarantist. Ettersom oppgaven fokuserer på hvorvidt kontrollen med politiets bruk av dataavlesing tilstrekkelig effektivt sikrer at slike inngrep ikke *er* uforholdsmessige, er det særlig domstolens forhåndskontroll som her er relevant. Som vi skal se i det følgende er det grunn til å stille spørsmål ved hvor reell denne domstolskontrollen faktisk er.

5.3.2 Inngrepets varighet

Tillatelse til dataavlesing gis for et bestemt tidsrom, som ikke må være lenger enn «strengt nødvendig», jf. § 216 f første ledd første punktum, jf. § 216 o siste ledd. Det tilsier at dataavlesing kun kan foretas så lenge det foreligger et presserende behov. Tillatelsen kan ikke gis for mer enn to uker om gangen, jf. § 216 o siste ledd første punktum. Etter § 216 f andre ledd, jf. § 216 o siste ledd skal metodebruken stanses før utløpet av fristen dersom vilkårene for kontroll ikke lenger antas å være til stede, eller dersom kontroll ikke lenger anses «hensiktsmessig». Kontrollen må sies å være hensiktsmessig så lenge den er formålstjenlig. Den vil ikke lenger være hensiktsmessig dersom mistanken avkreftes, eller det viser seg at mistenkte ikke bruker datasystemet som forutsatt.[186] Da vil avlesingen dessuten være unødvendig, og dermed uforholdsmessig.

Etter loven gjelder det ingen eksplisitte begrensninger for hvor mange ganger politiet kan begjære forlengelse av tillatelsen til dataavlesing, og dermed heller ikke for hvor lenge

[184] Bjerke, Keiserud og Sæther (2011) s. 752–253
[185] NOU 2009: 15 s. 138
[186] Bjerke, Keiserud og Sæther (2011) s. 756

kontrollen samlet kan pågå.[187] Lengden vil imidlertid spille en stor rolle for hvorvidt tvangsmiddelbruken er forholdsmessig. KK-utvalget påpekte i sin årsrapport fra 2017 at det i flere større saker utvalget har gjennomgått ikke fremkommer av begjæringene at forholdsmessigheten av den samlede tvangsmiddelbruken er vurdert.[188] I stedet for synes det som at tidligere innvilgelse av bruk av tvangsmidler brukes som del av begrunnelsen for å begjære ytterligere tvangsmiddelbruk.

5.3.3 Vurdering av forholdsmessighet

Domstolens rolle som rettssikkerhetsgarantist ved beslutninger om bruk av skjulte tvangsmidler har ved flere anledninger vært gjenstand for kritikk.[189] Det fremgår blant annet av Lund-kommisjonens undersøkelser fra 1995–1996 at tingrettene på den tiden kun foretok svært overfladiske prøvelser, at de utviste ukritiske holdninger og at de samlet sett ikke fungerte som den rettssikkerhetsgaranti de var ment å være.[190] Kommisjonen antok at dette hadde sammenheng med at dommeren hadde begrenset kunnskap om de faktiske forhold, og at han eller hun ikke hadde den oversikt som skulle til for å sette spørsmålstegn ved overvåkingstjenestens vurderinger.[191] I 2005 påpekte forsvarer John Christian Elden at han ikke var kjent med noen avgjørelser i kommunikasjonskontrollsaker hvor begjæringen ble avslått av domstolen som uforholdsmessig.[192] Ifølge ham ble det sjeldent overhodet drøftet i premissene. I 2009 foretok Metodekontrollutvalget en spørreundersøkelse angående betydningen av kommunikasjonskontroll for etterforskning.[193] Der ble det påpekt av en dommer at det var vanskelig for domstolen å foreta en reell prøving av politiets påstander, og at nesten alle begjæringer derfor ble godkjent.[194] Et gjennomgående tema i undersøkelsen var at domstolsbehandlingen langt på vei kun fungerte som en ren formalitet, på grunn av et underliggende problem med mangelfull begrunnelse og dokumentasjon.[195]

Det er fortsatt et problem at begjæringene til retten om tillatelse til skjult tvangsmiddelbruk, herunder dataavlesing, beskrives på en så generell måte at den rettslige kontroll

[187] Bruce og Haugland (2018) s. 218
[188] KK-utvalgets årsrapport 2017 s. 18
[189] Bruce og Haugland (2018) s. 142
[190] Dok.nr. 15 (1995–1996) s. 678; Bruce og Haugland s. 142.
[191] Dok.nr. 15 (1995–1996) s. 678
[192] Elden (2005)
[193] NOU 2009: 15 vedlegg 1
[194] NOU 2009: 15 s. 399
[195] NOU 2009: 15 s. 400

vanskeliggjøres.[196] Likevel tillater retten tvangsmiddelbruken i omtrent samtlige tilfeller. I 2018 ble det kun rapportert at tingretten avslo påtalemyndighetens begjæring om kommunikasjonskontroll i fire saker.[197] Om domstolen noen gang har avslått politiets begjæring om dataavlesing, og i så fall hvor mange ganger, er ikke kjent.

I Advokatforeningens årstale i 2017 påpekte Jens Johan Hjort at grunnen til at så få begjæringer avslås trolig skyldes at konsekvensene av et nei for mye kan være katastrofale. Det er politiet som presenterer faktum i saken og som begrunner sitt behov for å ta metoden i bruk. Definisjonsmakten ligger dermed hos politiet, mens et «uhåndterlig ansvar og umulige rammevilkår ligger hos advokat og dommer.»[198] Dersom dommeren avslår politiets begjæring risikerer man at politiet ikke får tilstrekkelig bevis til å straffeforfølge en person som er mistenkt for alvorlig kriminalitet. Konsekvensen av å tillate dataavlesing en gang for mye fremstår gjerne mindre, eller i hvert fall ikke like fremtredende, for dommeren.

Ved mangelfull informasjon kan det neppe foretas noen reell kontroll av hvorvidt metodebruken er eller vil være forholdsmessig. Metodekontrollutvalget stilte derfor spørsmål ved om domstolskontrollen med slike begjæringer fungerer tilfredsstillende.[199] For å bøte på problemet foreslo utvalget særlig to endringer i reglene: Forhandlingene skulle foregå muntlig og kjennelsene skulle begrunnes.[200]

5.3.4 Muntlige forhandlinger

Etter gjeldende rett skal kjennelser avsies i rettsmøte «om det er anledning til det», jf. strpl. § 52 første ledd andre punktum, jf. § 43 første ledd første punktum. Departementet fremhever i forarbeidene at dagens ordning i stor grad legger til rette for at saker om skjulte tvangsmidler blir tilstrekkelig belyst ved at dommeren eller den offentlig oppnevnte advokaten kan innkalle til muntlige forhandlinger ved behov, og at begge som regel kan få innsyn i sakens øvrige dokumenter.[201] I flertallet av landets domstoler avholdes det ikke muntlige forhandlinger ved behandling av begjæring om bruk av skjulte tvangsmidler.[202] Grunnen til dette er at muntlige

[196] KK-utvalget (2019)
[197] KK-utvalgets årsrapport (2018) s. 12
[198] Hjort (2017) s. 44
[199] NOU 2009: 15 s. 128
[200] NOU 2009: 15 avsnitt 11.9, 15.6 og 15.8
[201] Prop. 68 L (2015–2016) s. 66
[202] Bruce og Haugland (2018) s. 143

forhandlinger kan forsinke gjennomføringen av et tvangsmiddel og gjøre at påtalemyndighetens hastekompetanse brukes i større utstrekning.[203] Ifølge Marius Dietrichson i Advokatforeningens forsvarergruppe behandles slike saker som en kontorforretning av dommeren alene uten at partene er til stede.[204] Dette er en klar svakhet med systemet, da det går utover advokatens mulighet til å vareta mistenktes interesser.

5.3.5 Kjennelsens begrunnelse

Etter strpl. § 52 første ledd skal kjennelser begrunnes. Det følger av forarbeidene at rettens begrunnelse i seg selv virker skjerpende og begrenser muligheten for urettmessige og vilkårlige avgjørelser, ved at det fremtvinger en vurdering av om lovens vilkår er oppfylt.[205] Rettens begrunnelse må være slik at det er mulig å overprøve om vilkårene for tvangsmiddelet er oppfylt.[206] Det må dermed fremgå av kjennelsen hvilket faktum avgjørelsen bygger på og hvilken rettsanvendelse som er lagt til grunn.[207] Dette skal muliggjøre kontroll fra andre kontrollører.[208] Det må fremgå av rettens begrunnelse at den har vurdert om bruken av tvangsmiddelet vil innebære et uforholdsmessig inngrep, men det må ikke redegjøres for hvorfor den mener at det *ikke* vil være et uforholdsmessig inngrep å foreta tvangsmiddelet.[209]

I Metodekontrollutvalgets undersøkelse ble det påvist at rettens begrunnelser gjennomgående var knappe, og at det ikke sjelden ble anvendt standardformuleringer knyttet til hvorvidt vilkårene for tvangsmiddelbruken ble ansett oppfylt.[210] Verken utvalget eller departementet fant imidlertid grunn til å skjerpe kravet til begrunnelse ved rettens tillatelse til bruk av skjulte tvangsmidler.[211] Det ble vist til at «den offentlig oppnevnte advokaten har et særlig ansvar for å anke kjennelser som ikke holder mål».[212] Etter min mening er denne begrunnelsen noe tynn. At advokaten representerer en sikkerhet hvor kjennelsen ikke holder mål, burde ikke brukes som en grunn til å lempe på kravene som kan stilles til domstolen.

[203] Prop. 68 L (2015–2016) s. 66
[204] Stolt-Nielsen mfl. (2020)
[205] NOU 2009: 15 s. 172
[206] Ot.prp. nr. 64 (1998–1999) s. 145; Prop. 68 L (2015–2016) s. 66–67
[207] NOU 2009: 15 s. 172 med videre henvisning
[208] Ot.prp. nr. 64 (1998–1999) s. 145
[209] Ot.prp. nr. 64 (1998–1999) s. 146
[210] NOU 2009: 15 s. 172
[211] NOU 2009: 15 s. 172; Prop. 68 L (2015–2016) s. 67
[212] Prop. 68 L (2015–2016) s. 67

Videre kan det stilles spørsmål om dommerne har tilstrekkelig teknologisk kompetanse til å føre en reell kontroll med hvorvidt innholdet i politiets begjæring oppfyller lovens vilkår. Både de juridiske og de teknologiske spørsmålene som reises i overvåkingssaker kan være svært komplekse, og fordrer god forståelse for begge fagområder.[213] Dommerne må dermed ha en viss innsikt i det teknologiske aspektet av saken for å kunne vurdere tiltakets forholdsmessighet. Det kan synes som om dommerne i for stor grad stoler på politiets og påtalemyndighetens vurdering av saken, uten å foreta en selvstendig vurdering.

5.4 Advokatene

5.4.1 Offentlig oppnevnt advokat

Etter strpl. § 100 a første ledd første punktum skal retten «straks oppnevne offentlig advokat for den mistenkte» når den behandler en sak etter § 216 o. Ordlyden tilsier at oppnevningen skal skje øyeblikkelig etter at retten mottar begjæringen. Dette må ses i lys av viktigheten av at advokaten får tilstrekkelig tid til å forberede seg.[214] Offentlig advokat skal oppnevnes selv om mistenkte har forsvarer, jf. § 100 a første ledd andre punktum. Dette er fordi den opprinnelige forsvareren, på lik linje med mistenkte, ikke skal gjøres kjent med den skjulte tvangsmiddelbruken.[215]

Advokatens oppgave er å vareta den mistenktes og eventuelle tredjepersoners interesser i forbindelse med rettens behandling av begjæringen, jf. § 100 a andre ledd første punktum. Utgangspunktet er dermed at advokaten skal ha mulighet til å påvirke utfallet i saken fra starten av. I de tilfeller hvor påtalemyndigheten bruker sin hastekompetanse, innebærer det at offentlig advokat ikke blir oppnevnt før beslutningen senere forelegges retten for godkjennelse.[216] KK-utvalget har påpekt at påtalemyndigheten bruker sin hastekompetanse i omtrent 35% av tilfellene ved kommunikasjonskontroll, men foreløpig er det ikke kjent om eller hvor ofte denne blir bruk ved dataavlesing.[217] Dette vil i realiteten avskjære advokatens mulighet til å reagere i forkant, og gå på bekostning av mistenktes rettssikkerhet.

[213] NIM (2018) avsnitt 3.5
[214] Ot.prp. nr. 64 (1998–1999) s. 144
[215] Bruce og Haugland (2018) s. 136
[216] Ot.prp. nr. 64 (1998–1999) s. 144
[217] Prop. 68 L (2015–2016) s. 17

Advokaten har ikke samme mulighet til å vareta den mistenktes interesser som forsvarere ellers, ettersom vedkommende ikke kan «sette seg i forbindelse med den mistenkte», jf. § 100 a tredje ledd første punktum. At advokaten ikke kan forhøre seg med mistenkte vanskeliggjør rollen betraktelig, samtidig som den nettopp derfor er så viktig. Oppnevnelsen av offentlig advokat er nemlig ment å kompensere for den mistenktes manglende mulighet til å ta til motmæle mot politiets fremgangsmåte.[218] Vedkommende skal ivareta mistenktes interesser ved å sørge for at saken blir tilstrekkelig opplyst og påse at vilkårene for å foreta dataavlesing er oppfylt.[219] En viktig del av dette er å stille spørsmål ved om kravet til proporsjonalitet er oppfylt.[220]

Samme advokat skal også «så langt det er mulig» oppnevnes ved begjæring om forlengelse av bruken av tvangsmidler og ved begjæring om andre tvangsmidler mot mistenkte, jf. § 100 a andre ledd andre punktum. Reservasjonen «så langt det er mulig» tilsier at det kan gjøres et advokatbytte om det vil føre til forsinkelser som kan skade etterforskningen dersom man venter på den opprinnelige advokaten. Dersom samme advokat blir oppnevnt, gir det vedkommende en totaloversikt over mengden tvangsmidler som er iverksatt mot mistenkte. Det gjør vedkommende i stand til å foreta en samlet vurdering av forholdsmessigheten.[221]

Etter § 100 a andre ledd tredje punktum har den offentlige advokaten «krav på varsel til og tilstedeværelse under rettsmøte til behandling av begjæringen» og «rett til å uttale seg før retten treffer avgjørelse». Gjøres det feil etter § 100 a skal feilen vurderes etter strpl. § 343 første ledd.[222] Det vil bli ansett som et brudd på retten til kontradiksjon, noe som i praksis gjør at veien til opphevelse er kort.

5.4.2 Forsvarer

«Siktede» har rett til å la seg bistå av en forsvarer etter eget valg på ethvert trinn av saken, jf. strpl. § 94 første ledd første punktum. Stillingen som siktet inntrer først når underretning gis, jf. strpl. § 82 tredje ledd andre punktum. Forsvareren kommer dermed inn i saken når den går inn i en «åpen fase».[223]

[218] Ot.prp. nr. 64 (1998–1999) s. 82–83
[219] Ot.prp. nr. 64 (1998–1999) s. 83
[220] Ot.prp. nr. 64 (1998–1999) s. 83
[221] Bruce og Haugland (2018) s. 138
[222] Ot.prp. nr. 64 (1998–1999) s. 144
[223] NOU 2009: 15 s. 133

Forsvarere har vært viktige pådrivere for å styrke siktedes rettssikkerhet i møte med skjult tvangsmiddelbruk, særlig ved å utfordre politiets og påtalemyndighetens rettsoppfatning og fremgangsmåte.[224] Av betydning for både den offentlige oppnevnte advokatens og for forsvarerens muligheter til å ivareta mistenktes interesser, er særlig deres rett til innsyn i etterforskningsmateriealet fremhevet.[225]

5.4.3 Innsyn i etterforskningsmaterialet

Det er mye som tyder på at ordningen med offentlig oppnevnt advokat, i likhet med domstolskontroll, ikke fungerer som den rettssikkerhetsgarantien den var ment å være.[226] I 2005 påpekte Elden at det ble avgitt intetsigende eller manglende advokatuttalelser i saker hvor det åpenbart var grunn til å reise innvendinger.[227] Metodekontrollutvalgets evaluering i 2009 viste også at det fremmes få innsigelser mot påtalemyndighetens begjæringer.[228] EOS-utvalget foretok i 2005 en undersøkelse av ordningen med offentlig oppnevnt advokat ved PSTs begjæringer om skjult tvangsmiddelbruk.[229] Resultatet viste at domstolen stilte seg mer kritisk til begjæringer i saker der advokaten fremmet innsigelser, enn der den ikke gjorde det.

Problemet synes å være at advokaten ikke får tilstrekkelig innsyn i sakens dokumenter.[230] Etter § 100 a andre ledd tredje punktum skal advokaten gjøres kjent med «begjæringen og grunnlaget for den», og har «etter anmodning» krav på innsyn i sakens dokumenter med de begrensninger som følger av §§ 242 og 242 a. Grunnlaget for begjæringene er de rapporter og dokumenter som påtalemyndigheten legger frem for retten.[231] «Etter anmodning» tilsier at advokaten ikke får automatisk innsyn i sakens dokumenter. Bakgrunnen for at innsyn gis etter anmodning er at det vil kunne by på store praktiske utfordringer for politiet om advokaten skulle fått en automatisk oversendelse av alt materiale i saken.[232] Departementet fremhever

[224] Bruce og Haugland (2018) s. 151–152
[225] NOU 2009: 15 s. 134
[226] Bruce og Haugland (2018) s. 140 med videre henvisning
[227] Elden (2005)
[228] NOU 2009: 15 s. 134
[229] Bruce og Haugland (2018) s. 140 med videre henvisning
[230] Se Bruce og Haugland (2018) kap. 15 for mer om dette
[231] Rt. 2005 s. 203 U
[232] Prop. 68 L (2015–2016) s. 57

imidlertid at påtalemyndigheten må gi den offentlig oppnevnte advokaten innsyn på begjæring der vilkårene for dette er oppfylt.[233]

Advokat Knut Rognlien pekte i Tidsskrift for strafferett (2004) på at politiet vanligvis la frem en begjæring vedlagt en politirapport som var et resymé av de opplysningene politiet hadde.[234] I resymeet fremgikk det som regel bare at politiet visste noe, eller var av den klare oppfatning at noe var på en bestemt måte, uten at kildene eller nærmere opplysninger ble oppgitt. Som tidligere påpekt er det fortsatt et problem at politirapportene er for lite utfyllende. Innsyn i saksdokumentene må anses helt avgjørende for at advokaten skal kunne vurdere om vilkårene for å foreta dataavlesing er oppfylt, og med dette oppfylle sin kontrollfunksjon. Rognlien påpekte derfor at det hjelper "lite med en advokat som kontrollør, når advokaten ikke gis kontrollverktøyet, nemlig saksdokumentene."

5.5 KK-utvalget

5.5.1 Generelt

KK-utvalget (Kontrollutvalget for kommunikasjonskontroll) er et kontrollorgan oppnevnt av Kongen i statsråd i medhold av strpl. § 216 h og kommunikasjonskontrollforskriften (forskriften) kap. 2.[235] Utvalget er uavhengig og bestemmer selv sin arbeidsmåte, jf. forskriften § 18 første og andre ledd. En av utvalgets arbeidsoppgaver er å foreta etterfølgende kontroll med at politiet og påtalemyndighetens bruk av dataavlesing skjer innenfor rammen av lov og instrukser, jf. forskriften § 14 første ledd første punktum. Formålet med kontrollen er særlig å beskytte den enkeltes rettssikkerhet, jf. forskriften § 14 første ledd andre punktum. Utvalget foretar løpende kontroll, med stedlige kontroller i politidistriktene og gjennomgang av politidistriktenes, Kripos' og Økokrims kvartalsvis innrapporterte saker om dataavlesing.[236]

Metodekontrollutvalget påpekte at en av de mest avgjørende faktorer for at KK-utvalgets kontroll skal være effektiv, er at utvalget innehar høy og oppgaverelevant kompetanse og at

[233] Prop. 68 L (2015–2016) s. 57
[234] Rognlien (2004)
[235] Forskrift 9. september 2016 nr. 1047 om kommunikasjonskontroll, romavlytting og dataavlesing
[236] KK-utvalgets årsrapport 2018 s. 4

de kontrollerte og omverdenen oppfatter det slik.[237] Etter deres oppfatning hadde KK-utvalgets kontroll i etterforskningsporet både rom og behov for betydelig styrking.[238]

Etter Metodekontrollutvalgets vurdering i 2009 har det imidlertid skjedd endringer. KK-utvalgets arbeid har blitt mer tilgjengelig, blant annet ved at de har fått egen hjemmeside. Da KK-utvalgets kontrollområde i 2016 ble utvidet til også å gjelde dataavlesing, økte de årlige tildelingene fra 0,7 millioner kroner årlig, til om lag 6 millioner.[239] Det medførte at utvalget ble bedre rustet til å møte den teknologiske utviklingen og bruken av nye og mer inngripende metoder, som dataavlesing. I tillegg til en professor, to advokater, to dommere og en sorenskriver, består utvalget nå også av to sivilingeniører. Hensikten var å utvikle den tekniske siden av kontrollvirksomheten.[240] Rapporteringsinnholdet har også forbedret seg de siste årene. Nå blir det årlig offentliggjort årsrapporter som blant annet sammenfatter årets aktiviteter, statistikk, arbeidsmetode og andre særlige tema.

Politiet og påtalemyndigheten skal gi KK-utvalget de opplysninger, dokumenter, lydbåndopptak mv. om tvangsmiddelbruken som utvalget av hensyn til sin kontrollfunksjon finner nødvendig, jf. forskriften § 16 første ledd. Kontrollen tar for seg de tekniske aspektene, og hvordan dataavlesingen gjennomføres i det enkelte tilfelle. KK-utvalget er det eneste eksterne organ som kan se helheten og omfanget av dataavlesingen, noe som gjør utvalget til en svært viktig rettssikkerhetsgarantist på området.

Utvalget kan gi pålegg og stille vilkår ved brudd på politiregisterlovens regler om internkontroll og informasjonssikkerhet, jf. forskriften § 14 siste ledd første punktum.[241] For andre forhold kan de gi anmerkning, jf. forskriften § 14 siste ledd siste punktum. Utenom dette kan utvalget rette kritikk mot politiet om de finner grunn til det. Et sted KK-utvalget har funnet grunn til å rette kritikk mot politiet, er ved deres protokollføring av hvilke skritt de har tatt ved gjennomføringen av dataavlesing.

[237] NOU 2009: 15 s. 140
[238] NOU 2009: 15 s. 146
[239] KK-utvalgets årsrapport 2016 s. 8
[240] KK-utvalgets årsrapport 2018 s. 18
[241] Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten

5.5.2 Politiets og påtalemyndighetens protokollføring og kontrollen med den

5.5.2.1 Krav om protokollføring

En forutsetning for at den eksterne kontrollen skal være effektiv, er at den interne kontrollen i form av rapporteringer, fungerer tilfredsstillende.[242] I forarbeidene skriver departementet derfor at notoritet med hensyn til hvilke skritt politiet har tatt er en forutsetning for å sikre tilfredsstillende kontroll med politiets metodebruk.[243] Ettersom dataavlesing etterlater få ytre spor, er det ifølge departementet «særlig viktig at bruken av metoden dokumenteres på en måte som setter kontrollorganene i stand til å vurdere om det som er utført ligger innenfor de lovlige rammene, og så vidt mulig også til å konstatere at det ikke har blitt utført noe annet eller noe mer enn det som oppgis».[244]

For hvert tilfelle av dataavlesing skal det føres en protokoll i henhold til forskriften § 7. Opplysninger som skal fremgå av protokollen er blant annet hjemmelen for tvangsmiddelbruken, hvilke datasystem tvangsmiddelbruken rettet seg mot, når tvangsmiddelbruken startet og når den opphørte, jf. § 7 første ledd. I tillegg skal det etter andre ledd protokollføres opplysninger om blant annet hvilke typer data som er avlest, hvordan avlesingen ble gjennomført, hvilken risiko dette medførte og hvilket personell som utførte avlesingen.

Som nevnt innledningsvis sendte KK-utvalget et brev til Riksadvokatembetet i juni 2019 angående politiets rapportering ved dataavlesing. Her gjennomgikk utvalget enkelte av kravene til protokollføring gitt i forskriften § 7 andre ledd, som de mener bør være dekket i rapporten for å muliggjøre tilfredsstillende kontroll. Det var særlig elementer ved fremgangsmåten de anså å være for dårlig rapportert. Bakgrunnen for den mangelfulle rapporteringen er trolig fordi politiet får tilgang til store mengder data når de foretar dataavlesing. Å registrere og dokumentere enhver oppkopling og avkopling, samt hvilket materiale som er lastet ned, vil være svært ressurskrevende. Som påpekt av Oslo

[242] Bruce og Haugland (2018) s. 131
[243] Prop. 68 L (2015–2016) s. 272
[244] Prop. 68 L (2015–2016) s. 266

statsadvokatembeter gir metoden derfor ikke en særlig god notoritet som kan sikre mot misbruk.[245]

Ifølge forskriften § 7 andre ledd bokstav 3-5 skal det protokollføres «hvorvidt» det er benyttet tekniske innretninger, maskinvare eller programvare ved dataavlesingen, «hvorvidt» det er begått fysisk innbrudd for å gjennomføre dataavlesingen, og «hvorvidt» politiet har brutt eller omgått beskyttelse i datasystemet. I brevet påpekte KK-utvalget at begrepet «hvorvidt» inviterer til en utfyllende forklaring, ikke en kort konstatering av om noe er tilfelle eller ikke.[246]

5.5.2.2 Hvorvidt det er benyttet tekniske innretninger, maskinvare eller programvare

Når det gjelder rapportering av hvorvidt det er benyttet tekniske innretninger, maskinvare eller programvare ved dataavlesingen, jf. forskriften § 7 andre ledd nr. 3, krever utvalget beskrivelse av *hvilke* tekniske innretninger, maskinvare eller programvare som er brukt.[247] Som nevnt i avsnitt 4.6 spiller den tekniske gjennomføringsmåten en stor rolle for hvor inngripende tvangsmiddelet er i vedkommendes privatliv, og om den foreslåtte fremgangsmåten er innenfor lovens rammer. KK-utvalget har derfor påpekt at det er «vesentlig at politiet i tilstrekkelig grad informerer interne beslutningstagere og domstolene om hva man ser for seg å gjennomføre, på hvilken måte dette skal gjennomføres og de risikofaktorer som knytter seg til gjennomføringen».[248]

Videre fremhever KK-utvalget i henvendelsen til Riksadvokaten at:

> *Ved første gangs bruk av en innretning, maskinvare eller programvare må dennes egenskaper beskrives, slik at det sammen med øvrig rapportering gis mulighet til å ettergå de risikovurderinger som er gjort. Sentrale punkter er her om denne er egenutviklet, kjøpt eksternt eller er basert på for eksempel åpen kildekode. Hvis det er brukt innretninger eller programvare som er åpent eller kommersielt tilgjengelig, må det beskrives hvordan disse eventuelt er endret og tilpasset politiets bruk*.[249]

[245] Prop. 68 L (2015–2016) s. 258
[246] KK-utvalget (2019) s. 2
[247] KK-utvalget (2019) s. 2
[248] KK-utvalgets årsrapport 2018 s. 17
[249] KK-utvalget (2019) s. 2

Slik informasjon er viktig fordi det trolig vil medføre en lavere risiko, og generelt må antas å være mer betryggende, om overvåkingsverktøyet er utviklet i nasjonal regi enn om det er kjøpt på «gråmarkedet».[250]

5.5.2.3 Hvorvidt beskyttelse i datasystemet er brutt eller omgått

Ved rapportering av hvorvidt politiet har brutt eller omgått beskyttelse i datasystemet, jf. forskriften § 7 andre ledd nr. 5, bør det beskrives hvilke beskyttelsesmekanismer som eventuelt er brutt eller omgått, og om disse mekanismene permanent eller midlertidig har blitt satt ut av funksjon.[251] Begrunnelsen for en slik rapporteringsplikt er antageligvis at inngrepets forholdsmessighet vanskelig kan vurderes hvis ikke utvalget vet nøyaktig hva som har blitt gjort, og hvor store konsekvenser dette har fått, eller kan få, for vedkommende. Dersom beskyttelsesmekanismer i datasystemet er brutt eller omgått, kan dette potensielt åpne for at utenforstående tredjepersoner benytter seg av samme brudd eller omgåelse. Politiet kan «åpne en bakdør» for personer som har langt mindre aktverdige formål enn dem selv. Slik sett kan politiet bidra til at opplysningene som finnes i systemet midlertidig eller permanent også blir tilgjengelige for andre.

5.5.2.4 Hvilket personell som har gjennomført dataavlesingen

Videre bør det fremgå navn på det personellet som har gjennomført dataavlesingen, for å muliggjøre kontroll av at disse er utpekt av politimesteren som «særlig skikket», jf. strpl. § 216 p, jf. forskriften § 7 andre ledd nr. 8.[252] At rapporten utpeker personellet som har foretatt dataavlesingen med navn må anses sentralt for at utvalget skal kunne kontrollere at vedkommende har tilstrekkelig juridisk og teknologisk kunnskap. Slik kunnskap, særlig den teknologiske, er helt avgjørende for at politiet skal forstå risikoen metodebruken medfører, og dermed konsekvensene det har for den inngrepet går utover.

5.5.2.5 Hvilke risikoer datasystemet har vært utsatt for

Det punktet som trolig er mest utfordrende i praksis, er forskriften § 7 andre ledd nr. 6. Ifølge denne bestemmelsen skal det protokollføres hvilke *risikoer* datasystemet har vært utsatt for

[250] Se underavsnitt 4.6.2
[251] KK-utvalget (2019) s. 3
[252] KK-utvalget (2019) s. 3

ved dataavlesingen, og informasjon om hva som har vært foretatt for å avverge fare for driftshindring eller for skade på utrustning eller data, samt fare for at noen som følge av gjennomføringen settes i stand til å skaffe seg uberettiget tilgang til datasystemet eller vernet informasjon. I rapportene KK-utvalget har mottatt, har det kun blitt konstatert at dataavlesingen ikke medfører risiko for datasystemet eller for at farer som nevnt i bestemmelsen skal oppstå.[253] Utvalget påpeker etter dette at *enhver* bruk av dataavlesing vil ha en *iboende risiko*, som enten kan kompenseres for eller aksepteres. Hvis risikoen ved et datainnbrudd eller en installert programvareagent vurderes å være lav, forventer KK-utvalget at dette begrunnes i rapporten. Hvis risikoen i utgangspunktet er høy, men det er tatt kompenserende tiltak som senker denne til et nivå som anses å være akseptabelt, må de kompenserende tiltak beskrives.

Dette punktet gir tydelig uttrykk for forholdsmessighetskravet, nemlig at det må foretas en avveining mellom behovet for inngrepet og konsekvensene det får for den inngrepet rettes mot. Denne avveiningen kan neppe gjøres uten kjennskap til risikoen inngrepet medfører. Dersom risikoen er senket til et nivå som «anses å være akseptabelt», betyr det at konsekvensene det får for vedkommende overskygges av behovet for inngrepet i dennes privatliv. Uten informasjon om denne risikovurderingen og påfølgende avveining, er det vanskelig for KK-utvalget å kontrollere om politiet opererer i tråd med statens menneskerettslige forpliktelser.

Det kan ikke være tvil om at KK-utvalget foretar en inngående kontroll og at de er en viktig rettssikkerhetsgaranti. Som påpekt oppstår det likevel problemer i praksis. Roten til problemet, slik jeg ser det, er at utvalget ikke får tilstrekkelig informasjon fra politiets side. Det fordrer spørsmålet om utvalget med dette ikke får fanget opp, og derfor heller ikke får reagert på, potensielle overtredelser. Det blir spennende å se om politiet og påtalemyndigheten tar kritikken til seg og endrer rutinene for protokollføring av dataavlesing.

KK-utvalget har tidligere påpekt det de anser å være systematiske brudd på loven hva gjelder sletting av materiale etter overvåking. Utvalget påpekte forholdet i flere årsrapporter uten at det ble gjort noe med det. I 2018 sendte de derfor en innberetning til Justis- og beredskapsdepartementet.[254] Daværende leder i KK-utvalget, Therese Steen, skrev der at

[253] KK-utvalget (2019) s. 3
[254] KK-utvalget (2018)

utvalget frykter at vedvarende brudd på loven, på tross av gjentatt kritikk, vil svekke legitimiteten til kontrollregimet både blant de kontrollerte og i samfunnet. Dette er bekymringsverdig.

Som gjennomgangen i dette kapittelet viser er det flere problemer med muligheten til å foreta kontroll med hvorvidt politiets bruk av dataavlesing ikke er uforholdsmessig, noe som leder meg over til konklusjonen på den overordnede problemstillingen. Avslutningsvis vil jeg også forsøke å komme med forslag til hvordan de ulike aktørene i kontrollsystemet kan føre tilsyn med inngrepets forholdsmessighet på en mer effektiv og tilfredsstillende måte.

6 Avslutning

Min oppfatning er at loven langt på vei legger opp til et tilstrekkelig kontrollsystem med politiets bruk av dataavlesing. Det er likevel gjennomføringen av forpliktelsene i praksis som er «alfa og omega».[255] Jeg mener etter dette at det er grunn til å konkludere med at kontrollen med politiets bruk av dataavlesing ikke tilstrekkelig effektivt sikrer at slike inngrep i privatlivet ikke er uforholdsmessige.

Det at begjæringene til retten beskrives på en så generell måte at domstolens kontrollmulighet vanskeliggjøres, er en svakhet politiet vanskelig kommer utenom, all den tid de er i etterforskningsfasen av det straffbare forholdet. Jeg er imidlertid enig i Metodekontrollutvalgets forslag om en hovedregel om muntlige forhandlinger. Muntlige forhandlinger vil i det minste gjøre det enklere for dommeren å avklare uklare sider ved begjæringen, og vil sikre en bedre kontradiksjon. Dersom det ikke er praktisk gjennomførbart å gi advokaten automatisk innsyn i alle sakens dokumenter, vil muntlige forhandlinger også være avgjørende for advokatens mulighet til å ivareta mistenktes interesser.

Det kan potensielt være hensiktsmessig at lovgivningen endres til å differensiere mellom ulike fremgangsmåter og hvilken type informasjon som hentes ut, slik at politiet måtte spesifisert dette i begjæringen. At loven ikke skiller mellom de ulike inngrep dataavlesing kan gå ut på svekker rettens forutsetninger for å kunne vurdere hvilke inngrep som faktisk vil bli gjort, og dermed hva som er strengt nødvendig.[256] Lovgrunnlaget for dataavlesing bør utformes slik at det i større grad reflekterer inngrepene metoden reelt omfatter.[257]

Etter min mening har også forarbeidene enkelte svakheter. De fokuserer i for liten grad på risikoen dataavlesing medfører for den inngrepet går utover. Det er dermed grunn til å etterlyse en diskusjon av hvordan man sikrer effektiv kontroll med teknologien og dens bruk, og da særlig at proposisjonen bør gå lenger i å etablere robuste mekanismer for å ivareta rettssikkerheten.[258] For det første bør dataavlesingsverktøy utvikles i Norge.[259] Politiet vil da ha bedre innsikt i hva programvaren faktisk gjør, og kan være trygg på at informasjon ikke

[255] Aall (2018) s. 60
[256] NIM (2018) s. 50
[257] NIM (2020) s. 43
[258] Teknologirådet (2016) s. 3–4
[259] Teknologirådet (2016) s. 3

kommer på avveie til tredjeparter. I tillegg kan myndighetene legge inn funksjonsbegrensninger i verktøyet som benyttes. Ettersom dataavlesing kan medføre en sikkerhetsrisiko for både den som overvåkes og politiet, må verktøyene imøtekomme høye sikkerhetsstandarder og prøves gjennom sertifiseringskontroller av en egnet sikkerhetsmyndighet.[260] Jeg mener økt bevissthet rundt risikoen dataavlesing medfører er helt nødvendig for å kunne foreta en reell vurdering av inngrepets forholdsmessighet.

Ettersom loven og forarbeidene gir lite informasjon om de tekniske aspektene ved metoden og hvilken risiko de ulike fremgangsmåtene medfører, bør det stilles desto strengere krav til at beslutningstakerne selv har en høy grad av teknologisk kompetanse. Det er en særskilt utfordring at både gjennomføringen og overprøvingen av dataavlesing krever høy grad av teknologisk kompetanse, i tillegg til den juridiske. Som nevnt har KK-utvalget nylig økt sin teknologiske kompetanse ved å ansette sivilingeniører. Spørsmålet er hvordan vi kan sikre at dommeren, den offentlig oppnevnte advokaten og forsvareren har tilstrekkelig teknologisk kompetanse til å foreta en reell vurdering i saken.

Dersom domstolskontrollen ikke er reell, slik kritikerne hevder, kan det være en løsning at noen dommere ved hver domstol får særskilt opplæring og kursing i de tekniske aspektene ved dataavlesing. Det samme kunne også vært mulig for offentlig oppnevnte advokater og forsvarere. En slik innsikt ville trolig gjort dem bedre i stand til å se helheten av inngrepet, og dermed foreta en mer reell kontroll med inngrepets forholdsmessighet.

Hva gjelder problemet med mangelfull protokollføring, bør politiet i det minste innrette sin praksis etter kritikken fra KK-utvalget og kravene i kommunikasjonskontrollforskriften § 7. En mulig løsning kunne også vært utvikling og anvendelse av effektive digitaliseringsmekanismer med tilhørende analyseverktøy som kunne automatisert denne prosessen. Politiet kunne for eksempel brukt et dataavlesingsverktøy som loggfører enhver handling de foretar seg under dataavlesing. Kontrollorganene burde i så fall fått automatisk tilgang til denne loggen.[261] Et verktøy som automatisk loggfører politiets skritt ville spart politiet for mye arbeid og gitt KK-utvalget tilstrekkelig grunnlag for å kontrollere at dataavlesingen skjer innenfor lovens rammer. Samtidig ville det potensielt vært svært ressurskrevende for KK-utvalget å gjennomgå så store mengder data. I tillegg ville man stått

[260] Teknologirådet (2016) s. 4
[261] Teknologirådet (2016) s. 4

overfor andre personvernsproblemer, som omfattende og langvarig lagring av personopplysninger.

Jeg er også enig med Metodekontrollutvalget i at domstolene bør begrunne kjennelsen nærmere. Begrunnelsen mener jeg bør inkludere hvorfor retten mener at inngrepet ikke vil være uforholdsmessig. En grundigere begrunnelse fra rettens side vil gjøre det enklere for advokaten å vurdere om kjennelsen bør ankes, og for KK-utvalget å foreta en etterfølgende kontroll.

Avhandlingen er ikke ment som kritikk til verken politiet og påtalemyndigheten, KK-utvalget, dommerne eller advokatene som er involvert i slike saker, men snarere det systemet som setter samtlige i en tilnærmet umulig situasjon. Følgene av at kontrollen med politiets bruk av dataavlesing ikke tilstrekkelig effektivt sikrer at slike inngrep i privatlivet ikke er uforholdsmessige, er at det kan konstateres krenkelse av Grl. § 102 og EMK art. 8 nr. 2. Slike brudd vil påvirke tilliten til offentlige myndigheter, noe som kan virke ødeleggende for demokratiet.[262] Etter arbeidet med denne avhandlingen kan jeg derfor ikke annet enn å si meg enig med dem som etterlyser en gjennomgang av kontrollsystemet i overvåkingssaker.[263]

[262] Bruce og Haugland (2018) s. 23
[263] Se bl.a. Teknologirådet (2016) s. 3, NIM (2018) avsnitt 3.5, Advokatforeningen (2018) avsnitt 2.11

7 Kilderegister

Lover, forskrifter og konvensjoner

Grunnloven	Lov 17. mai 1814, Kongerikets Norges Grunnlov
Den europeiske menneskerettighetskonvensjonen	Europarådets konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter, 4. november 1950
SP-konvensjonen	Den internasjonale konvensjonen om sivile og politiske rettigheter, 16. desember 1966
Straffeprosessloven	Lov 22. mai 1981 nr. 30 om rettergangsmåten i straffesaker
Eksportkontrolloven	Lov 18. desember 1987 nr. 93 om kontroll med eksport av strategiske varer, tjenester og teknologi m.v.
EOS-kontrolloven	Lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste
Politiloven	Lov 4. august 1995 nr. 53 om politiet
Menneskerettsloven	Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett
Straffeloven	Lov 20. mai 2005 nr. 28 om straff
Utlendingsloven	Lov 15. mai 2008 nr. 35 om utlendingers adgang til riket og deres opphold her

Politiregisterloven	Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten
Endringslov til straffeprosessloven mv.	Lov 17. juni 2016 nr. 54 om endringer i straffeprosessloven mv. (skjulte tvangsmidler)
Kommunikasjonskontrollforskriften	Forskrift 9. september 2016 nr. 1047 om kommunikasjonskontroll, romavlytting og dataavlesing

Forarbeider og stortingsdokumenter

Ot.prp. nr. 60 (1984–1985)	Om lov om endringer i midlertidig lov 17 desember 1976 nr. 99 om adgang til telefonkontroll ved etterforskning av overtredelser av narkotikalovgivningen
Ot.prp. nr. 64 (1998–1999)	Om lov om endringer i straffeprosessloven og straffeloven mv. (etterforskningsmetoder mv)
Dok.nr. 15 (1995–1996)	Rapport til Stortinget fra kommisjonen som ble oppnevnt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere («Lund-rapporten»)
Ot.prp. nr. 60 (2004–2005)	Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)
NOU 2009: 15	Skjult informasjon – åpen kontroll. Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker

Dok.nr. 16 (2011–2012)	Rapport fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven
Innst. 186 S (2013–2014)	Innstilling fra kontroll- og konstitusjonskomiteen om grunnlovsforslag fra Per-Kristian Foss, Martin Kolberg, Marit Nybakk, Jette F. Christensen, Anders Anundsen, Hallgeir H Langeland, Per Olaf Lundteigen, Geir Jørgen Bekkevold og Trine Skei Grande om grunnlovfesting av sivile og politiske menneskerettigheter, med unntak av romertall X og romertall XXIV
Prop. 68 L (2015–2016)	Endringer i straffeprosessloven mv. (skjulte tvangsmidler)
NOU 2016: 24	Ny straffeprosesslov

Rettsavgjørelser

Fra Høyesterett

Rt. 1993 s. 1302	U
Rt. 2005 s. 199	U
Rt. 2005 s. 203	U
Rt. 2014 s. 1105	A
Rt. 2015 s. 93	A
HR-2016-2554-P	P
HR-2017-2015-A	A

Fra Den europeiske menneskerettighetsdomstolen

Klass mfl. mot Tyskland	[P], no. 5029/716, ECHR:1978
The Sunday Times mot Storbritannia	[P], no. 6538/74, ECHR:1979
X og Y mot Nederland	[J], no. 8978/80, ECHR:1985
Olsson mot Sverige	[P], no. 10465/83, ECHR:1988
Kruslin mot Frankrike	[J], no. 11801/85, ECHR:1990

Niemietz mot Tyskland	[J], no. 13710/8816, ECHR:1992
Roman Zakharov mot Russland	[GC], no. 47143/06, ECHR:2015
Szabó og Vissy mot Ungarn	[J], no. 37138/14, ECHR:2016
Centrum för Rättvisa mot Sverige	[GC], no. 35252/0819, ECHR:2018
Uzun mot Tyskland	[J], no. 35623/05, ECHR:2019

Litteratur

Aall (2018)	Aall, Jørgen, *Rettsstat og menneskerettigheter*, 5. utgave, Fagbokforlaget 2018
Bjerke, Keiserud og Sæther (2011)	Bjerke, Hans Kristian, Erik Keiserud og Knut Erik Sæther, *Straffeprosessloven, kommentarutgave*, 4. utgave, bind I og bind II, Universitetsforlaget 2011
Bruce og Haugland (2018)	Bruce, Ingvild og Geir Sunde Haugland, *Skjulte tvangsmidler*, 2. utgave, Universitetsforlaget 2018
Elden (2005)	Elden, John Christian, *Ytring*, Tidsskrift for Strafferett 02/2005. URL: https://www.idunn.no/tidsskrift_for_strafferett/2005/02/ytring (sist sjekket 6. juni 2020)
Fredriksen (2018)	Fredriksen, Steinar, *Innføring i straffeprosess*, 4.utgave, Gyldendal 2018
Høstmælingen (2012)	Høstmælingen, Njål, *Internasjonale menneskerettigheter*, 2. utgave, Universitetsforlaget 2012
Kjølbro (2020)	Kjølbro, Jon Fridrik, *Den Europæiske Menneskerettighedskonvention – for praktikere*, 5. utgave, Jurist- og Økonomforbundets Forlag 2020

Rognlien (2004) Rognlien, Knut, *Advokater som gisler i telefonavlyttingssaker*, Tidsskrift for Strafferett 2004/01
URL: http://www.lawnest.com/pres/kr-adv-gisl-tlfavl.htm
(sist sjekket 6. juni 2020)

Uttalelser, rapporter, årsmeldinger mv.

Datatilsynet (2012) Datatilsynet, «Kryptering», 24. januar 2012 (sist endret: 7. mars 2017).
URL: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/kryptering/ (sist sjekket 6. juni 2020)

Teknologiråd et (2016) Teknologirådet, «Innspill til Prop. 68 L – skjulte tvangsmidler», 25. mai 2016, URL: https://teknologiradet.no/wp-content/uploads/sites/105/2018/05/Innspill_Prop68L_250516.pdf (sist sjekket 6. juni 2020)

Hjort (2017) Hjort, Jens Johan, «Advokatforeningens årstale 2017», Kritisk juss 01/2018, URL:
https://www.idunn.no/kritisk_juss/2018/01/advokatforeningens_aarstale_2017 (sist sjekket 6. juni 2020)

KK-utvalgets årsrapport 2016, 2017 og 2018 Kontrollutvalget for kommunikasjonskontroll årsrapporter for årene 2016-2018
URL: https://www.kk-utvalget.no/rapporter.473489.no.html (sist sjekket 6. juni 2020)

KK-utvalget (2018) Kontrollutvalget for kommunikasjonskontroll, «Særskilt innberetning etter kommunikasjonskontrollforskriften § 17 – sletting av materiale fra kommunikasjonskontroll m.m.», 1. juni 2018, URL:
http://img4.custompublish.com/getfile.php/4191953.2254.abipwqtlbakapk/Vedlegg+til+%C3%A5rsrapport+-

+s%C3%A6rskilt+innberetning+1.6.2018.pdf?return=www.sivilrett.no (sist sjekket 6. juni 2020)

Advokatforeningen (2018) Advokatforeningen, «Advokatforeningens innspill til innhold i mandat for personvernkommisjon på justisfeltet», 24. juli 2018, URL: https://www.regjeringen.no/no/dokumenter/personvernkommisjon--innspill-til-mandat/id2607189/?uid=c99676cb-a8ad-45a8-aef2-8825e5cabd5c (sist sjekket 6. juni 2020)

NIM (2018) Norges nasjonale institusjon for menneskerettigheter, «Innspill til mandat til personvernkommisjon», 31. august 2018, URL: https://www.nhri.no/wp-content/uploads/2018/08/Innspill-til-mandat-til-personvernkommisjon-1.pdf (sist sjekket 6. juni 2020)

KK-utvalget (2019) Kontrollutvalget for kommunikasjonskontrolls brev til Riksadvokatembetet, «Politiets rapportering ved dataavlesing», 4. juni 2019. URL: https://mm.aftenposten.no/dokumenter/2019-10-16_V%C3%A5rt%20brev%20Radv_.pdf (sist sjekket 6. juni 2020)

PST (2020) PST, «Nasjonal trusselvurdering 2020», 4. februar 2020, URL: https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/ (sist sjekket 6. juni 2020)

NIM (2020) NIMs årsmelding, «Menneskerettighetene i Norge 2019», dokument 6 (2019–2020). URL: https://www.nhri.no/wp-content/uploads/2020/04/NIM_A%CC%8Arsmelding_2019_web.pdf (sist sjekket 6. juni 2020)

Stolt-Nielsen mfl. (2020) Stolt-Nielsen, Harald, Jan Gunnar Furulv, Andreas Bakke Foss, Frode Sætran, Trond J. Strøm og Nina Selbo Torset, «Kilder til Aftenposten: Politiet brukte skjult etterforskning mot Tom Hagen», *Aftenposten*, 28. april 2020. URL: https://www.aftenposten.no/norge/i/P9JR1J/kilder-til-

aftenposten-politiet-brukte-skjult-etterforskning-mot-tom-hagen (sist sjekket 6. juni 2020)