UiT Norges arktiske universitet

Det Juridiske Fakultet

Dataavlesing, etterforskning, og retten til privatliv

- *En analyse av vilkårene for dataavlesing etter strpl. § 216 o i lys av HR-2022-1314-A*

Johanne Svenning

Stor masteroppgave i rettsvitenskap – JUR-3901 – Mai 2024

Innhold

1 Innledning

1.1 Tema og problemstilling

Tema for avhandlingen er balansen mellom retten til privatliv og kriminalitetsbekjempelse i lys av EncroChat-dommen.[1]

Samfunnet er i konstant utvikling, og kriminalitet finner stadig nye arenaer og metoder. I en slik verden er vi avhengige av at politiet har effektive og tilstrekkelige etterforskningsmetoder for å ivareta samfunnssikkerheten.

Etterforskning er i hovedsak de undersøkelser politiet gjør for å avklare om det foreligger et straffbart forhold. Straffeprosessloven definerer ikke hva etterforskning er, men har bestemmelser om når etterforskning kan eller skal iverksettes,[2] og om hva som er etterforskningens formål.[3]

For å illustrere balansegangen mellom behovet for effektiv kriminalitetsbekjempelse og individets rett til privatliv vil oppgaven ta for seg det skjulte tvangsmiddelet dataavlesing. Det følger av straffeprosessloven[4] § 216 o at politiet kan gis tillatelse til å foreta avlesing av "ikke offentlig tilgjengelige opplysninger i et datasystem (dataavlesing)". På denne måten vil de blant annet kunne gripe inn i de mest diskré formene for kriminalitet.[5]

Alle mennesker har som et utgangspunkt rett til beskyttelse av grunnleggende rettigheter som retten til privatliv, jf. henholdsvis Grunnloven[6] § 102 og EMK[7] artikkel 8. Stater skal ikke uten videre gjøre inngrep i slike rettigheter, uten å kunne vise til legitime og tungtveiende

---

[1] HR-2022-1314-A
[2] Se Strpl. § 224.
[3] Se strpl. § 226.
[4] Lov om rettergangsmåten i straffesaker av 22. mai 1981 nr. 25.
[5] Eksempelvis grov menneskesmugling, menneskehandel, frihetsberøvelse og overgrepsbilder av barn. Disse lovbruddene kjennetegnes av at de byr på særlige etterforskningsmessige utfordringer, se Prop. 68 L (2015-2016) side 9.
[6] Lov av 17. mai 1814 Kongeriket Norges Grunnlov, heretter Grl.
[7] Europarådets konvensjon av 4. november 1950 om *beskyttelse av menneskerettighetene og de grunnleggende friheter* (Den europeiske menneskerettighetskonvensjon, heretter EMK).

behov.[8] Eksempelvis vil behovet for å bekjempe kriminalitet og sikre samfunnssikkerhet kunne være tilstrekkelig til å rettferdiggjøre inngrep overfor den enkelte.[9]

Demokratiet er avhengig av tillit fra folket for å kunne fungere. Åpenhet om hvilke metoder politiet har hjemmel for å bruke, og grensene for bruk av inngrep, er sentralt for å opprettholde en slik tillit. Borgere skal være beskyttet mot vilkårlighet ved inngrep i privatlivet, eller ved bruk av makt fra myndighetene.

Skjulte tvangsmidler utgjør i denne sammenheng et unntak til hovedregelen om åpenhet rundt bruk av inngrep. Tvangsmidler er metoder som anvendes mot en persons vilje. Felles for tiltak som omtales som "tvangsmidler" er at de er midlertidige tiltak i forbindelse med straffeforfølgning, som kan gjennomføres uten samtykke fra den personen som tiltaket rettes mot.[10] Ordinære tvangsmidler omfatter blant annet pågripelse[11] og fengsling,[12] ransakelse,[13] og beslag.[14]

Tematikken reiser spørsmål om i hvilken grad det kan gripes inn i borgeres rettigheter og interesser, hvilke vilkår som kreves for å tillate slike inngrep, og hvordan hensynet til individet veies opp mot hensynet til et effektivt rettssystem, og samfunnets sikkerhet. Disse spørsmålene skal besvares gjennom en undersøkelse av det skjulte tvangsmiddelet dataavlesing etter strpl. § 216 o.

Høyesterett berørte i 2022 bruk av materiale innhentet ved bruk av dataavlesing, fra franske etterforskningstjenester i den såkalte "EncroChat-saken".[15] Saken gjaldt primært om bevis som var innhentet av utenlandske tjenester kunne føres i en norsk straffesak. Høyesterett nevner knapt strpl. § 216 o, og foretar ikke en konkret tolkning av hjemmelen. Førstvoterendes uttalelser kan derimot ha indirekte betydning for hvordan man skal tolke vilkårene i strpl. § 216 o, og noen av hensynene som bestemmelsen bygger på. Jeg

---

[8] Se blant annet EMK art. 8 nr. 2.
[9] Prop. 68 L (2015-2016) side 14.
[10] Se Øyen (2020) *Straffeprosess* s. 195.
[11] Jf. Strpl. §§ 171, 172, 173 og 173 a.
[12] Jf. Strpl. § 184, jf. §§ 171-173a.
[13] Ransaking av hjem jf. § 192, ransaking av person, jf. § 195, for øvrig hjemles adgang til ransaking i strpl. kapittel 15.
[14] Jf. strpl. § 203, se for øvrig kapittel 16 i straffeprosessloven.
[15] HR-2022-1314-A

kommer nærmere inn på dette punkt 4.4 "Kravet til individualisering av mistankekravet og EncroChat-dommen".

1.2 Aktualitet

1.2.1 Forholdet mellom kommunikasjonskontroll og dataavlesing

Ved innføringen av dataavlesing vurderte lovgiver metoden i forhold til de tradisjonelle tvangsmidlene. Som et resultat av dette gjøres det mange sammenligninger av dataavlesing, hemmelig ransaking og kommunikasjonsavlytting.

Ett av de skjulte tvangsmidlene som politiet kan anvende er *kommunikasjonskontroll.* Metoden involverer overvåking av pågående kommunikasjon, mens dataavlesing fokuserer på tilgang til, innhenting, eller dekryptering av lagret eller sendt informasjon.

Begrepene "kommunikasjonskontroll" og "dataavlesing" kan overlappe på grunn av teknologiske utviklinger som utydeliggjør tradisjonelle grenser mellom lagring og overføring. Begge tvangsmidlene reiser viktige problemstillinger i tilknytning til personvernhensyn, og er tett regulert av hensyn til retten til privatliv.[16] En overordnet forståelse av kommunikasjonskontroll kan belyse praktiseringen og begrensningene til dataavlesing innen straffeprosessrettslige fremgangsmåter, og bidrar slik til å gi et mer helhetlig bilde av det aktuelle juridiske landskapet. Å forklare begrepene og den nærmere sammenhengen mellom dem, vil slik klargjøre grensene og den juridiske håndteringen av dem.

Kommunikasjonskontroll og dataavlesing har også enkelte likheter i juridisk kontekst. Dataavlesing innebærer typisk tilgang til, innhenting, og/eller dekryptering av lagret informasjon fra datasystemer, mens kommunikasjonskontroll innebærer overvåking av pågående kommunikasjon, typisk e-poster, tekstmeldinger, internettforbindelser eller telefonsamtaler.

[16] Se nærmere om personvernhensyn i punkt **Error! Reference source not found.**.

Begrepet "kommunikasjonskontroll" i straffeprosesslovens sammenheng omhandler bruk av avlytting og annen *kontroll* med kommunikasjonsanlegg.[17] Med "kommunikasjonsanlegg" menes enheter som kan underlegges kontroll, eksempelvis en mobiltelefon, nettbrett, datamaskin, eller bredbåndsruter.[18] Kommunikasjonskontroll innebærer i praksis hemmelig avlytting eller sporing fra politi av en mistenkt persons kommunikasjon, og reguleres av straffeprosessloven kapittel 16 a og 16 b.

Avlytting betyr i slik sammenheng at tjenestetilbyder (for eksempel Telenor) pålegges å overføre innhold fra en telefonsamtale eller brukerens internettdata til politiet, som deretter kan avlytte eller analysere innholdet.[19] Politiet kan også gi pålegg om at en samtale skal brytes eller en linje skal stenges.[20] Kommunikasjonskontroll brukes tradisjonelt i etterforskninger for å fange opp informasjon som blir overført mellom personer, og som regnes som relevant for en etterforskning av alvorlige kriminelle handlinger. Metoden begrenses av at den ikke gir tilgang til kryptert informasjon, men kun fanger opp data *etter* den er mottatt eller sendt.

Dataavlesing derimot, gir etterforskere tilgang til ukryptert informasjon. Innføringen av dataavlesing tilrettelegger for kontinuerlig overvåkning av et system, der politiet kan innhente opplysninger om aktivitet, inkludert bruk av programvare og behandling av ulike filer som ikke resulterer i data som blir lagret eller kommunisert, eller som senere gjøres utilgjengelig for politiet fordi de krypteres. Avlesing vil kunne omfatte lydstrøm tilknyttet mikrofoner og høyttalere, videostrøm, tastetrykk på mistenktes tastatur, innhold på harddisk, internettlogg og øvrig data.[21] Dataavlesing har på denne måten potensiale for å være mer inngripende enn kommunikasjonsavlytting.[22] Mistenktes tanker, assosiasjoner, og ønsker som ikke nødvendigvis skal kommuniseres, vil kunne bli gjenstand for avlesing.[23] Ved

[17] NOU 2004: 6 *Mellom effektivitet og personvern* side 24 punkt 1.3.8.8
[18] Prop. 68 L (2015-2016) side 72
[19] Årsrapport fra Kommunikasjonskontroll-utvalget 2022, side 21
[20] Jf. strpl. § 216 b første og andre ledd.
[21] Prop. 68 L (2015-2016) side 224.
[22] Dette vil jeg se nærmere på under punkt 4.3.
[23] Prop. 68 L (2015-2016) side 252.

kommunikasjonsavlytting må data sendes, lagres eller på annet vis overføres, før det kan avlyttes.

1.2.2 Forholdet til hemmelig ransaking

Lovgiver begrunnet blant annet behovet for dataavlesing i at de eksisterende skjulte tvangsmidlene har "tapt mye av sin effekt som følge av den teknologiske utviklingen".[24] Det er derfor hensiktsmessig å se nærmere på hvilke fellestrekk som foreligger mellom dataavlesing og hemmelig ransaking, og hvorfor sistnevnte metode ikke lenger regnes å være tilstrekkelig effektiv i forbindelse med bekjempelse av kriminalitet.

Straffeprosessloven § 192 hjemler politiets adgang til å foreta ransaking av mistenktes bolig, rom eller oppbevaringssted når det foreligger "skjellig grunn til mistanke" om at han har begått eller forsøkt å begå en straffbar handling. Hensikten med ransakingen må være å iverksette pågripelse, søke etter bevis eller etter ting som kan beslaglegges eller tas heftelse i.[25] Hjemmelen gir uttrykk for den alminnelige adgangen til å gjennomføre ransaking.

Ransaking innebærer søk av privat område uten eiers samtykke og utgjør dermed et tvangsmiddel. Reglene om ransaking reguleres nærmere i straffeprosesslovens kapittel 15. Kravet om "skjellig grunn til mistanke" må forstås på samme måte som ellers i loven, og krever at derfor at det må være sannsynlighetsovervekt for at mistenkte har begått eller forsøkt å begå en straffbar handling.[26]

Den alminnelige hjemmelen for ransaking suppleres av strpl. § 199 a og rettspraksis, som åpner for at politiet også kan foreta ransaking av "datasystemer eller lignende" blant annet i mistenktes hjem.[27] Der dette gjøres, kan politiet i henhold til strpl. § 199 a pålegge enhver som har befatning med datasystemet å gi opplysninger som er nødvendige for å få tilgang eller å åpne systemet ved bruk av biometrisk autentisering (eksempelvis ansiktsgodkjenning

[24] Prop. 68 L (2015-2016) side 259-260.
[25] Jf. strpl. § 192 første ledd.
[26] Jf. Rt. 2006 s. 582 avsnitt 19. Se også Prop. 68 L (2015-2016) side 87, 190, 200, og 269.
[27] Jf. strpl. § 199 a og HR-2019-610-A (Tidal Music AS) avsnitt 27.

eller fingeravtrykk).[28] Strpl. § 199 gir uttrykk for den såkalte "opplysningsplikten", og begrenses av det generelle forholdsmessighetsprinsippet i strpl. § 170 a.[29] Opplysningsplikten anses normalt ikke uforholdsmessig.[30]

Ransaking etter strpl. § 192 åpner for å foreta én ransaking, i motsetning til dataavlesing som tillater en kontinuerlig tilstedeværelse i et datasystem.[31] Både Politimetodeutvalget og Metodekontrollutvalget la til grunn at daværende norsk rett ikke åpnet for gjentatt eller fortløpende ransaking.[32] Dataavlesing var etter Justisdepartementets oppfatning nødvendig for å kunne møte utfordringene knyttet til kryptering og moderne kommunikasjonstjenester på en tilstrekkelig effektiv måte, herunder for å dekke det anførte behovet for å kunne gjennomføre fortløpende ransaking.[33]

Straffeprosessloven § 200 a utgjør en modifisering av den alminnelige regelen om varsling ved ransaking. Ifølge § 200 a kan retten av hensyn til etterforskningen avgjøre at ransaking skal skje uten at den mistenkte eller andre berørte blir underrettet på forhånd. Videre tillater § 200 a at underretning om ransakingen kan utsettes til etter etterforskningen er gjennomført, eller i særlige tilfeller utelates helt.

En av de sentrale forskjellene mellom ransaking og kommunikasjonsavlytting er hvor informasjonen som skal etterforskes befinner seg. Bestemmelsen om kommunikasjonsavlytting gir riktignok adgang til å avlytte signalstrøm mellom den enkelte brukers kommunikasjonsanlegg og tjenesteleverandørens kommunikasjonsanlegg, men dette vil ikke uten videre gi et fullstendig bilde av informasjon som utveksles mellom to personer.

Det går et skille mellom informasjon som er lagret, og informasjon som er i en overføringsfase mellom en avsender og en mottaker. Ransaking må benyttes for tilgang til

---

[28] Uttrykket "biometrisk autentisering" er ikke bundet til bestemte typer, se Prop. 106 L (2016-2017) side 9. Med "datasystem" forstås enhver innretning eller gruppe innretninger som er koblet sammen, hvorav en eller flere utfører programmert, automatisk behandling av data, se også punkt 4.2.1 nedenfor.
[29] Se mer om forholdsmessighetsprinsippet i punkt **Error! Reference source not found.** og 4.2.5 nedenfor.
[30] Se Ot.prp.nr. 40 (2004-2005) side 34.
[31] Se punkt 1.2 ovenfor.
[32] Se henholdsvis NOU 2004: 6 side 93, 94 og 98 og NOU 2009: 15 side 246.
[33] Prop. 68 L (2015-2016) side 265.

elektronisk lagret informasjon, mens kommunikasjonsavlytting må benyttes for å fange opp informasjon *under* overføring mellom ulike kommunikasjonsanlegg.[34]

Eksempelvis kan internettbaserte e-post og fildelingstjenester åpne for at flere, ved å dele tilgang til samme brukerkonto, går sammen om å opprette, lese og redigere dokumenter eller andre filtyper som lagres på tjenestetilbydernes servere, uten at informasjonen utveksles direkte mellom de involvertes kommunikasjonsanlegg. Da er det ikke uten videre gitt at kommunikasjonsavlytting etter strpl. § 216 a gir tilgang til informasjon, ettersom den ikke faktisk "kommuniseres" eller sendes.

I et slikt tilfelle vil ransaking kunne anvendes, gitt at politiet vet hvem som har adgang til e-postkontoen. Ettersom ransaking er begrenset til enkelttilfeller, vil det kunne bety at politiet ikke gis tilgang til eventuell informasjon som kan ha betydning som bevis. En ransakingstillatelse gir som nevnt ikke adgang til kontinuerlig overvåkning, men vil kun gi et øyeblikksbilde av den informasjonen som befinner seg på for eksempel en e-postkonto i det øyeblikket ransakingen gjennomføres. Dersom det gjennomføres en ny ransaking på et senere tidspunkt av samme objekt, kan det ha blitt utvekslet ny informasjon som senere har blitt slettet. Ransaking – også skjult ransaking, vil ikke gi en fullstendig oversikt eller ha anledning til å hente ut slettet informasjon.

1.2.3 Den teknologiske utviklingen av kommunikasjonskontroll

Kommunikasjonskontroll ble først introdusert i norsk lovgivning i 1915 ved lov om kontroll med post- og telegrafforsendelse.[35] Loven gjaldt opprinnelig bare post- og telegrafkontroll, men ble i 1950 utvidet til også å omfatte kontroll med telefonsamtaler.[36]

Formålet med kommunikasjonskontroll var å kunne føre kontroll dersom det ble antatt påkrevd av hensyn til rikets sikkerhet.[37] For saker ut over "rikets sikkerhet" ble bruk av "telefonkontroll" først tillatt ved midlertidig lov i 1976.[38] Loven muliggjorde politiets adgang,

---

[34] Prop. 68 L (2015-2016) side 260.
[35] Lov av 24. juni 1915 nr. 5
[36] Ved lov av 15. desember 1950 nr. 5, se Prop. 68 L (2015-2016).
[37] Prop. 68 L (2015-2016) side 86
[38] Lov av 17. desember 1976 nr. 99 om adgang til telefonkontroll ved etterforskning av overtredelser av narkotikalovgivningen.

etter rettens kjennelse, til å avlytte samtaler til og fra bestemte telefoner, teleksanlegg, og liknende anlegg for telekommunikasjon som den mistenkte hadde eller kunne antas å ville bruke, jf. § 1 første ledd.[39] Slik tillatelse strakk seg også til avbrytelse av samtaler, stenging av telefoner for samtaler eller pålegg til styrer av telefonsentral om å overgi opplysninger om hvilke telefoner som ble eller hadde vært satt i forbindelse med hverandre, jf. § 2.

Den midlertidige lovens anvendelsesområde var begrenset til å gjelde narkotikakriminalitet.[40] Loven ble gjort permanent og inntatt i et nytt kapittel i straffeprosessloven, kapittel 16 a, ved lov 5. juni 1992 nr. 52. Syv år senere ble begrepet "telefonkontroll" erstattet av "kommunikasjonskontroll" ved lov 3. desember 1999 nr. 82. Begrepsendringen var ment å speile at kontroll kunne føres uavhengig av kommunikasjonsenheten.[41] Tidligere var kommunikasjonskontrollen også begrenset til kun narkotikaovertredelser, men dette ble utvidet til også å gjelde generelt ved lovbrudd med en strafferamme på fengsel i ti år eller mer. Reglene om kommunikasjonskontroll ble igjen endret ved lovendringen i 2005, slik at de ikke lenger henviste til straffeloven av 1902 kapittel 8 og 9, men nå viste til konkrete straffebud.[42]

Introduksjonen av kryptert kommunikasjon har gjort tradisjonell avlytting mindre effektiv, da innholdet ikke lenger kan fanges opp i klartekst i sanntid. Denne teknologiske utviklingen har ført til at dataavlesing har blitt mer relevant. Ettersom mer kommunikasjon skjer digitalt og blir lagret enten bevisst av brukerne eller automatisk av tjenesteleverandører, har behovet for å kunne hente ut og analysere denne informasjonen økt. I tillegg gjør endringer i lovgivningen det mulig for myndigheter å kreve tilgang til lagret kommunikasjon, som ofte er nødvendig når kommunikasjonskontroll ikke strekker til, for eksempel i tilfeller der kommunikasjon er kryptert og ikke kan avlyttes i overføringsøyeblikket.

Fordi mange kommunikasjonsformer nå er laget for å være sikre og bare tilgjengelige for mottakeren eller senderen, blir utbyttet av å gjennomføre etterforskning ved bruk av kommunikasjonsavlytting begrenset. Dette har tvunget et skifte mot metoder som

---

[39] Lov av 17. desember 1976 nr. 99 om adgang til telefonkontroll ved etterforskning av overtredelser av narkotikalovgivningen.
[40] Prop. 68 L (2015-2016) side 86.
[41] Prop. 68 L (2015-2016) side 86.
[42] Lov av 17. juni 2005 nr. 87.

dataavlesing hvor tilgangen til informasjon skjer etter at den er lagret og potensielt dekryptert av mottaker.

1.2.4 Utviklingen av dataavlesing

Etableringen av skjult overvåkning som etterforskningsmetode bunner i et økende behov for effektiv, reell tilgang til elektronisk lagret og kommunisert informasjon.[43] I dag produseres, behandles, kommuniseres, og lagres informasjon i stor grad elektronisk ved hjelp av mobile nettbaserte tjenester. I møte med dette øker bruken av krypteringsløsninger og andre metoder for å beskytte brukeres informasjon. Slik beskyttelse er ikke lenger forbeholdt aktører med spesiell kompetanse og interesse, men presenteres nå som en "standardløsning" og et minimumskrav i elektronisk kommunikasjonssammenheng, eksempelvis i chatte-applikasjoner som "Whatsapp", eller "Facebook Messenger". Den teknologiske utviklingen og bruken av krypteringsløsninger har til gjengjeld ført til at politiet stadig oftere blir stående uten nødvendig og effektiv tilgang til informasjon som de ellers har hatt rettslig adgang til.[44]

Ved utarbeidelsen av forarbeidet til den nye straffeprosessloven i 2016, uttales det at forslaget til en ny lov er begrunnet med at det er "et stort og udekket behov for *effektiv* tilgang til elektronisk lagret og kommunisert informasjon" (mine kursiveringer).[45] Fra dette kan man trekke ut at de midlene som var tilgjengelig før dataavlesing ble introdusert som selvstendig metode, ikke var tilstrekkelig for å gi reell tilgang til den informasjonen som ble innhentet.

1.2.5 Samfunnsbehov

Behovet for dataavlesing som selvstendig tvangsmiddel bunner som sagt i den raske teknologiske utviklingen i samfunnet. Moderne løsninger for elektronisk behandling og formidling av informasjon legger til rette for effektiv kommunikasjon og stor elektronisk bevegelsesfrihet.

---

[43] Innst. 343 L (2015-2016) Innstilling fra justiskomiteen om Endringer i straffeprosessloven 31.05.2015.
[44] Eksempelvis gjennom kommunikasjonsavlytting, hemmelig ransakelse, eller beslag.
[45] Prop. 68 L (2015-2016) side 12.

Kripos ga i en trendrapport i 2015 uttrykk for at det kan påvises en sammenheng mellom fildeling av overgrepsbilder og fysiske seksuelle overgrep mot barn.[46] Dette er et vedvarende problem også i dag, og fortsetter å være en av de aktuelle problemstillingene politiet møter.[47] Denne kriminaliteten utføres gjerne av kriminelle nettverk som kontrollerer tilgang til barn som enten er hjemløse eller selges av sine foreldre. Slike overgrep kjennetegnes av at de kan være vanskelige å spore, da bevis normalt ikke lagres, eller kun lagres på krypterte tjenester, som gjør sporing vanskelig.[48]

Økende bevissthet om personvern, og allmennhetens interesse i å beskytte egen informasjon og kommunikasjon, har ført til nye "standardløsninger" og minimumsforventninger til digitale aktører. Generelt ønsker personer som benytter det åpne internettet å beskytte seg mot at utenforstående parter skaffer seg tilgang til deres informasjon. En av måtene den vanlige forbruker kan beskytte seg mot dette på, er ved krypteringsløsninger.[49] Kryptering innebærer at informasjon "lukkes" når den overføres eller lagres, ved å omforme data slik at den gjøres uleselig for personer som ikke eksplisitt gis tilgang.[50] Noen velger dette aktivt, og tar steg for å sikre kommunikasjon og informasjon mot at andre skaffer seg tilgang. Den vanlige forbruker er derimot neppe klar over hvor mye av deres kommunikasjon som faktisk er kryptert. Eksempelvis har den sosiale media-plattformen Facebook nylig gått over til å benytte såkalt ende-til-ende kryptering i deres chattetjeneste "Messenger", et annet populært eksempel er "WhatsApp", som også tilbyr samme type kryptering.

Ende-til-ende kryptering innebærer at tredjeparter forhindres i å skaffe tilgang til data som er kommunisert fra én enhet til en annen. Slik skapes det naturligvis også et stort handlingsrom for cyberkriminelle. Dette betyr ikke at alle tjenester som *ikke* tilbyr dette, eller hvor brukeren ikke bevisst har aktivert denne funksjonen, er åpne for at hvem som helst kan lese

---

[46] Trendrapport 2015 *Organisert og annen kriminalitet i Norge*.
[47] Trendrapport 2023 *Cyberkriminalitet 2023*. "Overgrepssider med forum og chattesider skaper et fellesskap der overgrep mot barn normaliseres, noe som kan føre til at enkelte seksualforbrytere som tidligere ikke har begått seksuelle overgrep, velger å begå fysiske overgrep. [...] Til tross for at de norske gjerningspersonene ikke er i fysisk kontakt med barna de utsetter de barn over hele verden for voldtekt og overgrep ved hjelp av enkel teknologi, i samarbeid med voksne som fysisk til stede med barna." Side 39.
[48] Prop. 68 L (2015-2016) side 31.
[49] Prop. 68 L (2015-2016) side 259.
[50] Tom Heine Nätt, *Store Norske Leksikon: Kryptering,* snl.no/kryptering. (Lest 2. april 2024).

meldingene, men det betyr at det er et ekstra sikkerhetslag for meldinger og telefonsamtaler mellom brukere.[51]

En forsterket informasjonsbeskyttelse, og en styrking av hverdagsforbrukerens forståelse av hvordan de kan navigere digitale miljøer, representerer en fordel for lovlig bruk av informasjonstjenester. Motstykket til dette er at kriminelle i økende grad vender seg til spesialtilpassede krypteringsløsninger eller andre sikrede chattetjenester for å unngå overvåking.

Ende-til-ende-krypterte plattformer gir mulighet til å produsere, laste ned, lagre og dele blant annet overgrepsmateriale uten at dette enkelt kan avdekkes.[52] Kriminelle søker stadig nye løsninger som å unngå innsyn i kommunikasjon som omhandler kriminelle handlinger, for eksempel deling og produksjon av overgrepsmateriale av barn. Snapchat er et velkjent eksempel på en tjeneste hvor standardinnstillingen er at meldinger slettes etter visning. Mer kjent i kriminelle kretser er EncroChat, en kommunikasjonstjeneste som har blitt kjent for sitt fokus på anonymitet og kryptering.[53] En slik utvikling tvinger lovgiver til å modernisere regelverket, og utvikle nye aktuelle metoder for å sikre tilgang til slik informasjon i etterforskningsøyemed.

1.2.6 Oppsummering

Kommunikasjonskontroll fokuserer på overvåking av pågående kommunikasjon, som telefonsamtaler og internettforbindelser, og tillater politiet å avlytte eller spore slikt innhold. Metoden blir derimot stadig mindre effektiv i møte med kryptert kommunikasjon, da den kun fanger opp data etter at de er mottatt eller sendt, og ikke gir tilgang til innholdet i krypterte meldinger i sanntid.

Hemmelig ransaking gir politiet adgang til å søke etter bevis blant annet på mistenktes datasystem og i deres bolig, men tillater kun et øyeblikksbilde av den informasjonen som

---

[51] "End-to-End Encryption on Messenger Explained", https://about.fb.com/news/2024/03/end-to-end-encryption-on-messenger-explained/. *Meta*. (Lest 2. april 2024); Se også "End-to-End Encryption" https://en.wikipedia.org/wiki/End-to-end_encryption, *Wikipedia, The Free Encyclopedia.* (Lest 2. april 2024).
[52] Trendrapport 2024 *Cyberkriminalitet 2024.* side 46.
[53] Jeg vil komme nærmere inn på EncroChat i punkt 4.4.

avdekkes. Dette har ført til behovet for nye metoder som dataavlesing, som tillater kontinuerlig overvåkning av datasystemer og gir tilgang til ukryptert informasjon. Dataavlesing har dermed blitt stadig mer aktuelt for å håndtere den teknologiske utviklingen og utfordringene knyttet til kryptering og moderne kommunikasjonstjenester, og representerer et viktig tilskudd til de tradisjonelle tvangsmidlene.

1.3 Metode

Det rettslige utgangspunktet for dataavlesing følger som nevnt av straffeprosessloven § 216 o. Oppgaven tar utgangspunkt i rettsdogmatisk metode.[54]

Det sentrale utgangspunktet vil være straffeprosesslovens hjemmel for dataavlesing, men også lovforarbeider fra utredninger rundt spørsmålet om dataavlesing og overordnet om overvåkning av borgere i etterforskningsøyemed.

Prop. 68 L (2015-2016) om endringer i straffeprosessloven gir omfattende innsikt i de tidligere utredninger som er gjort rundt spørsmål om bruk av dataavlesing, hva dataavlesing innebærer, fremgangsmåte, bakgrunn, historikk, og andre lands rett (særlig dansk og svensk rett).

Høyesterett har i liten grad vurdert bruk av dataavlesing og de problemstillinger som eksisterer rundt tvangsmiddelet. Rettens kjennelser om dataavlesing er for øvrig også unntatt offentligheten.[55] Fra norsk høyesterettspraksis er det som nevnt i realiteten bare HR-2022-1314-A (EncroChat) som berører strpl. §§ 216 o og 216 p. Dommen gir lite veiledning for spørsmål om retten til privatliv i lys av dataavlesing som skjult tvangsmiddel. EncroChat-dommen tar primært for seg bruk av etterforskningsmateriale innhentet ved utenlandske myndigheters skjulte tvangsmiddelbruk, med en metode som potensielt er urettmessig etter norsk straffeprosesslov. Dette kommer jeg nærmere tilbake til i punkt 4.4.

[54] Jf. Skoghøy 2023, s. 17-18.
[55] Med hjemmel i strpl. § 28 tredje ledd siste punktum, jf. Strpl. § 100 a første ledd, supplert av lov 13. august 1915 nr. 5 om domstolene (domstolloven) § 130 første ledd bokstav b; se også lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) § 23 annet ledd.

Dataavlesing som tvangsmiddel er som nevnt en slags krysning mellom kommunikasjonsavlytting og hemmelig ransaking. Det gjennomføres på mange måter innenfor rammene av kommunikasjonsavlytting og hemmelig ransaking, og det kan derfor være relevant å benytte analogiske tolkninger av rettspraksis før § 216 o for å trekke linjer til dataavlesing.[56]

Det følger av stprl. § 4 at folkeretten går foran straffeprosessloven. Bestemmelsen fastslår at loven gjelder med de begrensninger som anerkjennes i folkeretten, og innebærer i praksis at EMK og andre konvensjoner som Norge har forpliktet seg til vil gå foran straffeprosessloven ved motstrid.[57] En slik praksis vil også medføre at rettspraksis fra den Europeiske menneskerettsdomstol (heretter EMD) vil opptre veiledende for norske rettsanvendere. Det benyttes derfor en del rettspraksis fra EMD i avhandlingen, og der dette gjøres er det begrenset til å gjelde hovedsakelig EMK artikkel 8 om retten til privatliv og beskyttelse fra vilkårlige inngrep.

Det trekkes linjer til rettspraksis hvor EMD har vurdert bruk av skjulte tvangsmidler som kommunikasjonskontroll eller avlytting, oppbevaring av personlig informasjon, hemmelig ransakelse, eller andre liknende midler. I lys av de likhetstrekkene som foreligger mellom tvangsmidlene, anses dette som en hensiktsmessig bruk av tilgjengelig rettspraksis. EMD har ikke vurdert de konkrete vilkårene for å gjøre inngrep ved å benytte dataavlesing.[58] Der det er aktuelt å tolke bestemmelser fra EMK og praksis fra EMD vil det tas utgangspunkt i den selvstendige metodelæren utviklet av EMD.

1.4 Avgrensninger

1.4.1 Utgangspunkt

Avhandlingen vil i hovedsak utforske hvordan lovgiver har balansert behovet for effektiv kriminalitetsbekjempelse og ivaretakelse av kriminalitetsbekjempelse, mot individets rett til

[56] Prop. 68 L (2015-2016) side 264 punkt 14.8.4
[57] Underbyggende tolkning: Rt. 1994 s. 610; "Til dette bemerker jeg først at jeg er enig i at norske domstoler må anvende prosessreglene på strafferettens område slik at rettergangen blir forenlig med våre traktatforpliktelser, og at det kan bli tale om å sette Norges regler til side om det skulle foreligge motstrid, jf. strpl § 4."
[58] I skrivende stund, 01.03.2024.

privatliv og rettssikkerhet. Deretter vil jeg se på hvordan Høyesteretts uttalelser i EncroChat-dommen påvirker enkelte av de behovene.

Det primære fokuset i avhandlingen knytter seg til dataavlesing i forbindelse med etterforskning, ikke i lys av forebygging og avverging, jf. Politiloven[59] § 17 d og strpl. § 222 d. Jeg vil derimot kort si litt om hva som ligger i "forebygging" og "avverging", men går ikke nærmere inn på dette senere.

Rettigheter til tredjepersoner som kan berøres av overvåkningen behandles ikke nærmere.[60] Spørsmål om å kunne benytte seg av overskuddsinformasjon fra dataavlesing vil ikke behandles (såkalte tilfeldighetsfunn)[61]. Spørsmål om jurisdiksjon ved funn vil heller ikke behandles nærmere[62]. Kjernen av oppgaven knytter seg til vilkårene for å anvende dataavlesing, og hvordan de forstås i sammenheng med relevante rettskilder som EMK artikkel 8 og Grl. § 102, samt hvordan Høyesterett har tilnærmet seg bestemmelsen.

1.4.2 Dataavlesing i forebyggende og avvergende øyemed

Dataavlesing kan benyttes i forebyggende og avvergende øyemed, men foregår hovedsakelig i etterforskningssammenheng.[63] Ettersom oppgaven knytter seg til sistnevnte, har jeg valgt å avgrense mot forebyggende og avvergende øyemed. For helhetens skyld vil jeg kort si noe om hva dette innebærer, men det vil ikke drøftes videre.

Hjemmel for dataavlesing følger av straffeprosessloven § 216 o, og hjemmel for bruk av skjulte tvangsmidler i forebyggende øyemed er inntatt i lov av 4. august 1995 nr. 53 (heretter politiloven) § 17 d. Dataavlesing kan gjennomføres ved etterforskning av alvorlige kriminelle handlinger som nevnes i strpl. § 216 o første ledd,[64] eller som politimetode ved *forebygging*

---

[59] Lov 4. august 1995 nr. 53 om politiet (politiloven).
[60] Se mer om dette i Bruce og Haugland (2018) side 248-265, Prop. 68 L (2015-2016) punkt 6.6.5, og NOU 2009: 15.
[61] Se Prop. 147 L (2012-2013) kapittel 5, side 72-84.
[62] Se mer om dette i Bruce og Haugland (2018) kapittel 5.
[63] Jf. Strpl. § 216 o, jf. politiloven § 17 d og strpl. § 222 d.
[64] Med "alvorlige kriminelle handlinger" menes handlinger som etter loven kan medføre straff av fengsel i 10 år eller mer, eller "handlinger som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 129, 136, 136 a, 136 b, 232, 254, 257, 311, 333, 337 jf. 231, eller 340 jf. 231, utlendingsloven § 108 femte ledd, eller eksportkontrolloven § 5."

av alvorlig kriminalitet etter politiloven § 17 d. Det åpnes også for å anvende dataavlesing i *avvergende* øyemed etter strpl. § 222 d.

Politiets sikkerhetstjeneste (PST) kan etter § 17 d benytte skjulte tvangsmidler i forebyggende øyemed "dersom det er grunn til å undersøke om noen forbereder enkelte nærmere bestemte straffbare handlinger".[65] Hjemmelen gir PST adgang til å benytte tvangsmidler for å forebygge kriminalitet uten at det foreligger en etterforskning. Metodekontrollutvalget presiserte i forarbeidet til straffeprosesslovens § 216 o at en innføring av dataavlesing som selvstendig skjult tvangsmiddel, "(...) ikke vil kreve noen endring av politiloven § 17 d første ledd, ettersom det her vises til straffeprosessloven § 200 a og § 216 a som etter utvalgets forslag vil gi adgang til innbrudd i et datasystem".[66]

Stprl. § 222 d åpner for at retten ved kjennelse kan gi politiet tillatelse til å benytte tvangsmidler dersom det er "rimelig grunn til å tro" at noen kommer til å begå en nærmere bestemt straffbar handling.[67] Å "avverge" forstås som å hindre forholdsvis nært forestående lovbrudd, og skiller seg fra å "forebygge" som hindrer på lengre sikt.[68] Skillet mellom forebyggende og avvergende metodebruk knytter seg slik til tidspunktet metodebruken finner sted som ledd i etterforskning. Jo nærmere i tid handlingen som søkes hindret finner sted, jo nærmere går man fra "forebygging" til "avverging".[69]

Ved innføringen av dataavlesing, påpekte Justis- og beredskapsdepartementet i forarbeidene at dataavlesing tillatelse til å benytte dataavlesing etter strpl. § 222 d og politiloven § 17 d bare bør skje der "særlige grunner tilsier det".[70] Det gis dermed uttrykk for at det er en noe høyere terskel for å benytte dataavlesing i avvergende eller forebyggende øyemed, men av hensyn til oppgavens omfang vil jeg ikke gå nærmere inn på dette.

Hensikten med å vise til de ovennevnte bestemmelsene er å illustrere at dataavlesing også *kan* benyttes utenfor etterforskning av en konkret straffesak, men kun under visse omstendigheter.

---

[65] Prop. 68 L (2015-2016) side 246.
[66] Prop. 68 L (2015-2016) side 246.
[67] Jf. strpl. § 222 d første ledd.
[68] Se Ot.prp.nr. 60 (2004-2005) side 149-150.
[69] Se Prop. 68 L (2015-2016) side 171, jf. Ot.prp.nr. 60 (2004-2005) punkt 6.1 side 60.
[70] Prop. 68 L (2015-2016) side 274.

2 Konstitusjonelt og folkerettslig vern av privatlivet

2.1 Innledning

Som tidligere nevnt oppstiller Grunnloven § 102 og EMK artikkel 8 et vern for privatlivet. Begrepet "privatliv" er vidt og ubestemt. Enkelte områder er likevel definert både i konvensjonstekst, konvensjonspraksis, og Høyesterettspraksis. Bestemmelsene fremhever likevel at blant annet den enkeltes "kommunikasjon" og "hjem" er vernet.

Retten til privatliv er ikke absolutt, og det kan gjøres inngrep i den dersom det er i samsvar med lov, er formålsforankret, og "nødvendig i et demokratisk samfunn", jf. EMK artikkel 8 nr. 2. Adgangen til å gjøre inngrep kommer ikke like klart frem av ordlyden i Grl. § 102, men kan heller se ut som at de gir et generelt vern av retten til privatlivet. Høyesterett har derimot lagt til grunn at det kan gripes inn i retten til privatliv etter Grl. § 102, "dersom tiltaket har tilstrekkelig hjemmel, forfølger et legitimt formål og er forholdsmessig".[71]

Det er sikker rett at Grunnloven skal tolkes i samsvar med EMK.[72] Dermed er det hensiktsmessig å redegjøre for både Grl. § 102 og EMK art. 8, og forholdet mellom bestemmelsene. I det følgende vil jeg derfor nærmere på hva retten til privatliv innebærer, om dataavlesing er et inngrep, samt hvilke vilkår som må være oppfylt for å benytte dataavlesing.

2.2 Grunnloven § 102 – Konstitusjonelt vern

Retten til privatliv fremgår som nevnt av Grl. § 102 første ledd første punktum. Det følger av ordlyden at "[e]nhver har rett til respekt for sitt "privatliv" og familieliv, sitt hjem, og sin kommunikasjon". Det oppstilles et generelt vern for privatlivets fred som en individuell rettighet, men bestemmelsen sier ikke noe mer om det offentliges adgang til å gjøre inngrep i denne rettigheten.

[71] Jf. Rt. 2014 s. 1105 (Acta-dommen) avsnitt 28 og Rt. 2015 s. 93 (Maria-dommen) avsnitt 60.
[72] Jf. Rt. 2014 s. 1105 (Acta-dommen).

Bestemmelsen ble tilføyd ved grunnlovsreformen i 2014, og bygger på både SP-konvensjonen[73] artikkel 17 og EMK artikkel 8.[74] *Lønning-utvalget* utredet spørsmålet om en generell utvidelse av grunnlovens menneskerettsvern. Ved vurderingen hadde utvalget foreslått at det rettslige vernet av privatliv burde omtales direkte i grunnlovsbestemmelsen for å sikre "at all systematisk innhenting, oppbevaring og bruk av andres personlige opplysninger trenger hjemmel i lov".[75]

Hensikten med å innføre bestemmelsen var å sikre en generell og grunnleggende beskyttelse av privatlivet til enkeltpersoner, privatlivets fred, personvern og personopplysningsvern.[76] Ved å ta inn en slik rettighet i Norges øverste lov settes det en tydelig juridisk ramme for å beskytte enkeltmenneskers rett til privatliv, som også har symbolsk betydning.

Grl. § 102 oppstiller som sagt et overordnet universalt vern for privatlivets fred som en individuell rettighet. Det fremgår uttrykkelig av ordlyden at vernet omfatter respekt for privatliv, familielivet, hjemmet, og ens kommunikasjon. Ordlyden er generisk, og favner vidt. Bestemmelsen må derfor tolkes nærmere i lys av dens relevante rettskilder.

Høyesterett uttaler i Rt. 2015 s. 93 (Maria-dommen) at Grl. § 102 skal tolkes i lys av de folkerettslige forbildene, men likevel slik at fremtidig praksis fra de internasjonale håndhevingsorganene ikke har samme prejudikatsvirkning ved grunnlovstolkningen som ved tolkningen av de parallelle konvensjonsbestemmelsene.[77] Det er altså Høyesteretts ansvar å tolke Grunnloven i siste instans.

---

[73] De Forente Nasjoners internasjonale konvensjon 16. desember 1966 om sivile og politiske rettigheter.
[74] Rt. 2015 s. 93 avsnitt 57.
[75] Dok nr. 16 (2011-2012) side 179.
[76] GLFOR 30 (2011-2012) Dok.nr.12: 30 (2011-2012) Grunnlovsforslag om grunnlovfesting av sivile og politiske menneskerettigheter side 7.
[77] Rt. 2015 s. 93 Avsnitt 57

2.3 EMK artikkel 8 – Folkerettslig vern av privatlivet

2.3.1 Rettighetsvern

2.3.1.1 Privatliv

Som tidligere nevnt har alle mennesker en grunnleggende rett til privatliv.[78] Som et utgangspunkt har alle individer et uttrykt behov fTjesos.ssor en privatsfære, hvor de kan opptre og kommunisere som de vil uten innblanding fra myndigheter eller andre personer.[79] Ivaretakelsen av individers privatliv er elementært i en rettsstat og i demokratiet, da det muliggjør individers selvstendighet og frihet.

Det følger av EMK artikkel 8 nr. 1 at "[e]nhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse". Ordlyden stadfester individenes eksplisitte rett til et slikt "privatliv".

Uttrykket "privatliv" har ingen uttømmende definisjon. En naturlig tolkning av ordet innebærer at individer kan ha personlige områder, opplevelser, tanker og handlinger som ikke må deles med eller påvirkes av andre enn dem selv, eller andre som de velger å dele det med. I korte trekk innebærer det en rett til å være i fred fra andre.

EMD har uttalt at privatliv er et vidt begrep, som typisk omfatter "the sphere of personal autonomy in which everyone can freely pursue the development and fulfilment of his or her personality and to establish and develop relationships with other persons and the outside world".[80] Etter EMD's rettspraksis kan privatlivsbegrepet blant annet omfatte helse, familie og hjem, personlig autonomi og identitet, og lagring og publisering av personlig informasjon, herunder fingeravtrykk og DNA.[81] Begrepets betydning avhenger dermed ofte av konteksten.

---

[78] Se punkt 1.1, jf. Grunnloven § 102 og EMK artikkel 8.
[79] NOU 2009: 15 side 58.
[80] Se *Jehova's Witnesses of Moscow and others v. Russia* avsnitt 117.
[81] Se henholdsvis *Nada v. Switzerland* avsnitt 151; *Galev and Others v. Bulgaria; Aksu v. Turkey* avsnitt 58; og *S. And Marper v. the United Kingdom* avsnitt 194.

Privatliv omfatter heller ikke bare den umiddelbare private sfære, men også i noen grad retten til å etablere og utvikle kontakt med andre mennesker.[82] Utvikling av menneskers forhold til andre og deres sosiale identitet skjer hovedsakelig gjennom *kommunikasjon*. Artikkel 8 nr. 1 fremhever dette ved eksplisitt å nevne retten til respekt for korrespondanse. Typisk er dette brev, e-post eller meldinger.[83] Det er gjennom konvensjonspraksis lagt til grunn at avlytting av telefonsamtaler utgjør et alvorlig inngrep i retten til privatliv.[84] Også informasjon om internettbruk omfattes av korrespondanse-begrepet.[85]

Felles for konvensjonspraksis er at EMD ofte beskriver privatliv som et begrep som typisk berører individets "psykiske og fysiske integritet".[86] Dette har betydning for straffeprosessrett, ettersom flere sentrale straffeprosessuelle inngrep skjer nettopp på områdene for disse rettighetsaspektene. Et inngrep som dataavlesing vil alltid falle innenfor artikkelens anvendelsesområde, ettersom det er et tvangsmiddel, og benyttes uten mistenktes samtykke og forkunnskap. Et viktig moment i hva som omfattes av retten til privatliv, er om vedkommende kan ha en rimelig forventning om beskyttelse av sitt privatliv i det aktuelle tilfellet.[87]

2.3.2 Personvernets rettslige forankring

Begrepene *privatlivets fred, personvern*, og *personopplysningsvern* benyttes ofte om hverandre. For helhetens skyld kan det være hensiktsmessig å se til noen av de overordnede rammene for hva som skiller dem.

I internasjonale lover er det primært "privacy" som benyttes – som ofte oversettes til "personvern", men trolig må tolkes snevrere.[88] Personvernkommisjonen har gitt følgende definisjoner av personvern og personopplysningsvern:

---

[82] Se *Niemietz v. Germany* avsnitt 27-29.
[83] Se henholdsvis *Erdem v. Germany* og *Radaj v. Poland*.
[84] Se *Klass and Others v. Germany* avsnitt 41.
[85] Se *Copland v. The United Kingdom* avsnitt 41.
[86] Se *Van Kuck v. Germany* (35968/97) avsnitt 69.
[87] Se *P.G and J.H v. The United Kingdom* avsnitt 57 *og Perry v. The United Kingdom.* Se også *Halford v. The United Kingdom* avsnitt 45.
[88] Dok. Nr. 16 (2011-2012) side 172.

> "*Personvern* dreier seg om ivaretakelsen av personlig integritet; ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse.
>
> *Personopplysningsvern* dreier seg om regler og standarder for behandling av personopplysninger som har ivaretakelse av personvern som hovedmål. Reglenes formål er å sikre enkeltindivider oversikt og kontroll over behandling av opplysninger om dem selv. Med visse unntak skal enkeltpersoner ha mulighet til å bestemme hva andre skal få vite om hans/hennes personlige forhold."[89]

Personvernkommisjonens definisjon av begrepet "personvern" dekker retten til privatliv.[90] Uttrykket stammer fra det engelske uttrykket "privacy", og favner vidt.[91]

Personvern er forankret nasjonalt i Norges Grunnlov[92] § 102 gjennom ordlyden "respekt for sitt privatliv". Retten til privatlivets fred hjemles også i EMK artikkel 8,[93] i tillegg til flere internasjonale menneskerettskonvensjoner som Norge har forpliktet seg til.[94]

Personvernets essens innebærer at mennesker selv skal kunne avgjøre hvilken tilgang andre har til deres personlige informasjon og forhold.[95] Det følger av direktivet at medlemsstatene skal sikre vern av grunnleggende rettigheter, særlig retten til privatliv, ved behandling av personopplysninger.[96]

Med "personopplysning" menes "enhver opplysning om en identifisert eller identifiserbar person." [97] I forarbeidene til straffeprosessloven har Metodekontrollutvalget betraktet

---

[89] NOU 2009: 1 punkt 4.1.5, 4.1.4 og 4.2
[90] Dok. Nr. 16 (2011-2012) side 172.
[91] NOU 2009: 1 Individ og integritet side 29.
[92] Lov av 17. mai 1814 Kongeriket Norges Grunnlov, heretter Grl.
[93] Europarådets konvensjon av 4. november 1950 om *beskyttelse av menneskerettighetene og de grunnleggende friheter* (Den europeiske menneskerettighetskonvensjon, heretter EMK).
[94] Herunder de forente nasjoners internasjonale konvensjon om sivile og politiske rettigheter av 15. desember 1966 artikkel 17, og FNs erklæring om menneskerettigheter av 10. desember 1948, og Personverndirektivet (95/46 EF).
[95] NOU 2009: 15 side 50. Personvernet er beskyttelsen av individenes private sfære, som de har et behov for. Behovet for en privat sfære utgjør kjernen i personlig integritet. Personvernet bygger imidlertid ikke bare på et behov for å være i fred fra andre, men innebærer også en rett til å ha kontroll over opplysninger om en selv, særlig opplysninger som oppleves som personlige.
[96] Personverndirektivet 95/46/EF artikkel 1 nr. 1.
[97] Personverndirektivet 95/46/EF artikkel 2 bokstav a.

personopplysningsvernet som en del av det mer omfattende personvernbegrepet.[98] Retten til privatliv omfatter også opplysninger relatert til individets privatliv. Personopplysningsvernet står således i nær tilknytning til personvernet og retten til privatliv.[99]

2.3.3 Begrepene "privatlivets fred", personvern, og personopplysningsvern

I norsk juridisk litteratur ble begrepet først introdusert i 1970, i Erik Samuelsens forskningsrapport "Statlige databanker og personlighetsvern".[100] "Personvern" ble brukt som betegnelse på "en mulig interesse fra enkeltpersoners side i å utøve kontroll med den informasjon som beskriver dem".[101] Ordet har for øvrig blitt definert som en samlebetegnelse på *enkelte* ideelle interesser som tilligger enkeltmennesket (og eventuelt juridiske personer).[102]

Datatilsynet nevner senere at "[p]ersonvern kan være den interesse fysiske og juridiske personer har i å utøve kontroll med den informasjon som beskriver dem."[103] I årene som følger blir personvernbegrepet drøftet av ulike miljøer, men interessene de ulike miljøene mener er omfattet av uttrykkene er hovedsakelig individets rett til kontroll over dets fysiske og psykiske integritet.

De sentrale interessene som omtales rundt tolkningen av "personvern" er interessen i å ha kontroll om opplysninger om seg selv, herunder hvilke opplysninger som samles inn av hvem, hvem som har tilgang til disse og hva de brukes til, interessen i innsyn (den enkeltes interesse i å være orientert om hvordan behandling av opplysninger om dem skjer), interessen i fullstendighet (den enkeltes ønske om at avgjørelser som treffes på grunnlag av personopplysninger blir truffet på et fullstendig og korrekt grunnlag), og interessen i

[98] Se NOU 2009: 15 *Skjult informasjon – åpen kontroll* side 48.
[99] Lov av 14. april 2000 nr. 31 om behandling av personopplysninger § 1
[100] NOU 2009: 1 Individ og integritet side 29.
[101] Blekeli 1977, henvist i NOU 2009: 1 Individ og integritet side 29.
[102] NOU 1997: 19 Side 24 og *Myhrer 2001* side 79.
[103] NOU 2009: 1 Individ og integritet side 29; Datatilsynets årsmelding (1982).

privatlivets fred.[104] Interessen i et privatliv står sterkest i det private hjem, noe som reflekteres i Grunnloven § 102.[105]

Uavhengig av definisjonen er selve begrepet *personvern* særnorsk. I Sverige retter begrepet seg mot "integritet" i større grad.[106] Fokuset i norsk rett er i større grad rettet mot bevaringen av enkeltpersonens psykiske integritet. Sentralt er individers rett til kontroll over opplysninger om en selv.[107] Dette er også kjernen i *personopplysningsvernet*.

Begrepet "personopplysningsvern" er på sin side et relativt nytt begrep, og oppstod som en følge av økt innsamling, bruk og lagring av personopplysninger i samfunnet.[108] Loven definerer personopplysninger som "opplysninger og vurderinger som kan knyttes til en enkeltperson".[109] Personopplysningsvernet skal beskytte den enkelte mot innsyn i sensitiv og privat informasjon, samt beskytte den enkeltes identitet og retten til å være anonym. Personopplysningsvern kan derfor forstås som vern av den enkeltes rett til innflytelse på bruk og spredning av informasjon om seg selv.

Personopplysningsvern – som en underkategori av personvernet – dreier seg som nevnt hovedsakelig om *normer* for behandling av personopplysninger som har ivaretakelse av personvern som hovedmål. Reglenes formål er altså å sikre enkeltindivider oversikt og kontroll over behandling av opplysninger om dem selv.

Dette er en annen side av dataavlesing som knytter seg mer til behandlingen av eventuelle data som innhentes, og faller utenfor oppgavens problemstilling. Jeg vil derfor ikke gå nærmere inn på personopplysningsvernet.[110]

---

[104] NOU 2009: 15 *Skjult informasjon – Åpen kontroll* side 50.
[105] Se ovenfor, punkt 2.2.
[106] Begreper som kommer til bruk er blant annet "integritetsskydd" og "personlige integritet". Se Den svenske integritetsskyddskomiteens innstilling 2007.
[107] NOU 2009: 15 s. 49
[108] Dok. Nr. 16 (2011-2012) side 173.
[109] Lov av 15. juni 2018 nr. 1 om behandling av personopplysninger § 2, nr. 1
[110] For ytterligere uttalelser rundt skillet mellom personvern og personopplysningsvern, se NOU 2009: 1 side 32, med henvisning til Schartum og Bygrave (2004 s. 13 ff.)

2.3.4 Inngrepshjemmelen

I tillegg til at EMK artikkel 8 – i likhet med Grl. § 102 - oppstiller et *generelt* vern for privatlivet, åpnes det som nevnt også for å gjøre inngrep i denne rettigheten. Den såkalte "inngrepshjemmelen" er en av de sentrale forskjellene mellom de to bestemmelsene. I det følgende vil jeg se nærmere på hva EMK art. 8 nr. 2 inneholder, og hvordan det påvirker tilgangen til å benytte dataavlesing etter strpl. § 216 o.

Offentlig myndighet kan gjøre "inngrep" i enkelte rettigheter under nærmere bestemte vilkår. En alminnelig tolkning av "inngrep" tilsier at det må skje en endring i subjektets rettstilstand for eksempel i form av at deres rettigheter innskrenkes, utvides, eller overtredes.

Det åpnes for å gjøre inngrep i retten til privatliv når dette er "i samsvar med loven" og inngrepet er "nødvendig i et demokratisk samfunn" etter nærmere bestemte formål, jf. EMK art. 8 nr. 2. Inngrep vil derfor kunne aksepteres dersom det oppfyller lovkravet, det forfølger et legitimt formål, og det er nødvendig i et demokratisk samfunn.

Dataavlesing er en form for skjult overvåkning hvor offentlig myndighet kan foreta en fullstendig overvåkning av mistenktes tastetrykk, filer kommunikasjon over internett, samt mulighet for avlytting ved hjelp av mikrofonen og overvåkning gjennom webkameraet.[111] En slik form for overvåkning utgjør naturligvis et *sterkt* inngrep i individets rett til privatliv og kommunikasjon etter EMK artikkel 8. Etter omstendighetene kan dataavlesing berøre retten til privatliv så vel som korrespondanse, og gripe inn i den enkeltes fysiske og psykiske integritet. Metoden vil lett kunne rettes mot det privat hjem, hvor vernet etter artikkel 8 nr. 1 er særlig sterkt. Dette spiller en rolle ved vurderingen av inngrepets karakter. EMD uttaler i *Roman Zakharov v. Russia* avsnitt 232 at:

> "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".

[111] Se nærmere i punkt 4.

Ved vurdering av om dataavlesing kan benyttes, må man altså vurdere både Grl. § 102 og EMK art. 8. Igjen er det av betydning at bestemmelsene må sees i sammenheng. Høyesterett har som nevnt ved flere anledninger gitt uttrykk for at Grl. § 102 er en parallellbestemmelse til EMK artikkel 8, og at de to bestemmelsene har sammenfallende innhold. [112] Videre at grunnlovsbestemmelsen må tolkes med utgangspunkt i den tilsvarende bestemmelsen i EMK, se Rt. 2015 s. 93 (Maria-dommen) avsnitt 57 og 60, og Rt. 2015 s. 155 (Rwanda) avsnitt 40 og 44.[113]

2.3.5 Lovkravet

Det første vilkåret for å gjøre et inngrep i retten til privatliv er at det må ha tilstrekkelig hjemmel i nasjonal lovgivning, jf. ordlyden "i samsvar med loven" i EMK art. 8 nr. 2 Kravet er også inntatt i norsk lov ved Grunnlovens § 113. Hjemmelen fastslår generelt at "[m]yndighetenes inngrep overfor den enkelte må ha grunnlag i lov".

Lovkravet innebærer at rettsregelen skal være *tilgjengelig*, og rettstilstanden *forutsigbar*.[114] EMD har fastslått at ved vurderingen av om rettsregelen oppfyller kravene til tilgjengelighet og forutsigbarhet, må det foreligge prosessuelle garantier som innebærer at borgere skal kunne prøve lovligheten av inngrepet.[115]

EMD har videre lagt til grunn at både formell lov og ulovfestet rett oppfyller lovkravet.[116] Dette er imidlertid betinget av at hjemmelen er tilstrekkelig klar og i stand til å gi borgere et tydelig grunnlag for å kunne forutse sin rettsstilling, og under hvilke forhold myndighetene har anledning å gjøre inngrep i den rettsstillingen.[117]

---

[112] Se HR-2022-718-A avsnitt 85; HR-2017-2376-A avsnitt 53; HR-2016-2554-P (Holship-dommen); Rt-2014-1105 (Acta-saken).
[113] Direkte sitat fra HR-2016-2554-P Holship avsnitt 81.
[114] Se *Silver v. The United Kingdom* og *Saber v. Norway,* og *Roman Zakharov v. Russia* avsnitt 229-232.
[115] Se *Sanoma Uitgeves B.V. v. The Netherlands* avsnitt 100.
[116] Se *Sunday Times v. The United Kingdom* avsnitt 47
[117] Se *Roman Zakharov v. Russia* avsnitt 229.

I europeisk rettspraksis skiller dette seg fra norsk rett ettersom det norske legalitetskravet innebærer at loven må fremgå av formell lov. Man kan for eksempel ikke ilegge straff uten at dette følger eksplisitt av lovteksten.[118]

I tillegg til at det stilles et materielt klarhetskrav til inngrepets hjemmel, må det eksistere prosessuelle rettssikkerhetsgarantier som beskytter borgerne mot vilkårlige inngrep fra myndigheten. Eksempelvis følger det av strpl. § 216 o en begrensning for hvor lenge en kan overvåkes, prosedyrer for håndtering av materiale som innhentes, og regler for sletting og/eller videreformidling av materialet til andre relevante parter.[119]

EMD har lagt til grunn at retningslinjer for håndtering av materiale fra kommunikasjonskontroll er noe som tillegges stor vekt i vurderingen av om prosessuelle rettssikkerhetsgarantier er opprettholdt.[120] Dette vil også ha betydning for om inngrepet var nødvendig i et demokratisk samfunn, og EMD har tidligere vurdert at lovkravet og nødvendighetsvurderingen under visse omstendigheter kan tas under ett.[121] Jeg kommer nærmere tilbake til dette under punkt 2.4.5.

Forutsigbarhetskravet er noe som problematiseres av EMD, i lys av at individer ikke gis ordinær adgang til å kunne forutse sin rettsstilling. Det følger av konvensjonspraksis at forutberegnelighetskravet ikke kan tolkes alminnelig når det gjelder skjult overvåkning.[122] Dette begrunnes med at individet som overvåkes, ikke har krav på å kunne forutse når myndighetene trolig vil overvåke hans/hennes kommunikasjon, og dermed innrette seg deretter.[123] Ikke minst fordi dette vil undergrave hele inngrepets effektivitet. En slik svakhet i rettssikkerheten vil derimot kunne aksepteres dersom det innføres andre prosessuelle garantier.[124]

Når sterke inngrep, som inngrep i privatlivet i form av dataavlesing, må gjennomføres uten enkelte prosessuelle garantier må begrunnelsen bygge på de særlige hensyn til effektivitet

---

[118] Grl. § 113
[119] jf. henholdsvis § 216 o siste ledd, jf. § 216 f, § 216 g, §§ 216 i-216 k.
[120] Se *R.E v. The United Kindom* avsnitt 141, i relasjon til "t*he minimum safeguards"*
[121] Se *R.E v. The United Kingdom* avsnitt 122.
[122] Se *Adomaitis v. Lithuania* avsnitt 83.
[123] Se *Adomaitis v. Lithuana* avsnitt 83; Se også *Drakšas v. Lithuania* avsnitt 67.
[124] Se mer under punkt 2.3.7

som gjennomgående gjør seg gjeldende i behovet for en metode som dataavlesing.[125] For å hindre maktmisbruk og vilkårlighet, er det likevel et vilkår at visse materielle krav er oppfylt.[126]

EMD understreker viktigheten av å ha klare og detaljerte regler for kommunikasjonsavlytting, spesielt ettersom teknologi stadig utvikler seg.[127] Det ligger implisitt i dette et behov for å oppdatere og forbedre lovgivningen for at den skal være tilpasset forandringer i det teknologiske landskapet.

Det kan argumenteres for at lovkravet (herunder klarhetskravet) derfor er strengere når det gjelder dataavlesing.[128] Dataavlesing åpner for en kontinuerlig overvåkning i større grad enn kommunikasjonskontroll ettersom det ikke bare er muntlig kommunikasjon som kan avlyttes, men alt man gjør på datamaskinen, alt dens innhold, i *tillegg* til eventuell kommunikasjon. På bakgrunn av EMDs krav til prosessuelle garantier rundt bruk av kommunikasjonsovervåkning, er det dermed naturlig å anta at det samme, som et minimum, vil gjelde for dataavlesing.

2.3.6 Formålskravet

Det andre vilkåret er at inngrepet må forfølge et legitimt formål (formålskravet). De legitime formål som følger av EMK artikkel 8 nr. 2 er uttømmende, og skal tolkes innskrenkende.[129] Inngrep vil typisk begrunnes ut fra hensynet til nasjonal sikkerhet, hensynet til å forebygge kriminalitet, eller hensynet til å beskytte andres rettigheter.

Konvensjonsteksten stiller følgende krav til formål:

> "(...) in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".[130]

---

[125] Se også Aall (2013) *Prosessuelle garantier og forholdsmessighet,* side 228-229.
[126] Se nærmere punkt 4 og 4.2.2.
[127] Se *Adomaitis v. Lithuania* avsnitt 83 siste setning. Se også *Roman Zakharov v. Russia* avsnitt 229.
[128] Se *Roman Zakharov v. Russia* avsnitt 229.
[129] Jf. *S.A.S v. France*.
[130] EMK artikkel 8 nr. 2.

Formålet med gjennomføring av dataavlesing er kriminalitetsbekjempelse, jf. strpl. § 216 o og forarbeidene.[131] Når dataavlesing benyttes i etterforskning er dette med den hensikt å avdekke informasjon av "vesentlig betydning" for saker som omhandler alvorlige kriminelle handlinger, slik at straffeforfølgning kan gjennomføres effektivt.[132] Det kan derfor også sies at dataavlesing gjennomføres av hensyn til den nasjonale sikkerhet ("in the interests of national security"), offentlig trygghet ("public safety"), og ikke minst for å forebygge kriminalitet ("for the prevention of [...] crime").[133]

Formålet med dataavlesing er særlig relevant ved vurderingen av om inngrepet er forholdsmessig og nødvendig i et demokratisk samfunn. Dette kommer jeg nærmere tilbake til i punkt 4.1.2.5.

2.3.7 Nødvendighetskravet

Det tredje vilkåret er at inngrepet må være "nødvendig i et demokratisk samfunn". Ordlyden gir uttrykk for et nødvendighetskrav, som forstås som et overordnet krav til forholdsmessighet. Det følger av fast konvensjonspraksis at inngrepet typisk må begrunnes i "*a pressing social need*", og at det fremstår "*proportionate to the legitimate aim pursued*".[134]

Vurderingen av om et inngrep møter et pressende samfunnsbehov ("a pressing social need"), bygger på om inngrepet i seg selv er *nødvendig* for å imøtekomme et konkret behov i samfunnet. Det er ikke tilstrekkelig at det bare er ønskelig.[135]

Konvensjonspraksis har videre etablert at inngrep må være proporsjonale for det formålet de søker å oppnå ("proportionate to the legitimate aim pursued").[136] Ordlyden tolkes som at inngrepet må være egnet for å oppnå det formålet som begrunner det. Dersom et inngrep går

---

[131] Se også Prop. 68 L (2015-2016) side 258-259: "Inngrep skal bare kunne skje med grunnlag i tilstrekkelig klar lovhjemmel og på vilkår som sikrer at inngrepet ikke går ut over det som er nødvendig for å tjene det forhåndsbestemte formålet, altså kriminalitetsbekjempelse."
[132] Jf. strpl. § 216 o tredje ledd.
[133] Jf. strpl. § 216 o tredje ledd jf. EMK art. 8 nr. 2.
[134] Se *Olsson v. Sweden* avsnitt 67; Se også *Dudgeon v. The United Kingdom avsnitt 51-53.*
[135] Se *Silver and Others v. The United Kingdom* avsnitt 97
[136] Se *Z v. Finland* avsnitt 94; *Jehova's Witnesses of Moscow v. Russia* avsnitt 108;

lengre enn det som rent faktisk kreves for å oppnå et formål, vil det ikke være forholdsmessig, og dermed kunne stride med EMK art. 8 nr. 2.

EMD uttaler i *Klass and Others v. Germany* at konvensjonsstatene ikke har ubegrenset adgang for å utsette borgerne sine for hemmelig overvåkning.[137] Videre at statene ikke kan benytte et hvilket som helst tvangsmiddel, selv om de begrunner det i behovet for å bekjempe eksempelvis spionasje eller terrorisme.[138] Det må gjøres en vurdering av de fordeler som oppnås ved å iverksette inngrepet, veier tyngre enn de begrensninger som gjøres i individets vernede frihet, her retten til privatliv.[139]

Det følger videre av *Z v. Finland* at vurderingen av om et inngrep var nødvendig i et demokratisk samfunn, beror på om begrunnelsene som oppgis for å rettferdiggjøre inngrepet var relevante ("relevant") og tilstrekkelig ("sufficient"), og deretter om de var proporsjonale til hva formålet var.[140] Det må altså dokumenteres et behov for at aktuelle inngrepet skal tillates, og dette behovet må anses så tungtveiende at inngrepet ikke oppleves uforholdsmessig.

Konvensjonspraksis kan slik tolkes som at det må gjøres en vurdering av om inngrepet er egnet til å realisere formålet (herunder om formålet kan oppnås med andre mindre inngripende metoder), og om inngrepet er forholdsmessig etter det konkrete omstendighetene i saken.[141] For at et inngrep skal regnes som proporsjonalt, må de fordelene som oppnås ved å iverksette inngrepet veie tyngre enn de begrensninger som gjøres i den vernede rettigheten. Utgangspunktet her er at statene har en viss skjønnsmargin ved vurderingen, og dermed en viss grad av frihet til å tolke konvensjonsteksten i tråd med egne forutsetninger.[142]

---

[137] Avsnitt 49: "Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance."
[138] Se avsnitt 49: "The Court, being aware of the danger such law poses of undermining or even destroying democracy on the grounds of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."
[139] Se *Klass and Others v. Germany* avsnitt 50.
[140] Se *Z v. Finland* avsnitt 94: "Whether the impugned measures were "necessary in a democratic society", the Court will consider whether, in the light of the case as a whole, the reasons adduced to justify them were relevant and sufficient and whether the measures were proportionate to the legitimate aims pursued"
[141] Se *Z v. Finland* avsnitt 94.
[142] Se *Campbell v. The United Kingdom* avsnitt 44.

Avveiningen av om et inngrep er forholdsmessig ("proportionate") består slik i hovedsak av behovet for å benytte tvangsmiddelet, og hvor inngripende det aktuelle tiltaket er overfor den som utsettes for det.

Som nevnt ovenfor vil prosessuelle garantier spille en rolle i vurderingen av om et inngrep er forholdsmessig. For eksempel vil borgeres muligheter for å forutse sin rettsstilling ha betydning (kravet til forutsigbarhet). De hensyn som begrunner et inngrep som dataavlesing gjør derimot at en garanti som forutsigbarhet ikke kan gjennomføres på normal måte. Mistenkte kan rimeligvis ikke gis adgang til å forutse når han vil overvåkes, da det vil virke mot sin hensikt.

En svakhet i en av de prosessuelle garantiene kan imidlertid avbalanseres ved at det implementeres andre rettssikkerheter, for eksempel personelle kompetansekrav. En beslutning om dataavlesing krever rettslig kjennelse, jf. strpl. § 216 o. Videre følger det av strpl. § 216 p at dataavlesing må utføres av personell som er "særlig skikket til det" og utpekes av politimesteren, sjef PST eller den som bemyndiges.[143] Et krav om spesiell kompetanse underbygger de prosessuelle garantiene, i form av tillitvekkende personell beslutningskompetanse.[144] Det fremgår av ordlyden at dataavlesing bare kan utføres av personell som er "særlig skikket til det". Ordlyden krever tilsynelatende personell som har særskilt høy informasjonsteknologisk kompetanse.

I *Kruslin mot Frankrike* understreket EMD den betryggende effekten av at det var en domstol som hadde besluttet et inngrep – i den saken gjaldt det telefonavlytting. Det samme kan sies for beslutninger om dataavlesing, som i utgangspunktet krever en rettslig kjennelse, og videre må utføres av særlig skikket personell.[145]

Forholdsmessighetsvurderingen vil derfor bestå av følgende momenter: Behovet for å anvende tvangsmiddelet,[146] graden av inngrepet, sakens art og alvorlighet, konsekvenser for

[143] Se mer om dette i punkt 4.5.1 og 4.5.2.
[144] Se *Camenzind v. Switzerland* avsnitt 45 og 26, og *Kruslin v. France* avsnitt 34.
[145] Jf. strpl. § 216 o og § 216 p. Se mer om dette under punkt 4.5.
[146] "Pressing social need", jf. *Olsson v. Sweden* avsnitt 67 og *Dudgeon v. The United Kingdom* avsnitt 51-53.

den bruken av middelet rettes mot, rettssikkerhetsgarantier og nytteverdien sett mot inngrepet.[147]

[147] Se *Klass and Others v. Germany* avsnitt 50.

3 Historikk

3.1 Norsk historikk

Innføringen av dataavlesing og den lovtekniske gjennomføringen ble drøftet lenge før det rent faktisk ble vedtatt. *Lund-kommisjonen* var først ute i 1996 med å granske politiets bruk av overvåkningstjenester, og i hvilken grad det forelå irregulær eller ulovlig overvåking av norske borgere.[148] Kommisjonen fikk i oppgave å utrede i hvilken grad ulovlig eller irregulær overvåking av norske borgere forekom etter 1945. Det ble også vedtatt en særlov som ga granskingskommisjonen myndighet som en domstol til å avhøre vitner direkte for kommisjonen.[149] Granskingskommisjonen konkluderte med at det *hadde* foregått ulovlig politisk overvåkning i Norge etter andre verdenskrig, primært av kommunister og sosialister, som på den tiden ble antatt å utgjøre en trussel mot rikets sikkerhet under den kalde krigen.[150]

I anledning lovendringen av straffeprosessloven i 1999 ble *Kriminaletterretningsutvalget* oppnevnt til å undersøke og drøfte politiets etterforskningsmetoder for bekjempelse av kriminalitet.[151] Utvalget utredet hvilke muligheter politiet hadde for skjult etterforskning. Det ble med grunnlag i deres vurderinger innført en lovendring som ga politiet hjemmel til å gjennomføre kommunikasjonskontroll (avlytting og annen kontroll av kommunikasjon) i en rekke saker. Det ble videre åpnet for utsatt underretning om ransaking, beslag og utleveringspålegg samt at politiets bruk av teknisk sporing ble lovfestet og utvidet. Ved samme lov ble det innført en ordning med oppnevning av forsvarer for den mistenkte ved bruk av skjulte tvangsmidler, jf. straffeprosessloven § 100 a.

Etter hvert som behovet for å kunne bruke skjulte tvangsmidler i etterforskning økte, ble regelverket vurdert igjen i NOU 2003: 18 av *Lund-utvalget*, og senere av *Politimetodeutvalget* i NOU 2004: 6. *Lund-utvalget* fikk blant annet i oppgave å "vurdere om det er behov for å endre reglene om etterforskningsmetoder for de aktuelle typer av forbrytelser og/eller for

---

[148] Dok nr. 15 (1995-1996) – *Rapport til Stortinget* side 1 – "Kommisjonens oppnevnelse og mandat".
[149] Lov 25. mars 1994 nr. 6 om granskingskommisjonen for gransking av påstander om ulovlig overvåking av norske borgere.
[150] Prop. 68 L (2015-2016) side 13.
[151] NOU 1997: 15.

saker om terrorisme". I dette inngikk spørsmålet om bruk av spesielle data-baserte metoder i etterforskning, og det var her dataavlesing i realiteten ble tatt opp for første gang i norsk rett. Spørsmål rundt personvern ble her tatt opp, og Lund-utvalget benyttet Kriminaletterretningsutvalgets funn i sine drøftelser.

Lund-utvalget problematiserte behovet for å anvende "spesielle datatekniske metoder i etterforskningen, herunder ulike dataprogrammer - såkalte trojanske hester, ormer, sniffere mv".[152] Utvalget konkluderte med at det var naturlig å overlate vurderingen av ulike IKT-relaterte metoder til *Datakrimutvalget*. Datakrimutvalget ble oppnevnt av regjeringen 11. januar 2002, og la i NOU 2003: 27 frem et forslag til lovtiltak mot datakriminalitet.

I 2004 foreslo *Politimetodeutvalget* å innføre regler som ville tillate dataavlesing som forebyggende metode.[153] Utvalget begrunnet forslaget i at kommunikasjonskontroll ikke lenger var teknologisk avansert nok til å sikre politiet tilgang til krypterte meldinger, og at eneste måte å få tak i innholdet på var å fange opp meldinger før de krypteres.[154] Justisdepartementets vurdering etter høringen var at dataavlesing var en etterforskningsmetode som det var behov for å vurdere nærmere.[155]

Utvalgenes forslag ble delvis fulgt opp i Ot.prp.nr. 60 (2004-2005), og var delvis bakgrunnen for lovendringen i 2005.[156] Det ble her åpnet for romavlytting som etterforskningsmetode, og for å anvende tvangsmidler i avvergende og forebyggende øyemed. Politiet ble også nå gitt adgang til å identifisere mobiltelefoner og andre kommunikasjonsanlegg. Dataavlesing ble derimot ikke innført denne gangen heller.

Datakrimutvalget var så vidt borti spørsmålet igjen i 2007, da de nevnte dataavlesing som begrep.[157] Utvalget konkluderte med at dataavlesing som metode, bør behandles ved senere utredningsarbeid.[158] Etter dette gjorde Metodekontrollutvalget i 2009 en grundig evaluering av politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker. Igjen

---

[152] NOU 2003: 18 Rikets sikkerhet, Straffelovkommisjonens delutredning VIII punkt 8.1.2 side 126-127.
[153] NOU 2004: 6 Mellom effektivitet og personvern
[154] NOU 2004: 5 Side 179; Se også Prop. 68 L (2015-2016) side 239
[155] Ot.prp. Nr. 60 (2004-2005) side 141 punkt 11.3
[156] Lov 17. juni 2004 nr. 87 om rettergangsmåten i straffesaker
[157] NOU 2007:2 Lovtiltak mot kriminalitet side 47.
[158] NOU 2007: 2 Side 47

kom dataavlesing opp som metode, hvor utvalget foreslo å innføre dataavlesing som ledd i gjennomføringen av de eksisterende metodene, og ikke som et nytt selvstendig tvangsmiddel.[159]

I Prop. L 68 (2015-2016) om endringer i straffeprosessloven, la Justisdepartementet frem et forslag om lovendring som ga utvidet tilgang til bruk av skjulte tvangsmidler ved etterforskning, avverging og forebygging av alvorlige lovbrudd. Proposisjonens drøftelser følger dels opp Metodekontrollutvalgets utredning av 2009, men departementet fremmet her et forslag om dataavlesing som *selvstendig* tvangsmiddel, hvor politiet gis adgang til å fortløpende overvåke et datasystem i sanntid. Departementet konkluderte med at behovet for dataavlesing var sterkere enn Metodekontrollutvalget hadde kommet til, men sluttet seg til at behovet ikke kunne tallfestes.[160] Behovet ble begrunnet i at kommunikasjonskontroll ikke lenger kunne gi like effektiv forskning som dataavlesing ble ansett å tilby. Dataavlesing ble endelig inntatt i norsk lov ved lovendringen i 2016.[161]

3.2 Svensk og dansk rett

Norske lovgivere ser ofte hen til svensk og dansk rett ved lovendringer av flere grunner. For det første har Norge, Sverige og Danmark sammenfallende rettstradisjoner som del av den nordiske rettskretsen, hvor rettssystemene historisk sett har vært preget av liknende juridisk tankegang og rettsutvikling. Dette gjør at rettsprinsipper og lovgivning i de tre landene i stor grad kan være sammenlignbare.

Hvis Sverige eller Danmark er tidligere ute med en lovendring, kan det i noen tilfeller skape et press i retning av lignende endringer i norsk rett, spesielt når endringene bidrar til løsninger på grenseoverskridende utfordringer, som for eksempel miljøvern, digitalisering og

[159] NOU 2009: 15 side 247
[160] Innst. 343 L (2015-2016) punkt 1.15 "Økonomiske og administrative konsekvenser". "Det foreligger ikke detaljerte data for medgåtte ressurser knyttet til eksisterende lovgivning om politiets bruk av skjulte tvangsmidler. Det er derfor vanskelig å tallfeste merkostnadene ved lovendringer."
[161] Prop. 68 L (2015-2016).

personvern. I tillegg kan nordiske rettsavgjørelser noen ganger ha en viss presedensvirkning, i den forstand at de kan være veiledende eller ha en viss overtalelseseffekt.[162]

Sverige innførte ikke dataavlesing som selvstendig etterforskningsmetode før 1. april 2020, selv om utredningsarbeidet startet allerede i 2016.[163] De åpnet før den tid for kommunikasjons*avlytting* ved "*hemlig avlyssning av elektronisk kommunikation*" i etterforskningsøyemed.[164]

I likhet med det norske kriminalitetsbildet stod Sverige foran en økende internasjonalisering, og rask teknologisk utvikling hvor kryptering særlig var en utfordring.[165] Det ble fremmet et lovforslag i 2017 om å innføre dataavlesing, og den svenske regjeringen leverte proposisjonen "Hemlig dataavläsning" til Riksdagen i desember 2019, som ble vedtatt 19. februar 2020 og trådte i kraft 1. april 2020.[166]

Når det gjelder Sveriges senere innføring kan Norge, med sin tidligere erfaring, ha utviklet en mer sofistikert tilnærming til dataavlesing som kan ha vist seg nyttig for Sverige å vurdere når de utformet sine egne lover og reguleringer. Forskjellen i tidspunkt for innføring av dataavlesing betyr ikke nødvendigvis at Norge ikke kan dra nytte av svensk lovgivning og erfaringer i senere juridisk utvikling, da alle tre land regelmessig samarbeider for å lære av hverandre og forbedre sine egne juridiske systemer. Svensk rett har derimot neppe påvirket norsk rett i særlig bemerkelsesverdig grad i dette tilfellet, ettersom de var senere ute med innføringen av dataavlesing.

Danmark innførte dataavlesing i 2002 i forbindelse med blant annet anti-terrortiltak. [167] Hovedfokuset deres var å skape en lovgivning som kunne sikre effektiv terrorbekjempelse uten å forringe borgeres grunnleggende rettigheter.[168]

---

[162] I samtid skjer dette for eksempel i debatten om samtykkelov skal innføres i norsk straffelovgivning. Sverige innførte samtykkelov i 2018, og mange av argumentene for å innføre en liknende lov i Norge bygger på svenske erfaringer.
[163] SOU 2017: 89 side 596.
[164] Se Prop. 68 L (2015-2016) side 231-232.
[165] SOU 2017: 89 side 596.
[166] Prop. 2019/ 20:64, se også vedtaket av prop. 2019/ 20:77 side 109-111.
[167] Danmark innførte bestemmelser om dataavlesing ved lov nr. 378 av 6. juni 2002 i Retsplejeloven § 791 b.
[168] Prop. 68 L (2015-2016) side 231.

Danmarks tidlige innføring av dataavlesing hadde flere relevante aspekter for norsk rett. Ved innføringen av dataavlesing, så lovgiver hen til både dansk og svensk rett. Den danske retsplejeloven, som inneholdt regler om ulike former for tvangsmidler, herunder § 791 b om dataavlesing, ble vurdert i forarbeidene til lovendringen. Bestemmelsen gir danske myndigheter mulighet til å anvende dataavlesing under visse vilkår, og gir en detaljert ramme for hvordan og når slik dataavlesing kan foretas. Dette inkluderer kriterier for når det er tillatt å lese av data fra et informasjonssystem og prosedyrer for rettens godkjenning og tilsyn med anvendelsen av slike tvangsmidler.

Ved lovendringen tok Justisdepartementet stilling til den erfaringen dansk rett hadde hatt. Det danske Justitsministeriet redegjorde for sine erfaringer i "Redegørelse om erfaringerne med lovgivning indført i forbindelse med anti-terrorpakke I fra 2002 og anti-terrorpakke II fra 2006".[169]

Politiets Efterretningstjeneste rapporterte i den anledning at dataavlesning hadde spilt en sentral rolle i etterforskning av narkotikasaker og barneovergrepsaker. Metoden hadde et betydelig potensial som et komplement til ransakning og viste seg å være en svært nyttig etterforskningsmetode.[170]

Metodekontrollutvalget for lovendringen av straffeprosessloven kontaktet også den danske riksadvokaten, og forespurte blant annet statistikk som demonstrerer behovet for og effektiviteten av dataavlesning. Konkrete eksempler på hvordan denne metoden har vært avgjørende i etterforskningen og rettsprosessen av kriminelle handlinger var også av interesse. Utvalget ba videre om en vurdering av metoden for ulike typer kriminalitet, og spesielt hvordan dataavlesing har bidratt med ytterligere informasjon sammenliknet med andre tvangsmidler som kommunikasjonskontroll og ransaking/beslag.[171]

PET opplyste at det ikke finnes oversikt over antallet dataavlesinger i Danmark, og at det heller ikke kan fremskaffes slike opplysninger fra politiets saksbehandlingssystem. Riksadvokaten har likevel opplyst å være kjent med at dataavlesing

[169] Datert 9. september 2010.
[170] Se Prop. 68 L (2015-2016) side 230.
[171] Prop. 68 L (2015-2016) side 231.

har vært anvendt i en rekke konkrete saker, herunder to saker om forsøk på terror. I begge disse sakene ble det gjennomført dataavlesing av de siktedes datamaskiner. Dette frembrakte bevis for at de senere domfelte hadde nedlastet bombemanualer, hadde søkt etter kjemikalier mv. som kunne brukes til bombefremstilling, og hadde kommunisert via datamaskiner i tilknytning til planleggingen av forbrytelsene.[172]

Norske lovgivere har derfor kunnet dra nytte av de danske erfaringene, både med hensyn til hvordan reguleringen er strukturert, og ikke minst hvordan den har fungert i praksis. Ved å undersøke de praktiske virkningene av den danske lovgivningen, kunne norske myndigheter vurdere potensielle fordeler og ulemper ved å implementere en lignende eller tilpasset løsning i norsk rett. Det fremgår at de danske erfaringene med dataavlesing har vært i stor grad positive, og bruken av denne metoden har vært effektiv i etterforskning av blant annet terrorhandlinger og andre alvorlige forbrytelser.

Det skal imidlertid bemerkes at enhver innføring av nye tvangsmidler i norsk rett vil måtte tilpasses norsk rettskultur, og norske grunnlovsverdier. Norge kan ha sett på Danmarks erfaringer og praksis som en slags modell eller inspirasjonskilde når de utformet sine egne bestemmelser om dataavlesing, men i hvilken grad lovgiver vektla danske erfaringer er umulig å si.

[172] Prop. 68 (2015-2016) side 231

4 Vilkår for å gjennomføre dataavlesing

4.1 Grunnvilkår

Som tidligere nevnt er tvangsmidler metoder som anvendes mot en persons vilje i etterforskningsøyemed.[173] Skjulte tvangsmidler går et steg lengre enn ordinære tvangsmidler, ved at den tiltaket rettes mot ikke opplyses om inngrepet før etter det er gjennomført.

Bruk av tvangsmidler vil alltid innebære et inngrep overfor den enkelte, og krever derfor hjemmel i lov.[174] Bruk av tvangsmidler er videre begrenset av forholdsmessighets- og nødvendighetskravet.[175] For dataavlesing knytter forholdsmessighetsvurderingen seg også til måten avlesingen gjennomføres og innrettes på, hvilket reguleres i § 216 p andre ledd. Politiet skal så langt det er mulig unngå at andre enn mistenktes bruk fanges opp.

Det følger av de enkelte bestemmelsene hvilke vilkår som må være oppfylt for å benytte et tvangsmiddel, men de fleste bestemmelsene inneholder et mistankekrav, et strafferammekrav, et formålskrav, og et kompetansekrav. For skjulte tvangsmidler gjelder det også et indikasjons- og subsidiaritetskrav.

For helhetens skyld vil det nærmere innholdet i mistankekravet drøftes etter de overordnede vilkårene for dataavlesing er redegjort for. Vilkårene i strpl. § 216 o sammenfaller i stor grad med de prinsipper og hensyn som tidligere er redegjort for, og det er derfor hensiktsmessig å presentere de overordnede vilkårene først.

4.2 Overordnet om de materielle vilkårene i § 216 o

4.2.1 Introduksjon

Tvangsmiddelet dataavlesing reguleres av henholdsvis strpl. § 216 o og § 216 p. § 216 o regulerer de materielle vilkårene, og § 216 p regulerer de personelle og prosessuelle vilkårene. Ordlyden i § 216 o lyder slik:

---

[173] Se punkt 1.1.
[174] Jf. det alminnelige legalitetsprinsippet, og EMK art. 8 nr. 2.
[175] Jf. Strpl. § 170 a. Mer om dette under punkt 4.2.5

"Retten kan ved kjennelse gi politiet tillatelse til å foreta avlesing av ikke offentlig tilgjengelige opplysninger i et datasystem (dataavlesing) når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling

a. som etter loven kan medføre straff av fengsel i 10 år eller mer

b. som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 129, 136, 136 a, 136 b, 232, 254, 257, 311, 333, 337 jf. 231, eller 340 jf. 231, eller av lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v. § 5 eller av lov om utlendingers adgang til riket og deres opphold her § 108 femte ledd.

Dataavlesing kan besluttes selv om straff ikke kan idømmes på grunn av bestemmelsene i straffeloven § 20. Det gjelder også når tilstanden har medført at den mistenkte ikke har utvist skyld.

Tillatelse etter første ledd kan bare gis dersom det må antas at dataavlesing vil være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort. § 216 c annet ledd gjelder tilsvarende.

Det kan bare gis tillatelse til å avlese bestemte datasystemer eller brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester som den mistenkte besitter eller kan antas å ville bruke. Avlesingen kan omfatte kommunikasjon, elektronisk lagrede data og andre opplysninger om bruk av datasystemet eller brukerkontoen.

§§ 216 d til 216 k gjelder tilsvarende, likevel slik at rettens tillatelse ikke kan gis for mer enn to uker om gangen. Eventuelt utstyr som er benyttet for å gjennomføre dataavlesingen skal fjernes snarest mulig etter avlesingsperiodens utløp".

Strpl. § 216 o første ledd åpner med at det gis adgang til å "foreta avlesning av ikke offentlig tilgjengelige opplysninger i et datasystem (dataavlesing)". En alminnelig tolkning av ordet "dataavlesing" tilsier adgang til å lese av innhold i et ″datasystem″, typisk datamaskin eller mobiltelefoner. Med ″datasystem″ forstås blant annet smarttelefoner, datamaskiner og andre enheter som behandler data ved hjelp av dataprogrammer.[176] Avlesing etter § 216 o er ment å

[176] Prop. 68 L (2015-2016) side 270.

treffe "bestemte" datasystemer eller brukerkontoer, og dette må for øvrig også fremgå tydelig av politiets begjæring, og i rettens kjennelse.[177] Dette er kjernen av det jeg vil problematisere i EncroChat-dommen, og jeg vil derfor se nærmere på dette under punkt 4.4.2. For helhetens skyld presenteres de konkrete vilkårene for dataavlesing etter § 216 o først.

Dataavlesing er begrenset til å gjelde i maksimalt to uker, jf. § 216 o siste ledd. Inngrepet skal i utgangspunktet bare fange opp den data som produseres, lagres, sendes, lastes ned, eller kommuniseres innenfor dette tidsrommet, men kan i praksis fange opp all data som er lagret i et datasystem. Dataavlesing skal ikke foregå lengre enn det som er strengt nødvendig for å oppnå formålet. Uavhengig av tidsbegrensningen, skal politiet stanse avlesingen dersom vilkårene ikke lenger antas å være til stede, eller dataavlesing ikke lenger anses hensiktsmessig, jf. strpl. § 216 f annet ledd.[178]

Etterforskning som innebærer bruk av dataavlesing, har også et krav om å være *formålsstyrt*.[179] I dette ligger at informasjonsinnhenting og videre behandling av det som fanges opp må gjøres i tråd med bestemte saklige formål.[180]

Dersom alle vilkårene i strpl. § 216 o er oppfylt, er utgangspunktet at tvangsmiddelet kan benyttes. Strpl. § 216 c annet ledd skjerper vilkårene for å benytte dataavlesing i etterforskning dersom den mistenktes kommunikasjonsanlegg "er tilgjengelig for et større antall personer". Det må i slike tilfeller foreligge "særlige grunner" for å anvende skjulte tvangsmidler som dataavlesing eller kommunikasjonskontroll, jf. annet ledd første punktum.

Bestemmelsen nevner uttrykkelig at slike personer kan være en "advokat, lege, prest eller andre som erfaringsmessig fører samtaler av svært fortrolig art over telefon eller redaktør eller journalist". Dataavlesing kan fortsatt utføres mot personer innenfor denne gruppen, men terskelen er noe strengere. Hensikten bak dette er at dette er en gruppe mennesker som naturlig kommuniserer med sensitiv informasjon. Eksempelvis vil pressens kilder være av sentral betydning i et samfunn som bygger på demokrati og ytringsfrihet. Dersom deres

---

[177] Prop. 68 L (2015-2016) side 270. Mer om dette under punkt 4.4.1.
[178] Se også Prop. 68 L (2015-2016) side 273.
[179] Se Prop. 68 L (2015-2016) side 242 med henvisning til 2.2 artikkel 6 første ledd bokstav b. Europarådskonvensjonen artikkel 5 bokstav b og EUs rammebeslutning artikkel 3 nr. 1 og 2.
[180] Se NOU 2009: 15 side 54-55.

kommunikasjon ikke vernes tilstrekkelig, vil det kunne føre til at kritikkverdige forhold i samfunnet og andre forhold av samfunnsmessig interesse ikke kommer frem.[181]

Dataavlesing har i praksis et potensiale for å gå mye lengre i dens tilgang til informasjon, sammenlignet med kommunikasjonsavlytting og for eksempel hemmelig ransaking. Som tidligere nevnt får politiet ved bruk av dataavlesing ukryptert tilgang til *all* informasjon som avleses i perioden det gjennomføres.[182] Avlesing vil kunne omfatte lydstrøm tilknyttet mikrofon og høyttalere, videostrøm, alle tastetrykk på mistenktes tastatur, innhold på harddisk, og internettlogg og øvrig data i sanntid.[183] Dette vil i praksis innebære at også det mistenkte kun taster på tastaturet, men ikke sender eller laster opp på annet vis, vil kunne avleses. Mistenktes tanker, assosiasjoner, og ønsker som ikke nødvendigvis skal kommuniseres, vil dermed kunne bli gjenstand for avlesing.[184]

4.2.2 Mistankekravet

Det første vilkåret for å kunne gjennomføre dataavlesing er at "noen" med "skjellig grunn mistenkes for en handling eller forsøk på en handling", jf. § 216 o første ledd første punktum, jf. bokstav a og b.[185] Ordlyden er et utslag av det alminnelige mistankekravet som gjelder for de fleste bestemmelser om metodebruk i straffeprosessloven.[186]

Med "skjellig grunn" menes det at mistanken må bygge på objektive, konkrete forhold. Den må være forankret i faktiske, påviselige, og dermed etterprøvbare, omstendigheter. Det kreves at det er mer sannsynlig enn ikke at den inngrepet vil rette seg mot, har begått eller forsøkt å begå den straffbare handlingen.[187] Formuleringen "skjellig grunn [til mistanke]" er

---

[181] Prop. 147 L (2012-2013) side 133.
[182] Se punkt 1.2.1.
[183] Prop. 68 L (2015-2016) side 224.
[184] Prop. 68 L (2015-2016) side 252.
[185] Ordet "noen" kan tolkes som at mistanken til en viss grad må være individualisert, eller rettet mot et spesifisert individ. Jeg vil se nærmere på dette under punkt 4.2.1.1 "Kravet til individualisering av mistanken".
[186] Prop. 68 L (2015-2016) side 269. Se også NOU 2004: 6 side 49 og Ot.prp.nr. 60 (2004-2005) side
[187] Ordlydstolkningen utledes fra Rt. 1993 s. 1302, hvor Høyesteretts kjæremålsutvalg behandlet en anke over kjennelse om varetektsfengsling. Høyesterett la til grunn Lagmannsrettens forståelse av ordlyden "skjellig grunn til mistanke", som bygget på at "det skal være mer sannsynlig at siktede har begått den straffbare handling saken gjelder, enn at han ikke har det". Se også HR-2019-2282-U avsnitt 11-12.

gjennomgående i straffeprosessloven. Lovgivers bevisste valg av å gjenta denne ordlyden taler for at den skal tolkes forholdsvis likt.

4.2.3 Strafferammekravet

Strafferammekravet – også kjent som kriminalitetskravet, stiller krav til alvorlighetsgraden til den straffbare handlingen som mistanken knytter seg til. Dagens metodebruk avgrenses i hovedsak av dette kravet, med enkelte eksempler på konkrete aktuelle straffebud. Strpl. § 216 o første ledd deler strafferammekravet i to. Bokstav a fremmer et overordnet krav om at strafferammen for den straffbare handlingen må være minst 10 år. Hvilken straff mistenkte rent faktisk forventes å motta, er ikke relevant. Tidsrammen som angis i straffebudet skal legges til grunn (den abstrakte strafferammen).[188]

Straffeprosessloven § 216 o første ledd bokstav b viser til konkrete straffebud med lavere strafferamme enn 10 år, men som "på grunn av sine samfunnsskadelige konsekvenser eller særlige etterforskningsmessige utfordringer, kan forsvare en adgang til også å kunne iverksette skjult kameraovervåking på privat sted, slik som ved kommunikasjonskontroll". [189] Eksempelvis vil tilfeller som bokstav b er ment å dekke være knyttet til særlig organisert virksomhet, som utføres på måter som er vanskelig å avdekke; Typisk menneskehandel, produksjon og spredning av overgrepsmateriale av barn, organisering og planlegging av terror, og narkotikaovertredelser.[190] Felles for slike typer saker er at det gjerne er en fornærmet som ikke har evne eller vilje til å bidra til oppklaring. Dermed vil også oppklaring av saken i sin helhet bli vesentlig vanskeligere.

Strafferammekravet gjenspeiler hvor inngripende de ulike metodene er ansett å være.[191] Ved å sette en grense på minimum ti år, vil de mest alvorlige forbrytelsene omfattes av hjemmelen for dataavlesing. Strafferammekravets funksjon som en grunnleggende betingelse er sådan å

[188] Høyesterett uttalte i Rt. 2006 s. 1398 tredje avsnitt at det er "straffebudenes abstrakte strafferamme som er avgjørende for adgangen til å fengsle". Den straffbare handlingen må altså *kunne medføre* ti års fengsel, men dommen må ikke konkret være 10 års fengsel.
[189] Prop. 68 L (2015-2016) side 167
[190] Prop. 68 L (2015-2016) side 268
[191] Prop. 68 L (2015-2016) side 42.

begrense tilgangen til metoder mot straffbare handlinger som lovgiver ikke har regnet som tilstrekkelige til å rettferdiggjøre bruk av skjulte tvangsmidler.

Kravet innebærer ikke i seg selv en vurdering av om skjulte tvangsmidler kan brukes, dette må vurderes ut fra de øvrige vilkårene. Det sier derimot noe om alvorlighetsgraden av den straffbare handlingen.

4.2.4 Indikasjons- og subsidiaritetskravet

Det tredje vilkåret er at det må foreligge et *reelt behov* for dataavlesing. Det følger av § 216 o tredje ledd at dataavlesing bare kan tillates dersom det "må antas at dataavlesing vil være av vesentlig betydning for å oppklare saken," (indikasjonskravet)[192] og at "oppklaring ellers i vesentlig grad vil bli vanskeliggjort". (subsidiaritetskravet).[193] Vilkårene skal forstås på samme måte som i bestemmelsene om hemmelig ransaking, kommunikasjonskontroll, og romavlytting.[194]

Indikasjonskravet innebærer at metodebruken (her dataavlesing) må ha noen konkrete holdepunkter som tilsier at det vil frembringes opplysninger av stor betydning for etterforskningen i saken.[195] Ordlyden "må antas" stiller et krav om en viss grad av sannsynlighet, men det er ikke et krav om sannsynlighetsovervekt.[196] Det kreves noe mer enn "ren formodning" eller vag mistanke.[197] For eksempel vil ikke spekulasjoner eller rykter være tilstrekkelig.

Subsidiaritetskravet innebærer at mer inngripende tiltak bare skal benyttes dersom mindre inngripende metoder ikke kan oppnå samme resultat.[198] Kravet er en skjerping av nødvendighetskravet.[199] Eksempelvis kan det vurderes om det er nødvendig å benytte dataavlesing for å etterforske et individ som er mistenkt for salg av narkotika. Typisk i slike situasjoner er at mistenkte da kommuniserer via mobiltelefon for å avklare de nærmere

---

[192] Prop. 68 L (2015-2016) side 230.
[193] Prop. 68 L (2015-2016) side 44.
[194] Jf. henholdsvis strpl. § 200 a annet ledd, § 216 c første ledd og § 216 m tredje ledd.
[195] Prop. 68 L (2015-2016) side 88. Se også Rt. 2005 s. 199 og Ot.prp.nr. 60 (2004-2005) side 71.
[196] Se Rt. 2005 s. 199
[197] Se ot.prp.nr. 60 (2004-2005) side71
[198] Prop 68 L (2015-2016) side 88.
[199] Se punkt 4.2.5 nedenfor.

detaljene for slike salg. Dataavlesing vil utvilsomt i et slikt tilfelle være tilstrekkelig for å oppnå ønsket formål, altså å avdekke nødvendig informasjon om at et slikt salg foregår. Men i lys av subsidiaritetskravet må man gjøre en vurdering av om for eksempel kommunikasjonsavlytting etter § 216 a heller kan benyttes, eller om man kan avhøre siktede direkte. I saker hvor dataavlesing vil være aktuelt, vil avhøring av siktede mest sannsynlig ikke være tilstrekkelig. På den annen side krever ikke subsidiaritetskravet at andre metoder *må* ha vært forsøkt, men det må foretas en konkret helhetsvurdering av omstendighetene i hver enkelt sak for å avgjøre om dataavlesing vil fremstå som mer eller mindre inngripende enn andre tvangsmidler.[200]

4.2.5 Forholdsmessighets- og nødvendighetskravet

Det fjerde vilkåret for å kunne benytte dataavlesing er at inngrepet må være forholdsmessig og nødvendig, jf. strpl. § 170 a.[201] Forholdsmessighetsprinsippet nevnes ikke uttrykkelig i ordlyden til § 216 o, men gjelder tilsvarende for alle tvangsmidler i straffeprosessloven.[202] Dersom dataavlesing vil være et uforholdsmessig inngrep, kan det ikke tillates uavhengig av om de øvrige vilkårene er oppfylt.[203] Forholdsmessighetsvurderingen etter strpl. § 170 a sammenfaller i stor grad med den vurderingen som gjøres av et inngreps forholdsmessighet, jf. EMK artikkel 8 nr. 2.[204]

Forholdsmessighetskravet innebærer som nevnt i punkt **Error! Reference source not found.** at et tvangsmiddel må være egnet for å oppnå etterforskningsformålet, være så lite inngripende som mulig, og det må være nødvendig.[205]

Kravet til nødvendighet fremgår av ordlyden "tilstrekkelig grunn", jf. strpl. § 170 a første punktum. Tiltaket eller tvangsmiddelet må altså være av en slik art at det er egnet til å oppfylle formålet som inngrepet søker å oppnå.[206] Normalt anses kravet oppfylt dersom målet

[200] Prop. 68 L (2015-2016) side 269; Se også NOU 2009: 15 side 178.
[201] Se også EMK. Artikkel 8 nr. 1
[202] Jf. Strpl. § 170 a.
[203] Prop. 68 L (2015-2016) side 269.
[204] HR-2023-2224-A avsnitt 44.
[205] Prop. 42 L (2023-2024) Endringer i straffeloven side 46
[206] Se NOU 2016: 24 side 312-313.

med rimelighet ikke kan oppnås på en annen måte.[207] Minste inngreps-prinsipp gjelder også her, altså jo mer inngripende tvangsmiddelet er, jo strengere er kravet til nødvendighet.[208]

Terskelen for hva som anses "nødvendig" for å oppnå et formål vil avhenge av en tolkning av de faktiske omstendighetene i saken.[209] Det må foreligge et minimum av nødvendighet for at bruken av et tvangsmiddel skal være forholdsmessig. For skjulte tvangsmidler kan de bare anvendes dersom bruken av tvangsmidlet "vil være av vesentlig betydning for å oppklare saken" og "oppklaring ellers i vesentlig grad vil bli vanskeliggjort".[210]

Retten må i lys av ordlyden i strpl. § 216 o tredje ledd "vesentlig betydning for å oppklare saken", vurdere om innbrudd av datasystemet medfører at avlesingen utgjør et uforholdsmessig inngrep. Det vil naturlig være slik at dersom indikasjons- og subsidiaritetskravet er oppfylt, vil kravet til nødvendighet naturlig også kunne anses oppfylt.

Som redegjort for under punkt 2.3.7 vil prosessuelle garantier spille en rolle i vurderingen av om et inngrep er forholdsmessig. En svakhet i en av de prosessuelle garantiene kan imidlertid avbalanseres ved at det implementeres andre rettssikkerheter.[211] Som tidligere nevnt skal dataavlesing i utgangspunktet besluttes gjennom rettslig kjennelse.[212] Strpl. § 216 d åpner derimot for at hastekompetanse kan benyttes. Dette kommer jeg nærmere tilbake til under punkt 4.5.2.

4.3 Forholdet mellom dataavlesing, kommunikasjonskontroll, og sammenlignbare tvangsmidler

Det nevnes i straffeprosesslovens forarbeider at dataavlesing "kan oppleves mer inngripende enn kommunikasjonskontroll og hemmelig ransaking".[213] I et slikt tilfelle vil det som tidligere

[207] Se Ot.prp.nr. 64 (1998-1999) side 20.
[208] NOU 2016: 24 side 313.
[209] Se *Klass and Others v. Germany* avsnitt 49-50.
[210] Se strpl. § 200 a annet ledd, § 202 a annet ledd, § 202 c annet ledd, § 216 c første ledd, § 216 o tredje ledd, og § 216 m tredje ledd, se også punkt 4.2.4 indikasjons- og subsidiaritetskravet.
[211] Se punkt 2.3.7.
[212] Jf. strpl. § 216 o, se også punkt 2.3.7.
[213] Prop. 68 L (2015-2016) side 268.

nevnt være naturlig å anta at forholdsmessighetskravet da er strengere ved bruk av dataavlesing, enn for skjult ransaking og kommunikasjonskontroll.

Dataavlesings evne til å fange opp opplysninger som ikke var ment å kommuniseres til noen, eller å kunne lagres er en av begrunnelsene for at det sies å kunne "oppleves" mer inngripende.[214] Individets ufiltrerte tanker vil slik kunne bli utsatt for avlesing, uten at vedkommende har noen kunnskap om det.

Til dette har lovgiver uttalt en enighet i at politiets mulighet til å "tilegne seg kunnskap om enkeltindividers personlige betraktninger, medfører et vesentlig personverninngrep", men at dette ikke er noe nytt.[215] Det påpekes at skjult dataavlesing rettslig sett ikke skiller seg fra politiets anledning til å gjennomføre hemmelig ransakelse, og ta beslag i mistenktes dagbok, notater, eller tilsvarende. I realiteten bør det da ikke ha noe å si om informasjonen er lagret fysisk eller elektronisk.[216]

Justisdepartementet uttaler til dette at "forslaget om dataavlesing ikke åpner for mer vesentlige inngrep, i form av innsyn i personlig informasjon som er lagret elektronisk, enn adgangen som allerede følger av gjeldende rett".[217] Videre at selv om dette vil oppleves som et vesentlig personverninngrep, kan det likevel ikke veie tyngre enn "de viktige samfunnsinteressene som søkes vernet ved å gi politiet anledning til å benytte effektive virkemidler i bekjempelsen av alvorlig kriminalitet".[218]

Basert på uttalelsene i forarbeidet, fremstilles dataavlesing som et inngrep som er nokså sammenlignbart med andre skjulte tvangsmidler. Politiet gis ikke nødvendigvis tilgang til vesentlig mer eller personlig informasjon ved bruk av dataavlesing. Eksempelvis kan bestemmelsene om ransaking og beslag gi politiet tilgang til å ta speilkopi av individers mobiltelefoner, som kan inneholde alt fra private bilder, notater, dokumenter, og meldinger som finner sted over en mye lengre periode enn bare to uker. Dataavlesing er derimot som

[214] Prop. 68 L (2015-2016) side 265.
[215] Prop. 68 L (2015-2016) side 265.
[216] Prop. 68 L (2015-2016) side 265.
[217] Prop. 68 L (2015-2016) side 266.
[218] Prop. 68 L (2015-2016) side 266.

nevnt begrenset til to uker, men åpner for å kunne gi tilgang til all informasjon som er lagret på et datasystem.[219]

Tilsynelatende er det en "tilstedeværelse over tid" som gjør at dataavlesing hevdes å kunne oppleves som "mer inngripende".[220] Det er etter mitt synspunkt noe betenkelig hvorfor dette skal være avgjørende for hvorfor dataavlesing oppfattes som "mer" inngripende. Tilgangen til informasjon vil, i min mening, være det som føles inngripende for mistenkte. Det skjulte aspektet er også et moment som bidrar til at metoden kan føles mer inngripende ut, ettersom mistenkte ikke gis noen mulighet for å beskytte seg. Dette er derimot et nødvendig onde, ettersom metoden som tidligere nevnt vil miste sin tiltenkte effekt dersom mistenkte har mulighet til å innrette seg, og dermed forandre atferd.[221]

Den mest sentrale forskjellen mellom dataavlesing, kommunikasjonsavlytting og hemmelig ransaking er at dataavlesing gir tilgang til *dekryptert* informasjon, og informasjonsavlesing i sanntid. Dersom politiet ved mobilbeslag tar en speilkopi av innholdet på siktedes telefon, vil fortsatt meldinger, bilder eller relevante opplysninger kunne være skjult bak kryptering (passord eller biometrisk godkjenning), eller kunne gå tapt for eksempel ved fjernsletting. Det er nettopp denne hindringen dataavlesing kommer forbi, som Justisdepartementet også nevner som en av de sentrale formålene ved innføring av metoden.[222] Dataavlesing åpner for å rette overvåking mot for eksempel en spesifikk enhet, mobiltelefon eller datamaskin som det er grunn til å tro at mistenkte benytter, eller en bestemt brukerkonto. Hvor kommunikasjonsavlytting innebærer overvåking av et kommunikasjonsanlegg, for eksempel en ruter eller en datamaskin som deles av flere, vil avlyttingen kunne gjøre tredjepersoner til objekt for informasjonsinnhenting. Når dataavlesing da snevrer inn objektet som overvåkes, vil dette også kunne skjerme tredjepersoner bedre mot personverninngrep.[223]

Selv om politiet allerede har anledning til å gjennomføre for eksempel hemmelig ransaking, og slik skaffe seg tilgang til eksempelvis dagbøker og personlige notater, forutsetter det at mistenkte fysisk *har* skrevet ned slike tanker eller betraktninger. Dersom mistenkte har tatt

---

[219] Prop. 68 L (2015-2016) side 264.
[220] Prop. 68 L (2015-2016) side 265.
[221] Jf. punkt **Error! Reference source not found.** ovenfor, med henvisning til *Adomaitis v. Lithuania* avsnitt 83.
[222] Prop. 68 L (2015-2016) side 264-265.
[223] Prop. 68 L (2015-2016) side 265.

steg for å beskytte slik informasjon, for eksempel ved å bruke krypteringsløsninger for å skrive ned slik informasjon, fratar dataavlesing mistenkte muligheten for i det hele tatt å beskytte denne informasjonen. På denne måten har lovgiver ved innføringen av dataavlesing forsøkt å kompensere for det effekttapet kommunikasjonsavlytting og hemmelig ransaking har hatt som følge av teknologisk utvikling.

Justis- og beredskapsdepartementet uttalte i forarbeidene at forholdsmessighetskravet vil ha særlig betydning for adgangen til dataavlesing i saker som gjelder lovbrudd med vesentlig lavere strafferamme enn 10 års fengsel.[224] Også den krenkelsen som ofre utsettes for ved kriminelle handlinger som åpner for dataavlesing vurderes i forarbeidene. Departementet nevner at det inngrepet dataavlesing utgjør overfor siktede, "kan være beskjedent sammenlignet med den krenkelsen som ofrene for den alvorlige kriminaliteten må tåle".[225] På denne måten avveies krenkelsen av siktedes privatliv mot offerets rett til beskyttelse, og politiets behov for effektiv kriminalitetsbekjempelse.

Spørsmålet er om Justisdepartementets uttalelse om at dataavlesing "kan oppleves som mer inngripende" er reelt. Argumenter kan fremmes for at kommunikasjonsavlytting og mobilransaking har potensiale til å frembringe samme type informasjon som dataavlesing, og dermed kan oppfattes som minst like inngripende. Videre gir som nevnt ikke dataavlesingsmetoden politiet automatisk adgang til kvantitativt mer eller kvalitativt mer sensitiv informasjon.

Forarbeidene fremhever gjentatte ganger likhetene mellom dataavlesing[226], hemmelig ransakelse[227] og kommunikasjonsavlytting.[228] Der kommunikasjonsavlytting gir adgang til å avlytte signastrøm fra en brukers enhet til tjenesteleverandørens kommunikasjonsanlegg, gir ikke det nødvendigvis et fullstendig bilde av informasjonen som utveksles på grunn av potensielle krypteringsløsninger.[229] Forholdene som gjør tvangsmiddelet nødvendig er likevel ofte de samme, dataavlesing innebærer i realiteten bare en måte å bryte barrierer på ved at

[224] Prop. 68 L (2015-2016) side 269.
[225] Prop. 68 L (2015-2016) side 265.
[226] Strlp. § 216 o
[227] Strpl. § 200 a
[228] Strpl. § 216 a
[229] Se blant annet Prop. 68 L (2015-2016) side 225-228; Prop. 68 L (2015-2016) side 260.

politiet får tilgang til data som er kryptert og dermed umulig å sikre ved alminnelig kommunikasjonskontroll.

Kommunikasjonskontroll foregår i likhet med dataavlesing innen et gitt tidsrom i en konkret situasjon hvor det foreligger skjellig mistanke, og det er en spesifikk enhet som kan avlyttes. Det samme gjelder for hemmelig ransaking, hvor det er mistenktes oppholdssted som kan ransakes. Dataavlesing kan som nevnt skje på tilnærmet samme vilkår, og forholdene som åpner for bruk av kommunikasjonskontroll og hemmelig ransakelse kan derfor også åpne for dataavlesing. Ettersom forholdene er tilnærmet de samme, kan dette tale for at dataavlesing *ikke* er mer inngripende enn hemmelig ransaking og kommunikasjonskontroll, eller til og med beslag. Den sentrale forskjellen ligger i potensialet for hvilken informasjon som kan avleses eller innhentes, og mengden. Dette vil også kunne avhenge av individet.

Bruk av et hvilket som helst tvangsmiddel vil kunne utgjøre et inngrep i den personlige sfære. Forskjellen ligger som sagt i at et inngrep i ens datasystem utgjør et inngrep på flere arenaer for den mistenkte.[230] Datasystemer inneholder typisk både dokumenter, notater, bilder, nettbank, søkelogg, sosiale medier, og all kommunikasjon med andre. Skal man ta utgangspunkt i den gjennomsnittlige forbruker, benyttes data i dag i *betydelig* større grad enn tidligere, og man legger igjen "spor" uavhengig av hva man gjør.[231]

En slik teknologisk utvikling som har ført til at kildene som gjøres til gjenstand for avlesing ligger *svært* nært individets tankevirksomhet, begrunner et særskilt behov for beskyttelse. Dersom dette er reelt, vil det kunne tale for at dataavlesing *er* mer inngripende enn tidligere skjulte etterforskningsmetoder. Dette vil derimot ikke nødvendigvis være like inngripende dersom man ser på en forbruker som avviser digitale kommunikasjonsanlegg – og kanskje utelukkende benytter analoge metoder som dagbøker eller fysiske notater, brev, eller liknende.

---

[230] Jf. punkt 4.2.1.

[231] Statistisk sentralbyrås statistikk for bruk av IKT i husholdningene fra 2023. https://www.ssb.no/teknologi-og-innovasjon/informasjons-og-kommunikasjonsteknologi-ikt/statistikk/bruk-av-ikt-i-husholdningene besøkt 29.02.2024.

Hensynet til personvern tilsier som tidligere nevnt at individer har en interesse i å kunne styre andres tilgang til sin personlige informasjon og sine forhold.[232] Ved bruk av dataavlesing, faller et slikt vern bort til fordel for hensynet til kriminalitetsbekjempelse. Justisdepartementet har også uttalt i forarbeidene at en slik krenkelse kan være "beskjeden" i sammenligning med den krenkelsen som ofrene for alvorlig kriminalitet må tåle.[233] Dette er en av måtene lovgiver har balansert behovet for effektiv kriminalitetsbekjempelse, mot retten til privatliv. En alminnelig tolkning av departementets uttalelse, tilsier at det gjøres en avveining av inngrepet sammenlignet med den straffbare handlingen. Jo mer alvorlig kriminalitet det er snakk om, jo mer akseptabelt kan det være å benytte dataavlesing. Dette er noe av vurderingstemaet i EncroChat-saken.

4.4 Kravet til individualisering av mistankekravet og EncroChat-dommen

4.4.1 Krav til individualisering av mistanke

Det følger av juridisk litteratur at "skjellig grunn til mistanke *mot en bestemt person* er alltid et vilkår for bruk av tvangsmidlene kroppsundersøkelse, DNA-innhenting, kommunikasjonskontroll, dataavlesing, romavlytting, skjult kameraovervåking på privat sted og teknisk sporing" (mine kursiveringer).[234] Det følger av uttalelsen at mistankekravet må individualiseres før det er oppfylt, og at det ikke kan rettes skjellig grunn til mistanke mot en uidentifisert gruppe, eller ukjent omfang – antageligvis for å unngå masseovervåking på et uforholdsmessig nivå, og utenfor formålet. Øyen skriver at "[f]ormuleringen "skjellig grunn" til mistanke tolkes slik at det må være sannsynlighetsovervekt for at en bestemt person, eventuelt en ukjent gjerningsperson, er skyldig i det straffbare forholdet mistanken gjelder".[235]

Det følger som tidligere nevnt av strpl. § 216 o fjerde ledd at dataavlesing bare kan gis for "bestemte datasystemer eller brukerkontoer til nettverksbaserte kommunikasjons- og

[232] Jf. punkt **Error! Reference source not found.**.
[233] Prop. 68 L (2015-2016) side 265.
[234] Øyen (2020) side 200. Med henvisning til de aktuelle bestemmelsene i straffeprosessloven.
[235] Side 200. Med henvisning til Rt. 1993 side 1302, Rt. 2004 side 887 avsnitt 12, Rt. 2005 side 194 og Rt. 2006 side 582 avsnitt 19.

lagringstjenester som den mistenkte besitter eller kan antas å ville bruke".[236] Med "bestemte" datasystemer eller brukerkontoer er det naturlig å tolke ordlyden dit hen at avlesingen må rette seg mot en nærmere spesifisert enhet eller identitet.

Det følger av forarbeidene at "bestemte" datasystemer eller brukerkontoer innebærer at den som avleses må kunne identifiseres i politiets begjæring og rettens kjennelse (alternativt påtalemyndighetens beslutning, dersom hastekompetanse benyttes).[237] Kjernen i begrepet knytter seg til at det skal være så liten tvil som mulig rundt hvilke objekter som tillates avlest. Det fremgår videre av forarbeidene at ordlyden er avgrenset mot indirekte bruk, og at det "ikke [er] adgang til å foreta direkte avlesing av eksempel servere hos tjenesteleverandører mv. som mistenkte bare indirekte gjør bruk av. Tilgangen til opplysningene må skaffes gjennom mistenktes datasystem eller brukerkonto".[238]

Til sammenligning kan det gis tillatelse til ransakelse på bakgrunn av opplysninger om forbrytelser eller adresser som er åpne for et uspesifisert antall personer, uten at politiet på forhånd kjenner identiteten til de(n) mistenkte.[239] Straffeprosessloven § 194 første ledd hjemler at politiet ved nærmere angitte vilkår, kan ransake "alle hus eller rom i et nærmere bestemt område" dersom de har berettiget grunn til å "anta" at mistenkte oppholder seg skjult i området eller de kan finne bevis som kan beslaglegges. I et slikt tilfelle vil jo etterforskningen kunne favne ganske vidt, uten at de med sikkerhet vil finne relevante bevis. Dersom naboer eller slikt berøres av inngrepet, vil det også kunne treffe lovlydige borgere.

Utfordringen med å anvende inngrep som ransaking og dataavlesning på en etterforskningsmetode som i EncroChat-saken, er at det på et nettverk med rundt 60 000 brukere neppe kan konkretiseres en mistanke i forhold til bestemte forbrytelser eller mot enkeltpersoner.[240]

---

[236] Jf. punkt 4.2.1 ovenfor.
[237] Prop. 68 L (2015-2016) side 270.
[238] Prop. 68 L (2015-2016) side 271.
[239] Strpl. § 193 og § 194.
[240] Lentz (2023) side 54. "Internationale politiaktioner mod krypterede kommunikationsnetværk - EncroChat-aktionen i et dansk perspektiv."

En slik definisjon som følger av juridisk litteratur og ordlydstolkningen ovenfor, tilsier at data må avleses i en konkret tilknytning til mistenktes enhet, brukerkonto, eller datasystem – og ikke av for eksempel en større plattform som mistenkte benytter i fellesskap med flere, med mindre dataen avleses *gjennom* mistenktes brukerkonto og man da bare leser de meldinger som mistenkte mottar til *sin* konto. I et slikt tilfelle må man da sikre innloggingsdetaljene til mistenkte, eller på annet vis sikre data som mistenkte mottar til sin enhet eller brukerkonto. Dersom en slik forståelse legges til grunn, vil dagens rettstilstand stride med forarbeidenes uttalelser.

4.4.2 EncroChat-dommen – faktum og problemstillinger

Som redegjort ovenfor, tilsier strpl. § 216 o sin ordlyd at det må foreligge en viss konkretisering av hvem mistanken retter seg mot, jf. ordlyden ”bestemte” brukerkontoer eller datasystemer. Høyesteretts uttalelser i HR-2022-1314-A (EncroChat) kan derimot trekke i retning av det motsatte. Dommen tar primært for seg bruk av etterforskningsmateriale innhentet ved utenlandske myndigheters skjulte tvangsmiddelbruk, med en metode som kan sies å stå i motsetning til ordlyden i strpl. § 216 o.

I norsk rett har spørsmålet om bruk av dataavlesing hittil fått begrenset oppmerksomhet. EncroChat-dommen utgjør ett av få tilfeller som berører strpl. § 216 o. Høyesterett tar primært for seg bruk av etterforskningsmateriale innhentet ved utenlandske myndigheters skjulte tvangsmiddelbruk, med en metode som potensielt er urettmessig etter norsk straffeprosesslov.[241] I snever forstand går de ikke nærmere inn på vilkårene for å gjennomføre dataavlesing etter norsk rett. Faktum er derimot noe interessant for vurderingen av vilkårene i dataavlesing, ettersom enkelte momenter i vurderingen om bevisførsel har indirekte betydning for hvordan vilkårene for dataavlesing skal forstås.

Basert på en tolkning av Høyesteretts uttalelser i EncroChat-dommen er det for meg uklart om mistankekravet faktisk må rette seg mot en spesifikk person, eller om det kan gjelde en uidentifisert større plattform, server, eller gruppe. Skal man tolke mistankekravets omfang direkte ut fra bestemmelsens ordlyd, vil det måtte være en viss konkretisering av hvem mistanken retter seg mot, jf. ordlyden "bestemte" brukerkontoer eller datasystemer i strpl. §

[241] Se punkt 1.3.

216 o. Basert på Høyesteretts uttalelser i EncroChat-dommen, vil mistankekravet derimot kunne tolkes mye videre enn ordlyden i strpl. § 216 o gir uttrykk for.

Høyesteretts uttalelser er relevant for vilkårene i dataavlesing nettopp fordi Høyesterett i sammenheng med vurderingen av bevisreglene, legger til grunn et faktum som impliserer at mistankekravet potensielt er oppfylt. Høyesterett sier ingenting konkret om at mistankekravet *var* oppfylt, men i det tilfellet at det ikke er det vil det uansett ikke stride med grunnleggende norske verdier å akseptere Kripos' fremgangsmåte i saken. Dataavlesing som gjennomføres som i EncroChat-aksjonen kan derfor aksepteres etter norske rettsregler, i henhold til domsslutningen.

Selv om Høyesteretts vurdering rent metodisk er mest relevant, har Oslo tingrett og Borgarting lagmannsrett redegjort for faktum på en vesentlig pedagogisk måte. Det er derfor inntatt enkelte utdrag fra deres redegjørelser som Høyesterett ikke nødvendigvis berørte, i den følgende redegjørelsen av faktum.

EncroChat-saken gjaldt spørsmål om data innhentet fra et kryptert kommunikasjonsnettverk av utenlandske etterretningstjenester kan føres som bevis i en norsk straffesak. Saken gjaldt tre personer som var tiltalt for befatning med en meget betydelig mengde narkotika,[242] og to av dem var også tiltalt for aktivitet i en organisert kriminell gruppe.[243]

Saken løfter frem to hovedproblemstillinger. For det første, hvorvidt norsk politi var passive mottakere av data eller aktive deltakere i etterforskningen foretatt av fransk og nederlandsk påtalemyndighet. For det andre, spørsmålet om selve innhentingspunktet for dataene var EncroChat-serveren eller de individuelle brukernes enheter. Det er i realiteten bare det andre spørsmålet som er relevant for reglene om dataavlesing, og fokuset vil derfor rette seg mot spørsmålet om innhentingspunktet for dataene fra EncroChat-etterforskningen.

Kjernen av EncroChat-saken knytter seg til Høyesteretts vurdering av om det vil stride med norske grunnleggende verdier å føre beviset. Vilkåret følger av rettsnormen som ble etablert i Rt. 2002 s. 1744 (Spansk mobilavlytting). Kjennelsen gjaldt telefonavlytting av en norsk

---

[242] Lov 20. mai 2005 nr. 28 om straff (heretter straffeloven el. Strl.) § 232 annet ledd, jf. § 231 første ledd, jf. § 15.
[243] Straffeloven § 79 bokstav c.

statsborger som befant seg i Spania. Avlyttingen var lovlig etter spansk rett, men ville ikke vært tillatt i Norge. Høyesteretts kjæremålsutvalg etablerte i kjennelsen en ulovfestet lære om at etterforskningsmateriale som er lovlig innhentet etter lokale lovverk av utenlandske myndigheter, kan føres som bevis i en norsk straffesak. Dersom avlyttingen ikke hadde vært lovlig etter norske rettsregler, er det tre vilkår for å benytte materiale innhentet av utenlandske etterforskningstjenester: innhentingen må være lovlig etter det aktuelle lands regler, den tiltalte må ha rett til innsyn i alle opplysningene som er innhentet, og innhentingen må ikke være gjennomført på en måte som strider med grunnleggende norske verdier.[244] Riksadvokaten etablerte videre i 2003 at innhentingen heller ikke kan ha en karakter av å være en ren omgåelse av norske rettsregler.[245]

Høyesterett la til grunn i EncroChat-saken at Kripos ikke var aktive deltakere i etterforskningen, og besvarer derfor den første problemstillingen avkreftende. Det har betydning om Kripos var aktive deltakere i etterforskningen eller ikke, fordi det vil kunne oppfattes som at de nettopp forsøkte å omgå norske rettsregler dersom de *ba* franske myndigheter om å bruke en metode som ikke ville vært lovlig etter norsk rett. Høyesterett avkrefter derimot dette, på bakgrunn av at lagmannsretten konkluderte med at det ikke var holdepunkter for at de deltok aktivt.[246]

Det andre spørsmålet i EncroChat-dommen var om dataene var innhentet på EncroChats servere, eller om det ble innhentet på de individuelle brukernes enheter. Spørsmålet har indirekte betydning for mistankekravet som følger av strpl. § 216 o første og fjerde ledd.

Høyesterett legger som tidligere nevnt til grunn et utgangspunkt som strider med lovgivers uttalelser om hvordan mistankekravet i § 216 o skal forstås.[247] Det er dermed ikke Høyesteretts vurdering av vilkårene for bevisføring som kritiseres i det følgende, men den betydningen det har for reglene om dataavlesing at Høyesterett velger å akseptere at mistankekravet ikke var individualisert før etterforskning ble satt i gang. Som det fremgår av rettsnormen fra Rt. 2002 s. 1744 (Spansk avlytting) kan bevis som innhentes ved bruk av en

[244] Jf. HR-2022-1314-A (EncroChat) avsnitt 26 med henvisning til Rt. 2002 s. 1744 på side 1747. Avgjørelsen er videre fulgt opp i Rt. 2005 s. 1524, HR-2021-1336 (AnoM-saken) og HR-2021-1538-U.
[245] Jf. HR-2022-1314-A (EncroChat) avsnitt 27, med henvisning til Riksadvokatens brev 20. januar 2003.
[246] Jf. HR-2022-1314-A avsnitt 45.
[247] HR-2022-1314-A avsnitt 6.

metode som ikke ville vært lovlig etter norsk rett, likevel aksepteres så lenge det ikke strider med grunnleggende norske verdier å føre beviset.

Som tidligere nevnt er det et vilkår for bruk av blant annet dataavlesing at mistanken rettes mot en bestemt person.[248] Det kan ifølge juridisk litteratur ikke rettes mistanke mot en uidentifisert gruppe, eller et ukjent omfang.[249]

Spørsmålet er derfor om EncroChat-dommen har endret kravet til individualisering.

For å forstå EncroChat-dommen er det nødvendig å se til hva EncroChat-plattformen faktisk er. Lagmannsretten beskriver EncroChat slik:

> "EncroChat er navnet på én av flere tilbydere av krypterte kommunikasjonsløsninger via bruk av krypterte mobiltelefoner. Telefonene leveres med et eget operativsystem, som kun tillater bruk av bestemte kommunikasjonsapplikasjoner. Telefonene fungerer i praksis kun i kontakt med andre krypterte telefoner av samme type og tilbyr kommunikasjon med høy sikkerhet. EncroChat-telefonene leveres med forhåndsbetalte, internasjonale sim-kort. Telefonene kan heller ikke kjøpes i butikk, men utelukkende gjennom EncroChats nettsider eller på tredjepartssider som eBay.
>
> All kommunikasjon mellom slike telefoner er kryptert datatrafikk, og kan derfor ikke avlyttes i transportfasen. Tjenesten har også en mulighet for «panikksletting», «fjernsletting» og automatisk sletting av meldinger etter en gitt tid. Disse funksjonalitetene gjør telefonene egnet for kriminell kommunikasjon". [250]

Nederlandsk politi hadde innledet etterforskning av EncroChat i 2018, og senere etablert et felles internasjonalt etterforskningsteam – Joint Investigation Team (JIT) med fransk politi. I dette samarbeidet kopierte politiet EncroChats servere, og fikk slik tilgang til datainformasjon og logger på tjenesten. Med bistand fra Eurojust og Europol, ble det i begynnelsen av 2020

[248] Se punkt 4.4.1, med henvisning til Øyen. (2020) Side 200.
[249] Se punkt 4.4.1. Det må understrekes at Øyens bok er skrevet før EncroChat-saken fant sted. Det kan virke som at rettstilstanden på den tiden (2020) var en annen.
[250] LB-2021-168568 side 4 – sakens spørsmål og bakgrunn.

utviklet en teknisk løsning for å dekryptere og avlese datatrafikken fra EncroChat. Slik muliggjorde politiet dataavlesning i sanntid.

Serveren ble knyttet til byen Roubaix i Frankrike, og Lille tingrett – den stedlige tingretten i Roubaix, ga tillatelse til dataavlesning av EncroChat-serveren. Dataavlesingen avdekket at det blant annet var norske brukere på nettverket. I etterkant av dette, mottok Kripos sanntidsdata fra fransk politi om norske brukeres data fra og med 2. april 2020. På grunnlag av dette materialet, sammenholdt med spaningsinformasjon, ble flere brukere identifisert og mistankegrunnlaget for dataavlesing ble deretter individualisert. Kripos fikk deretter Oslo tingretts tillatelse til kommunikasjonsavlytting av blant annet A, B og C i den aktuelle saken.

Da Kripos ble tilbudt å motta datamateriale fra den utenlandske etterforskningen, aksepterte de vilkårene og mottak av dette samme dag.[251] Høyesterett uttaler også at datainnhentingen fant sted på EncroChats server, ikke de individuelle mobiltelefonene. Det følger derimot av en relatert britisk avgjørelse at det *var* de enkelte telefonene i de ulike jurisdiksjonene som ble avlest, på bakgrunn av det faktum som ble presentert for Liverpool Crown Court.[252] Lagmannsretten nevner at den britiske domstolen konkluderte med at kommunikasjonen ble hentet "direkte fra telefonene, og ikke fra serveren". I etterkant av denne dommen foretok også Kripos nye undersøkelser av om avlesingen skjedde på franske servere, eller på telefonene i Norge, uten å kunne konkludere.[253]

Lagmannsretten konkluderer med at dataavlesing som i EncroChat-saken, ikke ville vært lovlig etter norsk rett på bakgrunn av mistankekravet. Førstvoterende uttaler på side 12:

> "Lagmannsretten finner det ut fra dette klart at den som besitter eller antas å bruke datasystemet eller brukerkontoen som skal avleses, må identifiseres i begjæringen og rettens kjennelse, og at kravet om skjellig grunn til mistanke må være oppfylt for vedkommende. Med andre ord ville man etter norsk rett ikke kunne få tillatelse i

[251] HR-2022-1314-A Avsnitt 45.
[252] LB-2021-164345 – LB-2021-164360 – LB-2021-168568 side 11.
[253] LB-2021-164345 – LB-2021-164360 – LB-2021-168568 side 12.

> medhold av straffeprosessloven § 216 o til avlesing (...) uten at grunnvilkåret om skjellig grunn til mistanke hadde vært oppfylt for den enkelte brukeren".[254]

Høyesterett uttaler derimot at det er "personar og selskap knytte til EncroChat og den identifiserte sørvaren i Roubaix som tenestetilbydar – og ikkje brukarane av tenesta" som primært avleses.[255] Ved å legge til grunn at EncroChat-serveren var det sentrale målet for dataavlesing, og ikke brukerne av tjenesten, går Høyesterett bort fra lovgivers uttalelser om hvordan mistankekravet skal forstås.[256]

Høyesterett legger som nevnt til grunn at det ikke var de individuelle telefonene som ble avlest, til tross for at dette medfører at mistankekravet i § 216 o ikke var oppfylt. Førstvoterende går rett til unntaket som følger av Rt. 2002 s. 1744, om at bevis likevel kan føres under visse forutsetninger.[257] Det sentrale vurderingstemaet i førstvoterendes drøftelse er om føringen av beviset vil stride med "grunnleggende norske verdier".

Førstvoterende kommer til at en plattform som EncroChat ikke har krav på vern, ettersom det er en plattform som "i all hovedsak benyttes av kriminelle til bruk for kriminell kommunikasjon".[258] EncroChat er i utgangspunktet en krypteringsplattform som er utviklet av sivile, for å sikre konfidensiell kommunikasjon. Slike plattformer er en viktig forutsetning for ytringsfrihet og retten til privatliv.[259] Statene har i utgangspunktet også en plikt til å respektere og sikre slik ytringsfrihet, og i retten til privatliv ligger også et ansvar for å beskytte kryptert kommunikasjon.[260] Igjen må det gjøres en balansering av hensynet til individet, mot hensynet til effektiv kriminalitetsbekjempelse.

---

[254] LB-2021-164345 – LB-2021-164360 – LB-2021-168568 side 12.
[255] Jf. HR-2022-1314-A avsnitt 6.
[256] Se punkt 4.4.2 med henvisning til Prop. 68 L (2015-2016) side 270.
[257] Se ovenfor; Innhentingen må være lovlig etter det aktuelle lands regler, den tiltalte må ha rett til innsyn i alle opplysningene som er innhentet, og innhentingen må ikke være gjennomført på en måte som strider med grunnleggende norske verdier. Innhentingen kan heller ikke kan ha en karakter av å være en omgåelse av norske rettsregler.
[258] HR-2022-1314-A Avsnitt 42.
[259] EU-rådets resolusjon om kryptering 24. november 2020 13084/1/20.
[260] EU-rådets resolusjon om kryptering 24. november 2020 13084/1/20.

Høyesteretts uttalelse om at EncroChat ikke er en type plattform som har krav på vern, er en videreføring av førstvoterendes uttalelser i AnoM-saken.[261] Flertallet uttalte at brukere av en slik plattform som i AnoM-saken "i det minste må være klar over at politiet vil gå ut fra at krypteringstjenesten i stor utstrekning brukes av kriminelle nettverk, og at brukerne dermed lett kan bli gjenstand for overvåkning og etterforskning".[262]

Saken gjaldt bruk av materiale som var innhentet av en kryptert kommunikasjonsplattform som var etablert og styrt av amerikansk politi. Plattformen var utviklet særlig med tanke på kriminelle, spredt blant kriminelle, og ble gjennomgående benyttet av kriminelle. Det måtte brukes spesialtilpassede telefoner, og brukere måtte inviteres inn av andre brukere.[263] Siktede i saken befant seg i Norge når overvåkningen skjedde. Saken har slik overføringsverdi for EncroChat-dommen på bakgrunn av dens liknende faktum. Saken hadde en dissens på to mot én.

Mindretallet mente derimot at det skulle "mer til for å akseptere som bevis opplysninger som stammer fra en overvåkning som er foretatt av et annet lands myndigheter og er rettet mot en person med opphold i Norge enn om personen oppholdt seg i det landet som utførte overvåkningen", noe flertallet ikke hadde tatt stilling til.[264]

Tradisjonelt i norsk straffeprosess må det som nevnt være en viss konkretisering av mistanken og den straffbare handlingen før skjulte tvangsmidler kan benyttes, noe som gjenspeiles i de ovennevnte kravene til alvorligheten av kriminaliteten, styrken av mistanken og formålet med inngrepet. Disse kravene sikrer samlet sett at inngrep begrenses til det nødvendige i forhold til den forbrytelsen som etterforskes.

Det kan tenkes at det franske politiet anvendte tidligere straffesaker med opplysninger om at EncroChat var benyttet, for å kunne oppgi et estimat for hvor mange franske EncroChat-brukere man kunne anslå. Fransk politi ville i så fall ha kunne vist til saker der EncroChat allerede med sikkerhet ble benyttet til kommunikasjon mellom kriminelle, og ikke minst var

[261] HR-2021-1336-U avsnitt 21.
[262] HR-2021-1336-U avsnitt 21.
[263] HR-2021-1336-U avsnitt 19.
[264] HR-2021-1336-U avsnitt 31.

det kanskje en faktor at EncroChats egenskaper appellerte til kriminelle. Dette er derimot bare antagelser, og ikke uttalt med sikkerhet.

Dersom dette skulle blitt gitt overføringsverdi til norsk politi i en fremtidig liknende etterforskningsaksjon, vil utfordringen knytte seg til at norske domstoler må ta utgangspunkt i at brukerne av nettverket er kriminelle. Mistankekravet står derimot i veien for dette, ettersom det må være "skjellig grunn til mistanke", altså sannsynlighetsovervekt. Skulle dette kravet likevel oppfylles, kan det under ingen omstendigheter gjennomføres etterforskning som har en karakter av å være masseovervåkning. I EncroChat-saken var det snakk om omtrent 60 000 brukere, og norsk rett åpner som sagt ikke for slik masseroverv̊åkning av borgere.

For anførselen om at dataavlesingen fremstår som masseovervåkning, slutter førstvoterende seg til en tysk dom i relasjon til EncroChat-aksjonen.[265] Den tyske dommen konkluderte med at EncroChat-aksjonen ikke var masseovervåking, fordi fransk politi hadde innledet etterforskning under mistanke om at EncroChat-brukere naturlig ville komme i kontakt med kriminelle aktiviteter innen organisert kriminalitet, på grunn av de betydelige kostnadene forbundet med kjøp og bruk av en EncroChat-telefon som ikke var tilgjengelig via vanlige salgskanaler.[266]

4.4.3 Rettstilstanden etter EncroChat

Som nevnt ovenfor skal dataavlesing rettes mot "bestemte" datasystemer eller brukerkontoer.[267] Ifølge forarbeidene må man kunne identifisere den som avleses, og det skal være så liten tvil som mulig rundt hvilke objekter som tillates avlest.[268] Mer sentralt er det som sagt, at lovgiver uttaler at det ikke er adgang til å foreta direkte avlesing av "eksempel servere hos tjenesteleverandører mv. som mistenkte bare indirekte gjør bruk av. Tilgangen til opplysningene *må skaffes gjennom mistenktes datasystem eller brukerkonto"* (mine kursiveringer).[269]

---

[265] HR-2022-1314-A avsnitt 41.
[266] Jf. Vedtak fra den tyske høyesterett for sivile saker og straffesaker – Bundesgerichtshof – 2. mars 2022, sak 5 StR 257/21 avsnitt 37.
[267] Jf. strpl. § 216 o fjerde ledd, se også punkt 4.1.1.1, og side 41 og 42.
[268] Jf. Prop. 68 L (2015-2016) side 270.
[269] Prop. 68 L (2015-2016) side 271.

EncroChat-dommen er i korte trekk problematisk fordi det virker som at Høyesterett går bort fra lovgivers uttalelser om vilkårene for dataavlesing, og gjør en "utvidelse" av hvordan mistankekravet skal forstås. Selv om førstvoterende ikke tar stilling til de konkrete hjemlene i strpl. § 216 o, har saken som nevnt en indirekte betydning for hvordan man skal forstå vilkårene i hjemmelen for dataavlesing.

Jeg nevnte tidligere at mistankekravet må individualiseres, slik at det kan rettes mot "bestemte" datasystemer eller brukerkontoer. Strpl. § 216 o fjerde ledd kan derimot ikke lenger tolkes slik som forarbeidene, juridisk litteratur, eller naturlig ordlydstolkning tilsier, basert på Høyesteretts uttalelser i EncroChat-dommen. Etter EncroChat, kan mistankekravet tolkes slik at dersom det er skjellig grunn til mistanke om at en *tjeneste* i hovedsak benyttes til alvorlig kriminalitet, men det ikke er konkret mistanke mot identifiserte personer, kan mistankekravet etter EncroChat-dommen likevel anses oppfylt.

EncroChat-dommen stiller derfor lovforarbeidet til stprl. § 216 o i et usikkert lys. Hvor lovgiver uttaler at det "ikke er adgang til å foreta direkte avlesing av [...] servere hos tjenesteleverandører", vil det nå kunne åpnes for nettopp det. EncroChat-dommen åpner for at det *ikke* må foreligge en konkret mistanke rettet mot en individuell bruker, noe som vanskelig kan forenes med utgangspunktet om at det skal være minst mulig tvil rundt hvilke objekter som tillates avlest, slik lovgiver opprinnelig hadde tenkt.[270]

Som tidligere nevnt, har ikke stater en ubegrenset adgang til å gjøre inngrep overfor individer av hensyn til effektiv kriminalitetsbekjempelse, dersom dette kan undergrave demokratiske verdier.[271] En av disse verdiene er nettopp retten til privatliv, jf. EMK art. 8 nr. 1. Vilkårene for å gjennomføre dataavlesing etter strpl. § 216 o er utviklet med særlig fokus på at tvangsmiddelet anses å være et "vesentlig personverninngrep".[272] Lovgiver forsøkte å avbalansere krenkelsen dette inngrepet utgjør, nettopp ved å innføre strenge prosessuelle garantier, slik også EMD har understreket viktigheten av.[273] Høyesteretts indirekte "utvidelse"

[270] Prop. 68 L (2015-2016) side 270.
[271] Se punkt 2.3.7, med henvisning til *Klass and Others v. Germany* avsnitt 49.
[272] Jf. prop. 68 L (2015-2016) side 265.
[273] Se *Roman Zakharov v. Russia* avsnitt 229 og *Adomaitis v. Lithuania* avsnitt 83 siste setning.

av hvordan mistankekravet kan tolkes i forbindelse med bruk av dataavlesing, er derfor vanskelig å stille seg bak.

Ettersom dataavlesing i alle tilfeller utgjør et inngrep i retten til privatliv, jf. EMK artikkel 8 nr. 2, bør statene utvise forsiktighet med å flytte på grensene for hva som tillates ved gjennomføringen og tolkningen av hvordan de nasjonale inngrepshjemlene skal forstås.[274] Som jeg redegjorde for under punkt 2.4.3 har EMD ved gjentatte tilfeller understreket viktigheten av klare og detaljerte regler for kommunikasjonsavlytting – som gis overføringsverdi til dataavlesing.[275]

Uavhengig av om Kripos var aktive deltakere i etterforskningen av EncroChat eller ikke, og om de bevisst ønsket å omgå norske rettsreglers begrensninger, har de i ethvert tilfelle bygget en straffesak på materiale som er innhentet ved bruk av etterforskning som bærer likhetstrekk til masseovervåkning. Tillatelse til dataavlesing uten en tilstrekkelig individualisert mistanke kan i verste fall resultere i en form for masseovervåkning, hvor tusenvis av brukere blir overvåket uten konkrete bevis for at de begår eller forsøker å begå kriminelle handlinger. Dette kan svekke rettssikkerhetsfølelsen til enkeltpersoner, og undergrave tilliten til myndighetens evne til å beskytte individenes rettigheter. Ikke minst kommer det ikke klart frem av strpl. § 216 o at politiet har adgang til å utøve slik makt.

Det er, etter min mening, problematisk at førstvoterende uttaler at slike plattformer som EncroChat "ikke har krav på vern", fordi den hovedsakelig ble benyttet av kriminelle. EncroChat-aksjonen har i alle tilfeller bekreftet et slikt utsagn, men nettverket har utvilsomt hatt lovlydige brukere som kanskje bare ønsket økt personvern, beskyttelse mot datainnsamling, eller som naturlig kommuniserer med sensitiv informasjon. Krypterte kommunikasjonsplattformer kan like gjerne fremstå som særlig attraktive for brukere som advokater, universiteter, og journalister, som de kan for kriminelle. Eksempelvis er krypterte kommunikasjonsplattformer potensielt attraktive for personer som faller innenfor ordlyden i

[274] Her strpl. § 216 o.
[275] Jf. *Adomaitis v. Lithuania* avsnitt 83 og *Roman Zhakarov v. Russia* avsnitt 229.

strpl. § 216 c annet ledd, og derfor har krav på at det foreligger "særlige grunner" før deres kommunikasjon avleses.[276]

Høyesterett ser ut til å utvikle en norm som tilsier at tjenester som "hovedsakelig benyttes til kriminell kommunikasjon" ikke er beskyttelsesverdige, og at dersom brukere velger å ta i bruk slike tjenester, må de være innstilt på å overvåkes eller etterforskes.[277] Den alminnelige forbruker vil neppe ha noen større formening om hvilken type kommunikasjon en plattform "hovedsakelig" benyttes til. Dersom det er krypteringsløsningen som gjør at en plattform fremstår som mer attraktiv for kriminelle, vil som nevnt kommunikasjonsplattformer som WhatsApp, Facebook Messenger, og Snapchat like gjerne ha potensiale for å benyttes av kriminelle.

Dersom det er selve kostnaden for å skaffe seg tilgang til slike tjenester, slik som den tyske domstolen fremhever, kommer ikke dette klart frem av Høyesteretts uttalelser eller tidligere rettspraksis. Dersom man tar utgangspunkt i Oslo tingretts kjennelse i forbindelse med EncroChat, kan det virke som at det er mulighetene for fjernsletting og automatisk sletting etter en gitt tid, i sammenheng med en høy eksklusivitet for telefonene, den høye kostnaden for telefonen, og den begrensede tilgangen til informasjon om bruk og brukere som gjør at EncroChat fremstår så attraktivt for kriminelle.[278] Dette vil i så fall være momenter som alle forbrukerne er klar over, ettersom de må gjennomgå den samme prosessen for å anskaffe en EncroChat-mobiltelefon.

Individer har ikke krav på å vite at de blir utsatt for dataavlesing, da det åpenbart vil undergrave hele inngrepets tiltenkte effekt.[279] De har derimot krav på å kunne forutse sin rettsstilling, og under hvilke forhold myndighetene har anledning til å gjøre inngrep i den rettsstillingen.[280] En rettsutvikling som medfører at mistankekravet "utvides" til også å gjelde

---

[276] Se punkt 4.2.1: "advokat, lege, prest eller andre som erfaringsmessig fører samtaler av svært fortrolig art over telefon eller redaktør eller journalist".
[277] Jf. HR-2022-1314-A avsnitt 42, jf. HR-2021-1336-U (AnoM-saken) avsnitt 21.
[278] Se TOSL-2021-30329-1 side 11.
[279] Se punkt **Error! Reference source not found.** ovenfor, med henvisning til *Adomaitis v. Lithuania* avsnitt 83 og *Drakšas v. Lithuania* avsnitt 67.
[280] Se punkt **Error! Reference source not found.** ovenfor, med henvisning til *Roman Zakharov v. Russia* avsnitt 229.

en tjenestetilbyders server i sin helhet, og ikke bare individets bestemte datasystem eller brukerkonto, er vanskelig å forene med EMDs uttalelser om tilstrekkelig klar lovhjemmel.

Inngrep overfor den enkelte skal også blant annet være proporsjonale for det formålet som søkes oppnådd.[281] I EncroChat-saken er formålet riktig nok kriminalitetsbekjempelse, men det åpner ikke uten videre for å tillate overvåkning av om lag 60 000 brukerkontoer. På den andre siden kan det være vanskelig å se for seg hvordan Kripos ellers kunne ha avdekket nettopp *hvem* som sto bak brukerkontoene for de kriminelle handlingene som A, B, og C ble tiltalt for i EncroChat-dommen.

Overvåking som pågår over lang tid og/eller i stort omfang, vil naturlig ramme et større omfang personer, slik som i EncroChat-saken. Det medfører typisk en innhenting av større mengder informasjon som ikke er relevant for etterforskningen. Dette vil komme i kontrast med nødvendighetskravet, ettersom dataavlesing som tidligere nevnt skal begrenses til det som er nødvendig for å oppnå formålet med inngrepet. [282]

Det må videre tas i betraktning at selv om enkeltstående opplysninger ikke alltid er særlig inngripende, vil slike opplysninger samlet sett kunne gi et detaljert og intimt bilde av brukerens bevegelsesmønstre, preferanser og holdninger – og dermed utgjøre et ganske fullstendig bilde av et individ.

4.4.4 Oppsummering

En analyse av EncroChat-dommen åpner for å kritisere flere sider av (den manglende) tolkningen av minstekravet i strpl. § 216 o i lys av Høyesteretts uttalelser. Selv om Høyesteretts uttalelser kun indirekte retter seg mot vilkårene for dataavlesing, har de en direkte betydning for hva bestemmelsen åpner for. Høyesteretts vurdering skal i utgangspunktet fokusere på sakens konkrete spørsmål. Imidlertid har de også en viktig rettsavklarende funksjon, som ofte går utover sakens spørsmål i snever forstand.

Høyesteretts slutning vil lett kunne skape usikkerhet rundt hvordan vilkårene i strpl. § 216 o skal forstås. En praksis som åpner for en mer generell adgang til avlesing vil stride med

[281] Se punkt 2.3.7 ovenfor.
[282] Jf. ordlyden "nødvendig" i EMK art. 8 nr. 2.

tidligere rettspraksis, juridisk litteratur, og EMDs uttalelser slik de var før EncroChat-dommen. Som det fremgår av den tidligere redegjørelsen av mistankekravet, er det essensielt å skape minst mulig usikkerhet om hvilket objekt som avleses.[283]

Det fremstår nå etter avgjørelsen som at sentrale rettigheter som retten til privatliv og hensynet til personvern vil måtte trå til side til fordel for en reell, effektiv kriminalitetsbekjempelse. Kriminalitet hvor den kriminelle nettopp drar nytte av anonymisering eller en skjult identitet, vil i sin natur vanskeliggjøre en individualisering av mistankekravet. Høyesterett åpner gjennom sin avgjørelse for en mindre konkretisert tilnærming til etterforskning og tilgang til data når det gjelder tjenester som "hovedsakelig benyttes for kriminell kommunikasjon".

En slik slutning tydeliggjør nettopp det spenningsfeltet som foreligger mellom behovet for effektiv kriminalitetsbekjempelse og behovet for på sikre grunnleggende rettsverdier og individuell frihet. Enhver videre anvendelse av dataavlesing som tar utgangspunkt i EncroChat, bør balansere disse hensynene nøye.

4.5 De prosessuelle vilkår for dataavlesing

4.5.1 Introduksjon

Strpl. § 216 p oppstiller de prosessuelle og personelle kravene til bruk av dataavlesing. Bestemmelsen knytter seg til selve gjennomføringen av dataavlesing etter § 216 o, og lyder slik:

> "Dataavlesing etter § 216 o kan bare utføres av personell som er særlig skikket til det og utpekes av politimesteren, sjef PST eller den som bemyndiges. Avlesing kan foretas ved hjelp av tekniske innretninger, dataprogram eller på annen måte. § 199 a gjelder tilsvarende. Politiet kan bryte eller omgå beskyttelse i datasystemet dersom det er nødvendig for å kunne gjennomføre avlesingen. Tekniske innretninger og kan installeres i datasystemet og i annen maskinvare som kan knyttes til datasystemet. Når retten ikke bestemmer noe annet, kan politiet også foreta innbrudd for å plassere eller

[283] Se punkt 4.4.1.

fjerne tekniske innretninger eller dataprogram som er nødvendig for å gjennomføre dataavlesingen.

Dataavlesingen skal innrettes slik at det ikke unødig fanges opp opplysninger om andre enn mistenktes bruk av datasystemet. Avlesingen skal utføres slik at det ikke unødig voldes fare for driftshindring eller for skade på utrustning eller data. Politiet skal så vidt mulig avverge fare for at noen som følge av gjennomføringen settes i stand til å skaffe seg uberettiget tilgang til datasystemet eller vernet informasjon eller til å begå andre straffbare handlinger".

Bestemmelsen sier noe om hvordan dataavlesing etter § 216 o kan gjennomføres. Det følger av første ledd *hvem* som kan gjennomføre avlesingen (personelle krav), og hvilke virkemidler som kan tas i bruk (prosessuelle krav). Annet ledd er ment å begrense graden av inngrep, og supplerer forholdsmessighetskravet i strpl. § 170 a.

Strpl. § 216 p annet ledd oppstiller en rekke rettsikkerhetsgarantier som er ment å verne om retten til privatliv etter Grl. § 102 og EMK artikkel 8. For øvrig gjelder bestemmelsene i §§ 216 d til 216 k.

Det fremgår av ordlyden at dataavlesing bare kan utføres av personell som er "særlig skikket til det". Ordlyden krever som tidligere nevnt tilsynelatende personell som har særskilt høy informasjonsteknologisk kompetanse.[284]

Det følger av første ledd annet punktum at gjennomføring av dataavlesing kan gjøres ved hjelp av "tekniske innretninger, dataprogram, eller på annen måte". Politiet får forholdsvis stor frihet til å velge hvilken praktisk fremgangsmåte som skal benyttes i det enkelte tilfellet. Blant annet gis de anledning til å foreta innbrudd for å plassere avlesingsverktøy, og annen ransaking av stedet der datasystemet er plassert krever egen beslutning.

Lovgivers vage beskrivelse av den konkrete fremgangsmåten var et bevisst valg, av hensyn til at "det ikke er hensiktsmessig eller mulig" å beskrive gjennomføringsmåtene i detalj.[285] Departementet begrunner dette med at de tekniske mulighetene er mange, og den

[284] Se punkt 2.3.7, og Prop. 68 L (2015-2016) side 272.
[285] Prop. 68 L (2015-2016) side 264.

teknologiske utviklingen er uforutsigbar og rask, og vil derfor ikke være hensiktsmessig å inkludere i lovteksten. Dataavlesing begrenses derimot av at det er "informasjon som genereres i og av datasystemet, og mistenktes bruk av datasystemet, som skal kunne kontrolleres gjennom dataavlesing".[286]

I forarbeidene understrekes det at retten ikke bør gi tillatelse til fysisk innbrudd dersom politiet vil kunne gjennomføre avlesingen ved hjelp av andre fremgangsmåter.[287] Uttalelsen er også en supplering til forholdsmessighetskravet, og forstås som et utslag av minste inngrepsprinsipp.[288]

4.5.2 Hastekompetanse

Dersom det ved opphold er stor fare for at etterforskningen vil lide, kan påtalemyndigheten gis såkalt "hastekompetanse" til å beslutte bruk av dataavlesing, uten kjennelse fra retten, jf. strpl § 216 d. Terskelen for å tillate hastekompetanse er høy, og det må foreligge stor fare for at etterforskningen vil lide.[289] Adgangen for å tillate slik kompetanse likestilles her med at den samme regelen gjelder for kommunikasjonsavlytting og hemmelig ransaking.[290]

Kravet om at det må foreligge "stor fare for at etterforskningen vil lide" tolkes som at det vil være betydelig risiko for at etterforskningen vil bli negativt påvirket eller hindret dersom beslutning om å benytte dataavlesing ikke treffes. I slike saker bør påtalemyndigheten etter lovgivers syn kunne tre i stedet for rettens kjennelse, parallelt med reglene for kommunikasjonsavlytting og hemmelig ransaking.[291]

Ved innføring av bestemmelsen understreket Justisdepartementet at hjemmelen for hastekompetanse kun bør anvendes under særlige omstendigheter.[292] Det er ikke tilstrekkelig at det er mer praktisk for påtalemyndigheten å starte inngrepet før retten har avgitt sin kjennelse. Påtalemyndigheten må ha grunn til å tro at avlyttingen vil avdekke viktige

[286] Prop. 68 L (2015-2016) side 264.
[287] Se Prop. 68 L (2015-2016) side 271 og 285.
[288] Se punkt 4.2.5.
[289] Prop. 68 L (2015-2016) side 272
[290] Jf. henholdsvis strpl. § 216 d og § 200 a sjette ledd, jf. Prop. 68 L (2015-2016) side 272
[291] Prop. 68 L (2015-2016) side 272.
[292] Se Ot.prp.nr. 40 (1991-1992) side 41.

opplysninger før det er mulig å bringe saken inn for retten.[293] Antakeligvis bør det foreligge sannsynlighetsovervekt både for at det er stor fare, og at dette er viktig for etterforskningen.

En slik høyere terskel for å treffe beslutning om bruk av skjulte tvangsmidler er som tidligere nevnt en av måtene lovgiver kan avbalansere andre prosessuelle svakheter – eksempelvis en manglende forutsigbarhet om ens egne rettsstilling, eller manglende muligheter for kontradiksjon.[294]

Hastekompetanse vil som hovedregel tilfalle politimesteren eller visepolitimesteren i det aktuelle politidistriktet, og vil i hovedsak kun gjelde for 24 timer (foruten helger og helligdager). I slike situasjoner vil det kreves at påtalemyndigheten utøver et skjønn som bygger på rettssikkerhet og personvern.[295] Bakgrunn for beslutning om hastekompetanse må også fremkomme av informasjonen som sendes til domstolen i ettertid, jf. § 216 d første ledd fjerde punktum.[296]

4.5.3 Stedlig kompetanse

Begjæring om bruk av dataavlesing vurderes av en tingrett på det sted hvor det mest praktisk kan skje, jf. strpl. § 216 e første ledd. Avgjørelsen treffes uten at mistenkte eller den som avgjørelsen ellers rammer, gis adgang til å uttale seg og kjennelsen meddeles ikke dem, jf. § 216 e annet ledd. Ettersom mistenkte ikke gis kontradiksjonsmulighet, er det opp til påtalemyndigheten å avgjøre hvor det er mest praktisk at en sak skal behandles.

4.5.4 Rettigheter for den dataavlesing rettes mot

Normalt vil mistenkte gis status som siktet dersom det besluttes bruk av tvangsmidler.[297] Etter strpl. § 82 tredje ledd fremkommer det at personen likevel ikke vil få stilling som "siktet", dersom det gjelder tvangsmidler som det ikke skal gis underretning om (skjulte tvangsmidler). I slike saker, har mistenkt ikke krav på å varsles om rettsmøter, jf. § 86, eller rett til å være til

[293] Se Ot.prp.nr. 40 (1991-1992) side 41.
[294] Se nærmere om dette under punkt 2.3.7 og 4.2.5
[295] Ot.prp.nr. 64 (1998-1999) side 63
[296] Se også Kommunikasjonskontrollforskriften § 1 annet ledd annet punktum.
[297] Strpl. § 82 første ledd

stede under forhandlingene, jf. § 92. Det følger også av unntaket at det ved skjult etterforskning nektes innsyn etter stprl. § 242 a.

Etter dataavlesingen opphører, skal den mistenkte og/eller den som råder over datasystemet underrettes, jf. strpl. § 216 j første ledd. Retten kan likevel ved kjennelse beslutte at underretning utsettes eller unnlates dersom det vil være "vesentlig til skade for etterforskningen i saken" eller "hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig".[298]

4.5.5 Offentlig oppnevnte advokater etter strpl. § 100 a

Dataavlesings utbytte avhenger i stor grad av at mistenkte ikke har kunnskap om at han/hun blir overvåket. Det ligger i sakens natur at etterforskningen må holdes skjult overfor mistenkte. Det stilles til gjengjeld særskilte krav til gjennomføringen av tvangsmiddelet for å sikre kontradiksjonsretten, og ivaretakelsen av mistenktes rettssikkerhet.[299]

Ved forholdsmessighetsvurderingen av slike tiltak vil prosessuelle garantier som kontradiksjon, og i dette tilfellet mangelen på det, være et viktig moment. Nytteverdien av dataavlesing som etterforskningsmetode bidrar til at en prosessuell garanti som kontradiksjon, ikke kan gjennomføres som normalt. Et strengt krav til personell avgjørelseskompetanse[300] vil også bidra til å avbalansere den mangelen tap av retten til kontradiksjon utgjør. Mistenkte vil således ha sikret rettssikkerhet i mye lavere grad dersom både hastekompetanse og unnlatt underrettelse er tilfellet.

Det kontradiktoriske prinsipp ivaretas i så måte (så langt det lar seg gjøre) gjennom strpl. § 100 a. Hensikten er at advokaten skal ivareta mistenktes interesser, men ikke kontakte mistenkte eller deres forsvarer. Hun skal ikke opptre som en forsvarer, men sørge for at faktum belyses allsidig og grundig, og vil være bedre skikket til å vurdere om proporsjonalitetskravet og de øvrige vilkår for bruk av skjulte tvangsmidler er oppfylt. På denne måten har lovgiver forsøkt å balansere mistenktes fratatte mulighet til å kontrollere og

[298] Jf. strpl. § 216 j første ledd annet punktum.
[299] Aall, J. (2013). "Prosessuelle garantier og forholdsmessighet i straffeprosessen." Jussens Venner. Vol. 48 side 230.
[300] Jf. strpl. § 216 p første ledd første punktum.

bestride begjæringen, mot behovet påtalemyndigheten har for å gjennomføre effektiv etterforskning.[301]

Bakgrunnen for § 100 a knytter seg til hensynet til kontradiksjon når retten behandler en begjæring fra påtalemyndigheten om tillatelse til bruk av skjulte tvangsmidler. En forsvarer som oppnevnes etter § 100 a vil kunne komme med innvendinger dersom hun/han mener at vilkårene for å bruke tvangsmidler ikke er oppfylt slik faktum presenteres. Forsvareren skal så langt det er mulig komme i den samme prosessuelle stillingen som om den mistenkte var klar over tvangsmidlet.[302]

Advokaten skal gjøres kjent med begjæringens innhold, grunnlag, og faktiske omstendigheter. Videre har hun rett til å varsles om rettsmøter som behandler begjæringen, og hun har rett til å uttale seg før det treffes en avgjørelse. Advokaten har også rett til å fremlegge dokumenter og annet skriftlig materiale, selv om dette ikke nevnes uttrykkelig i § 100 a.[303]

[301] Ot.prp.nr. 64 (1998-1999) side 84
[302] Ot.prp.nr. 64 (1998-1999) side 145
[303] Ot.prp.nr. 64 (1998-1999) side 145

5 Oppsummering og avsluttende betraktninger

Formålet med avhandlingen var å analysere vilkårene for dataavlesing etter strpl. § 216 o samt drøfte hvordan retten til privatliv blir ivaretatt gjennom vilkårene. Videre ønsket jeg å se på hvordan strpl. § 216 o skal forstås etter EncroChat-saken.

En økning i den vanlige forbrukerens kunnskap og bevissthet rundt eget personvern, og interesse i å beskytte egen informasjon, har ført til at krypteringsløsninger blir stadig mer populære. I "den digitale alderen" som vi nå er i, har hverdagsforbrukeren en større interesse i å beskytte sin informasjon, være det i form av personopplysninger, eller sporing av hva man shopper etter på nett.

Flere har i dag et ønske om at deres informasjon eller vaner beskyttes, og man lærer stadig mer om hvilke steg man kan ta for å unngå å bli sporet på det åpne nettet. Motstykket til dette er som tidligere nevnt at kriminelle i økende grad også vender seg til ytterligere spesialiserte krypteringsløsninger eller sikrede chattetjenester for å unngå overvåkning. Slik har lovgiver blitt tvunget til å modernisere lovverket, slik at man kan fortsette å ha effektive etterforskningsmetoder.

Justisdepartementets forslag om å innføre dataavlesing som et selvstendig tvangsmiddel var begrunnet hovedsakelig med at det var et "stort og udekket behov for effektiv tilgang" til elektronisk lagret og kommunisert informasjon.[304] Avhandlingen begynte med å se på det overordnede forholdet mellom dataavlesing og sammenlignbare tvangsmidler.[305] Det var deretter nødvendig å se til den teknologiske utviklingen, og hvordan dette har underbygget et konkret behov for dataavlesing som selvstendig metode – ikke bare fremgangsmåte.[306]

Lovgiver presenterer en hjemmel som i realiteten gir politiet adgang til å overvåke mistenktes bruk av et datasystem i sanntid, med mulighet for å gi tilgang til all annen data som er lagret

[304] Prop. 68 L (2015-2016) side 12 punkt 1.10. Se også 1.2.4 i avhandlingen.
[305] Se punkt 1.2.1.
[306] Se punkt 1.2.3 og 1.2.4

på systemet. Til dette uttales det at dataavlesing også kan *oppleves* mer inngripende enn tidligere tvangsmidler.[307]

En økning i myndighetenes adgang til å utøve makt, særlig gjennom å utvide statens mulighet for overvåkning av borgere, forsterker risikoen for maktmisbruk. En slik utvikling vil naturligvis også kunne svekke borgernes tillit til offentlige myndigheter, forstyrre maktbalansen mellom staten og borgerne, og potensielt virke ødeleggende for demokratiet.

Dataavlesing presenterer sådan ny fremgangsmåte innen etterforskning, som ikke nødvendigvis gir kvantitativt mer tilgang til informasjon enn eksempel hemmelig ransaking eller kommunikasjonsavlytting. Informasjonen kan være den samme, men dataavlesing gir etterforskere muligheten til å forbigå krypteringer, på samme måte som en nøkkel åpner en dør.

Derimot gir det som nevnt under punkt 4.2, tilgang til informasjon som ligger ekstremt nært mistenktes tankevirksomhet, og det er etter min mening *derfor* det kan oppleves som "mer inngripende". Følelsen av hvor inngripende en slik krenkelse er forhøyes av at mistenkte ikke vet at de blir overvåket. Som tidligere nevnt vil styrken av et personverninngrep bero på mengden informasjon som samles inn.[308] Overvåking som pågår over lang tid og/eller i stort omfang, og som også kan ramme flere personer, medfører en innhenting av større mengder informasjons om ikke er direkte relevant for etterforskningen. Dette kommer i kontrast med hensynet til personvern, nødvendighetskravet som fremgår av EMK artikkel 8 nr. 2, og proporsjonalitetskravet som fremgår av både EMK artikkel 8 og EMDs praksis.

Innføringen av dataavlesing har utfordret balansen mellom individets rett til privatliv og myndighetenes behov for effektiv kriminalitetsbekjempelse. En stadig raskere teknologisk utvikling har også ført til at trusselbildet har endret seg, og kriminalitet nå skjer på stadig flere arenaer enn før, som nå er vanskeligere å spore. Kriminelle individer og nettverk benytter seg av ny teknologi, hvor planlegging, gjennomføring og kommunikasjon blir mer utfordrende å avdekke, og politiet sliter med å kunne følge denne utviklingen.

---

[307] Jf. Prop. 68 L (2015-2016) side 268. Se også punkt 4.2 i avhandlingen.
[308] Se punkt 4.2.

Gjennomføringen av dataavlesing vanskeliggjøres ytterligere av at de sikkerhetsmekanismene politiet må bryte for å få tilgang til datasystemet, er de samme som datasikkerhetsbransjen kontinuerlig jobber med å styrke. Det finnes heller ingen ensformig fremgangsmåte som gir tilgang til alle typer datasystemer, fremgangsmåtene må utvikles og tilpasses for ulike typer enheter, ulike operativsystemer og ulik programvare.

Konklusjonen i EncroChat-saken tydeliggjør vanskeligheten med å balansere samfunnets behov for effektiv kriminalitetsbekjempelse mot individets rett til privatliv. Det er som redegjort for i avhandlingen, essensielt at lovverket og rettskildene forblir dynamiske og tilpasningsdyktige for å kunne holde følge med det teknologiske landskapets utvikling og de grunnleggende rettighetene som står på spill.

Saker som EncroChat representerer mer enn bare en lovteknisk og rettslig utfordring, da slike krypteringsplattformer tilsynelatende har kommet for å bli. Krypteringstjenester som EncroChat har som formål å vanskeliggjøre identifisering av dens brukere og deres informasjon. Dermed vil det naturligvis også bli vanskeligere å oppfylle kravet til individualisering av mistanke.

Hvis EncroChat-dommen er noe å dra erfaring av, kan det virke som at vi beveger oss mot en rettslig utvikling hvor tradisjonelle, sentrale rettigheter som retten til privatliv, blir svært sårbare i møte med hensynet til effektiv kriminalitetsbekjempelse. Dersom EncroChat-dommen blir fulgt opp av Høyesterett, vil det videreføre en hovedvekt på hensynet til effektivitet i tilfeller som berører kommunikasjonsnettverk som hovedsakelig benyttes av kriminelle.

I en slik situasjon hvor materielle vilkår ikke nødvendigvis *kan* sikres, vil det bli et større behov for at man har tilstrekkelige prosessuelle garantier. EMD understreker som nevnt viktigheten av dette ved flere anledninger.[309] Sentralt i vurderingen deres er sjeldent de materielle vilkårene, men hvilke rettssikkerhetsgarantier som oppstilles.[310] Når Høyesterett da

---

[309] Se *Roman Zakharov v. Russia* avsnitt 229, *Adomaitis v. Lithuania* avsnitt 83, og *Drakšas v. Lithuania* avsnitt 67.

[310] Domstolen vil likevel prøve om en hjemmel er for vidt utformet, og som sådan er for vid, og om en forbindelse med en konkret bruk går utenfor det som er "nødvendig i et demokratisk samfunn". Et annet moment er om inngrepet utelukkende rammer person som med rimelig grunn kan mistenkes, og hvilket kriminalitetskrav

i beste fall tilsidesetter ett av de materielle vilkårene for dataavlesing (mistankekravet), uten å gå nærmere inn på hvordan de har avbalansert dette gjennom prosessuelle garantier, vil det kunne sette EMDs uttalelser i et vanskelig lys.

Problemstillingene rundt dataavlesing utfordrer våre grunnleggende prinsipper og rettigheter, som kravet om at lovbestemmelser skal være klare og forutberegnelige. Det er enkelt å føle at sentrale friheter som demokratier bygger på trues, for eksempel ytringsfrihet og rett til privatliv. Det kan argumenteres for at retten til privatliv og personvern tenkes byttet bort til fordel for tiltak som skal føre kontroll med borgerne, og slik forhindre alvorlig kriminalitet nettopp med den hensikt å beskytte dem. På den ene siden kan det argumenteres for at slike tiltak er nødvendige for å beskytte samfunnet. Derimot er det uklart om slike tiltak faktisk vil ha en positiv virkning, og de vil i beste fall true grunnleggende friheter.

Åpenbart er kriminelle nettverk og øvrig organisert kriminalitet et samfunnsproblem, og erfaringsmessig er det ett som bare blir større.[311] Straffbare handlinger vil på generelt grunnlag kunne virke destabiliserende på samfunnet. Dersom borgere opplever at trusselen for kriminalitet blir for stor, vil dette kunne skape en utrygghetsfølelse som igjen vil kunne true samfunnssikkerheten ved at borgere tar beskyttelse i sine egne hender. En slik utrygghetsfølelse vil også kunne svekke borgernes tillit til staten, en tillit som er en forutsetning for vår samfunnsorden og vårt demokrati.

Det er klart at teknologi- og kriminalitetsutviklingen har medført et pressende behov for nye etterforskningsmetoder. I tråd med EMDs uttalelser er det avgjørende at det foreligger tilstrekkelige prosessuelle garantier for å beskytte individet.[312] Teknologisk utvikling er ikke et ukjent fenomen, men det vil bli stadig viktigere å etablere solide rammeverk og klare retningslinjer for å ivareta våre fundamentale rettigheter, slik som personvern og privatliv. For å vise tilbake til EMDs uttalelse i *Klass and Others v. Germany* er det viktig å utvise en

---

bestemmelsen oppstiller. Videre vurderes typisk hvor alvorlig den kriminelle handlingen er. Se *Texeira de Casto v. Portugal.*

[311] Trendrapport, *Cyberkriminalitet 2024.*

[312] Se *Roman Zhakharov v. Russia* avsnitt 229.

viss tilbakeholdenhet når det gjelder maktbruk, ettersom man risikerer "destroying democracy on the grounds of defending it".[313]

[313] Se avsnitt 49.

Referanseliste

Norske lover

Grunnloven	Lov 17. mai 1814 Kongeriket Norges Grunnlov
Straffeprosessloven	Lov 22. mai 1981 om rettergangsmåten i straffesaker
	Lov 17. juni 2004 nr. 87 om rettergangsmåten i straffesaker
Straffeloven	Lov 20. mai 2005 nr. 28 om straff
Politiloven	Lov 4. august 1995 nr. 53 om politiet
Personopplysningsloven	Lov 15. juni 2018 nr. 38 om behandling av personopplysninger
	Lov 14. april 2000 nr. 31 om behandling av personopplysninger.
Domstolloven	Lov 13. august 1914 nr. 5 om domstolene
Politiregisterloven	Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten
Menneskerettsloven	Lov 21. mai 1999 om styrking av menneskerettighetenes stilling i norsk rett

Lov om granskingskommisjonen	Lov 25. mars 1994 nr. 6 om granskingskommisjonen for gransking av påstander om ulovlig overvåking av norske borgere.

Forarbeider

NOU 1997: 15	
NOU 1997: 19	
NOU 2003: 18	
Ot.prp.nr. 40 (2004-2005)	
Ot.prp.nr. 60 (2004-2005)	
NOU 2004: 5	
NOU 2004: 6	*Mellom effektivitet og personvern*
NOU 2007: 2	*Lovtiltak mot kriminalitet*
NOU 2009: 1	*Individ og integritet*
NOU 2009: 15	*Skjult informasjon – åpen kontroll*
Dok. Nr. 16 (2011-2012)	*Menneskerettighetsutvalget: Menneskerettigehter i Grunnloven*

Dok. Nr. 12: 30 (2011-2012)	*Grunnlovsforslag 30 om grunnlovfesting av sivile og politiske menneskerettigheter*
Prop. 147 L (2012-2013)	*Endringer i straffeprosessloven mv. (behandling og beskyttelse av informasjon)*
Prop. 68 L (2015-2016)	*Endringer i straffeprosessloven mv. (skjulte tvangsmidler)*
Prop. 42 L (2023-2024)	*Endringer i straffeloven*
NOU 2016: 24	
Dok. Nr. 15 (1995-1996)	
Innst. 343 L (2015-2016)	

Høyesterettsavgjørelser

Rt. 1994 s. 610	
Rt. 2014 s. 1105	Acta-dommen
Rt. 2015 s. 93	Maria-dommen
Rt. 2015 s. 155	Rwanda
HR-2017-2376-A	Familieinnvandring

HR-2016-2554-P	Holship
Rt. 2002 s. 1774	Spansk mobilavlytting
HR-2022-1314-A	EncroChat-dommen
HR-2017-2376-A	
HR-2022-718-A	
HR-2023-2224-A	
Rt. 2005 s. 1524	
HR-2021-1336-U	AnoM
HR-2021-1538-U	

Lagmannsrettsavgjørelser

LB-2021-164345 – LB-2021-164360 – LB-2021-168568	Borgarting lagmannsrett - EncroChat

Tingsrettsavgjørelser

TOSL-2021-30329-1	Oslo tingrett - EncroChat

Forskrift

Kommunikasjonskontrollforskriften	Forskrift 9. september 2015 nr. 1047 om kommunikasjonskontroll, romavlytting og dataavlesing

Traktater

Verdenserklæringen om menneskerettigheter	Verdenserklæringen om menneskerettigheter 10. desember 1948
Den Europeiske Menneskerettskonvensjonen	Europarådets konvensjon 4. desember 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter
SP-konvensjonen	De Forente Nasjoners internasjonale konvensjon 16. desember 1966 om sivile og politiske rettigheter
Konvensjon om datakriminalitet	Europarådets konvensjon 23. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi.

Direktiver og resolusjoner

Personverndirektivet	Europaparlaments- og rådsdirektiv 24. Oktober 1995 nr. 46 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.
EU-rådets resolusjon om kryptering	EU-rådets resolusjon om kryptering 24. november 2020 13084/1/20.

Internasjonal rettspraksis

Klass and Others v. Germany	No. 5029/71, ECHR 1978
Dudgeon v. The United Kingdom	[P], no. 7525/76, ECHR 1981
Silver v. The United Kingdom	No. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, ECHR 1983
Olsson v. Sweden	[P], no. 10465/83, ECHR 1988
Sunday Times v. The United Kingdom	[P], no. 13166/87, ECHR 1991
Campbell v. The United Kingdom	No. 13590/88, ECHR 1992
Niemietz v. Germany	No. 13710/88, ECHR 1992
Erdem v. Germany	No. 38321/97, ECHR 1997

Halford v. The United Kingdom	No. 20605/92, ECHR 1997
Z v. Finland	No. 22009/93, ECHR 1997
Radaj v. Poland	No. 29537/95, ECHR 2002
Van Kuck V. Germany	No. 35968/97, ECHR 2003
Perry v. The United Kingdom	No. 63737/00, ECHR 2003
Copland v. The United Kingdom	No. 62617/00, ECHR 2007
S. and Marper v. The United Kingdom	[GC], no. 30562/04, 30566/04, ECHR 2008
Galev and Others v. Bulgaria	No. 18324/04, ECHR 2009
Jehova's Witnesses of Moscow and Others v. Russia	No. 302/02, ECHR 2010
Sanoma Uitgevers B.V. v. The Netherlands	[GC], no. 38224/03, ECHR 2010
P.G and J.H v. The United Kingdom	No. 44787/48, ECHR 2011
S.A.S v. France	No. 19606/08, ECHR 2011
Aksu v. Turkey	[GC], no. 4149/04, 41029/04, ECHR 2012

Drakšas v. Lithuania	No. 36662/04, ECHR 2012
Nada v. Switzerland	[GC], no. 10593/08, ECHR 2012
R.E v The United Kingdom	No. 62498/11, ECHR 2015
Roman Zakharov v. Russia	[GC], no. 47143/06, ECHR 2015
Saber v. Norway	No. 459/18, ECHR 2020
Big Brother Watch and Others v. The United Kingdom	[GC], no. 58170/13, 62322/14 og 24960/15, ECHR 2021
Adomaitis v. Lithuania	No. 14833/18, ECHR 2022
Centrum för rättvisa v. Sweden	[GC], no. 35252/08, ECHR 2022

Internasjonale lover

Retsplejeloven	Lov 6. juni 2002 nr. 378

Svenske lovforarbeider

SOU 2017: 89

Prop. 2019/20: 64

Juridisk litteratur

Bruce og Hagland 2018	Bruce, Ingvild og Haugland, Geir Sunde, *Skjulte tvangsmidler,* 2. Utgave, Universitetsforlaget 2018.
Øyen 2020	Øyen, Ørnulf, *Straffeprosess,* 2. Utgave, Fagbokforlaget 2020.
Skoghøy 2023	Skoghøy, Jens Edvin, *Rett og rettsanvendelse,* 1. Utgave, Universitetsforlaget 2018.
Lentz 2023	Wacher Lentz, Lene, "Internationale politiaktioner mod krypterede kommunikationsnetværk – EncroChat-aktionen i et dansk perspektiv" *Juristen* nr 2 2023, s. 52-61.

Aall 2013 — Aall, Jørgen, "Prosessuelle garantier og forholdsmessighet i straffeprosessen." *Jussens Venner* Vol. 48.

Digitale kilder

Statistisk sentralbyrås statistikk for bruk av IKT i husholdningene fra 2023. — https://www.ssb.no/teknologi-og-innovasjon/informasjons-og-kommunikasjonsteknologi-ikt/statistikk/bruk-av-ikt-i-husholdningene besøkt 29.02.2024.