ADVOKATFORENINGEN
THE NORWEGIAN BAR ASSOCIATION

Advokatforeningens årstale 2017:

Det liberale grenseforsvar

Trygghet og privatliv er to umistelige verdier. Hva gjør vi når de står mot hverandre?

1 Innhold

1. INNLEDNING

Vi lever i et av verdens beste land, i historiens kanskje beste tidsalder. Bytt til noe annet sted i verden, noen annen tid i historien, og du vil høyst sannsynlig få det ganske mye dårligere.

Hvorfor har vi det så godt? Jo, delvis fordi vi har nok mat og materiell rikdom, men også fordi vi har skapt etiske og verdimessige rammer rundt livene, kulturen og sivilisasjonen vår – som gjør at vi føler oss trygge, at vi er en del av flere viktige fellesskap – og at vi har kontroll og råderett over eget liv: Vi har et privatliv.

Aldri før har vi hatt så mye trygghet som nå. Risikoen for å dø i en ulykke er nesten halvert de siste førti årene.

Vi har fått stadig mer trygghet, og vi har også fått stadig mer privatliv.

Det antas at mennesket har et instinktivt behov for privatliv, at vi har en naturlig sjenanse og et naturlig behov for å føle oss som individer – med et eget privat rom. Gjennom menneskehetens historie har likevel tilgangen til et privatliv slik vi kjenner det i dag, vært svært begrenset. Det vanlige har vært at man lever, bor og sover i fellesskap. Det lille av informasjon som fantes om innbyggerne frem til ca. år 1900, i kirkebøker, gjennom folketellinger og lignende, var gjerne offentlig tilgjengelig.

Den 15. desember 1890 publiserte *Harvard Law Review* artikkelen «The Right to Privacy» av Samuel Warren og Louis Brandeis. Artikkelen anses som en av de mest innflytelsesrike i amerikansk og vestlig juridisk og filosofisk historie, og argumenterte for retten til et privatliv – med særlig fokus på «a right to be let alone».

Privatliv, teknologi og velferd har alltid hørt sammen. Økt tilgang på hus med flere rom, samtidig som stadig flere familier fikk råd til mer enn én seng, initierte den økende oppmerksomheten om «a right to be let alone». Oppfinnelsen av kameraet, og at man stadig oftere kunne oppleve å bli fotografert, økte bevisstheten om temaet.

Retten til respekt for privatlivet er i dag for lengst rubrisert som en menneskerettighet,[1] og retten har i Norge fått grunnlovs trinnhøyde.[2]

Så er spørsmålet; opplever vi nettopp nå privatlivets storhetstid? Kan vi ikke bare se bakover, på en tid med langt mindre privatliv – men også å se fremover – på en utvikling mot det samme?

Mens nye teknologier har vært en forutsetning for privatlivets fremvekst, ser vi i dag at ny teknologi kanskje også kan forårsake privatlivets fall – teknologi, sammen med en mektig trussel mot vår trygghet, nemlig terror og annen alvorlig kriminalitet.

2. GRUNNLOVEN OM BALANSEPUNKTET

Det har stort sett gått én vei når personvernhensynet har blitt avveid mot ønsket om nye metoder for å bekjempe alvorlig kriminalitet. Det har blitt funnet for lett, og har måttet vike.

Jeg skal ikke si at retningen i seg selv har vært gal. Vårt samfunn står overfor utfordringer som ikke tidligere var der. Å sørge for borgernes trygghet er en av statens mest sentrale oppgaver. Vi må i en viss grad finne oss i at det gjøres inngrep i privatlivet for å motvirke visse typer kriminalitet.

Som alle er enige om må vi finne balansen mellom de to umistelige verdiene; trygghet og privatliv. Men hvor balansepunktet befinner seg, er det uenighet om.

Rettslig sett angir Grunnloven § 102 balansepunktet. Denne fastslår at

> *«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon».*

[1] Jf. bl.a. EMK artikkel 8.
[2] Jf. Grl. § 102.

Det er sikker rett at bestemmelsen skal forstås slik at muligheten for å gjøre inngrep i rettigheten er den samme som følger av EMK artikkel 8 nummer 2.

Kort fortalt: Overvåkning skal ha hjemmel i lov, og den skal ivareta et nærmere angitt formål. I tillegg skal den skal være nødvendig for å oppnå dette formålet. Med «nødvendig» siktes det til hva som er nødvendig i et demokratisk samfunn. Dette betyr at en ren interesseavveiing ikke er tilstrekkelig. Det kreves etter rettspraksis at det foreligger et *presserende samfunnsmessig behov* for overvåkningen, og at den står i forhold til formålet. Det skal være proporsjonalitet mellom inngrep og mål.

Dessuten – som et utslag av forholdsmessighetskravet – er det et krav om tilstrekkelige rettssikkerhetsgarantier ved bruken av inngrepet.

Når vi snakker om at «det gjelder å finne den rette balansen» har vi altså nedfelt oppskriften for dette i vår grunnlov.

La oss i det følgende se nærmere på hva som ligger i vektskålene når de umistelige, men til dels motstridende, verdiene skal veies mot hverandre.

3. BETYDNINGEN AV PRIVATLIVET

Vi forstår alle hva trygghet er verdt. Begreper som samfunnssikkerhet og terrorbekjempelse gir høyst konkrete assossiasjoner for oss alle.

Privatlivet derimot, er mer vagt. Hva er verdien av dette, egentlig?

De fleste av oss vil prioritere livet foran privatlivet. Føler man seg truet, vil mange akseptere overvåkning som et nødvendig onde. Ja, innenfor terrorfryktens logikk er det helt naturlig med et spørsmål man kan høre ganske ofte; «hvorfor er det så farlig om man blir overvåket, kikket i kortene, hvis man har rent mel i posen?».

Jeg skal forsøke å være konkret når det gjelder privatlivets verdi – og hva som står på spill.

Overgangen fra barn til ungdom og voksen, er nettopp en reise fra formynderi, der foreldrene ser og bestemmer alt – via stadig mindre innsyn og tilsyn – til man en dag selv er moden for å ta kontroll over sitt privatliv.

Privatlivet er en forutsetning for vår voksne selvråderett og selvrespekt – for et liv uten innsyn og innblanding utenfra – fra noen som har myndighet til å følge med, reagere og korrigere.

Hvordan skal vi kunne utvikle vår voksne identitet og personlighet – uten et privatliv? Og våre mange ulike sosiale sfærer – defineres ikke de nettopp av graden av hvor eksklusive og intime de er? Fra den offentlige sfære, via de mer private med kolleger og venner, til våre innerste sirkler av familie, ektefelle eller kjæreste – og aller innerst oss selv? Hva skjer med alt dette, hvis vi mistenker at noen ser på?

Personvernet og respekten for privatlivet er en forutsetning for selvrespekt, for gjensidig tillit og dype vennskap, for intimitet og kjærlighet. Uten et privatliv vil ikke retten til frihet, individualitet, identitet og et tillitsbasert sosialt liv la seg danne og opprettholde.

Økende overvåkning endrer oss som individer – men også som samfunnsmedlemmer. Man vil la handlinger og ytringer påvirkes av frykten for å etterlate seg spor som kan gi negative konsekvenser. Dette kalles gjerne for nedkjølingseffekt.

En Oxford-studie i kjølvannet av Snowden-avsløringene i 2013 viste 20 prosent nedgang i sidevisninger på Wikipedia-artikler som handlet om terrorisme, og som for eksempel nevnte «Al-Qaeda», «bilbombe» eller «Taliban».[3] En av forskerne uttalte følgende til The Washington Post:

> *«Hvis folk blir skremt eller usikker på konsekvensene av å lese om viktige politiske temaer som terrorisme og nasjonal sikkerhet, er det en reell trussel for den opplyste demokratiske debatten»*.[4]

Nedkjølingseffektens press på ytringsfriheten vil begrense åpen meningsutveksling, og dette i større grad jo lenger fra det konforme sentrum en mening befinner seg. Dette vil i sin tur svekke demokratiet og dets legitimitet.

Vår trygghet er en svært tung vekt i den ene vektskålen. Vårt liv og vårt samfunn slik vi kjenner det i dag, ligger i den andre.

4. UTVIKLINGEN I OVERVÅKNINGSMETODENE

4.1. Innledning

Listen med tilgjengelige skjulte politimetoder har de siste tiårene est ut. Parallelt med at antallet metoder har vokst, har også anvendelsesområdet for metodene, blitt utvidet.

Grunntanken bak det betydelige lovarbeidet har blant annet vært at kriminaliteten har blitt mer internasjonal, at samfunnet har blitt mer uoversiktlig – og at den teknologiske utviklingen har gitt kriminelle nye verktøy.[5]

Særlig lovendringene som trådte i kraft i 2000, førte til en solid utvidelse av katalogen med skjulte tvangsmidler.[6]

Politiet fikk da blant annet tilgang til hemmelig ransaking,[7] teknisk sporing i kjøretøy eller andre gjenstander og klær eller annet som mistenkte bærer på seg,[8] og hemmelig beslag.[9] I tillegg ble anvendelsesområdet for kommunikasjonskontroll[10] utvidet. I 2005 ble romavlytting vedtatt, samtidig

[3] Tilgjengelig her per 16. november 2017: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645.
[4] Tilgjengelig her per 16. november 2017: https://www.washingtonpost.com/news/wonk/wp/2016/04/27/new-study-snowdens-disclosures-about-nsa-spying-had-a-scary-effect-on-free-speech/?utm_term=.50853b5c7160.
[5] Se NOU 1997: 15 s. 6 flg.
[6] Jf. lov av 3. desember 1999 nr. 82.
[7] Jf. strpl. § 200 a.
[8] Jf. hhv. strpl. §§ 202 b og 202 c.
[9] Jf. strpl. § 208 a.
[10] Jf. strpl. § 216 a.

som det ble åpnet for bruk av skjulte tvangsmidler i avvergende og forebyggende øyemed, det vil si før det overhodet er begått noe kriminelt.[11]

Etter en blindvei via Datalagringsdirektivet, fikk vi i fjor dessuten dataavlesning som ny metode, og i dag ligger forslaget om det digitale grenseforsvar til behandling i Forsvarsdepartementet.

Alt dette har skjedd på bare 17 år.

Samtidig ser vi at straffeprosessuelle prinsipper settes under press. Eksempelvis utfordres utgangspunktet om at det må foreligge skjellig grunn til mistanke mot noen for å anvende et tvangsmiddel mot dem. Vi ser det i den nye bestemmelsen om bruk av tvang ved biometrisk autentisering ved ransaking av datasystem – som også retter seg mot andre enn mistenkte og deres datasystem.[12] Vi ser det i adgangen til å sikre elektronisk lagrede data i for eksempel mobiltelefoner i utlendingssaker hvor utlendingen ikke er mistenkt for noe kriminelt,[13] og vi ser det i masseovervåkningen som digitalt grenseforsvar vil føre med seg.

4.2. Formålsutglidning

En ny overvåkningsmetode blir gjerne vedtatt for svært avgrensede tilfeller.

Men så ser man at de tilfellene metoden kan benyttes for, sakte, men sikkert blir flere.

Dette fenomenet kalles «formålsutglidning», og jeg tror de fleste av oss kan kjenne oss igjen i mekanismen. Vi kjøper TV til hytta kun for å følge med på Dagsrevyen, men når den først henger på veggen, ønsker vi også å se Gullrekka.

La oss gå tilbake i tid og se hvordan formålsutglidningen kan arte seg.

Adgangen til å foreta kommunikasjonskontroll ble innført i 1915. Denne gjaldt post- og telegrafkontroll i saker om rikets sikkerhet.[14] Fra 1950 gjaldt den også telefonsamtaler.[15]

26 år senere forlot man rikets sikkerhet som eneste grunnlag, ved at en midlertidig lov åpnet for telefonkontroll også ved etterforskning av narkotikalovbrudd.

I 1992 ble ordningen gjort permanent og flyttet til straffeprosessloven. Justiskomiteen understreket at;

> *«telefonavlytting er et ekstraordinært etterforskningsmiddel som bare må tillates brukt ved alvorlig og sterkt samfunnsskadelig kriminalitet der andre etterforskningsmetoder kommer til kort.»*[16]

[11] Se strpl. § 222 d og politil. § 17 d.
[12] Jf. strpl. 199 a.
[13] Se Det kongelig justis- og beredskapsdepartement, Høring om forslag til endringer i utlendingslovens regler om tvangsmidler, 19. desember 2016 s. 84 og 100.
[14] Jf. lov 24. juni 1915 nr. 5 om kontroll med post- og telegrafforsendelse og med telefonsamtaler § 1.
[15] Jf. lov 15. desember 1950 nr. 5.
[16] Jf. Innst.O.nr.61 (1991-1992) Innstilling fra justiskomiteen om lov om endringer i straffeprosessloven (telefonavlytting i narkotikasaker) pkt. 3.1.

Syv år senere ble adgangen til telefonavlytting gjort generell – i saker med strafferamme på fengsel i 10 år eller mer. Dette gjaldt foruten alvorlige allmennfarlige forbrytelser også blant annet grove legemsbeskadigelser og kvalifiserte former for pengefalsk.[17]

I 2016 ble det, som en foreløpig slutt, åpnet for kommunikasjonsavlytting i saker som gjelder «alvorlige integritetskrenkelser» og i tillegg kjennetegnes av «alvorlige etterforskningsmessige utfordringer».[18]

Også *romavlytting* er et godt eksempel på formålsutglidning. Utgangspunktet var at myndighetene hadde store kvaler ved innføringen av metoden.

I et høringsnotat[19] fra 1984 avviste departementet romavlytting og viste til at det synes

> *«… å være allmenn enighet om at det her må settes grenser selv om formålet med overvåkingen på det enkelte område er det beste»*.

Departementet imøtekom heller ikke Metodeutvalgets forslag om å innføre romavlytting 13 år senere.[20] Betenkelighetene var så store at metoden ikke kunne rettferdiggjøres.[21]

Seks år senere – etter Politimetodeutvalgets utredning – mente imidlertid departementet at det forelå et dokumentert behov for romavlytting, og dagens hjemmel ble innført i 2005.[22]

Departementet understreket da at det er begrenset hvor langt samfunnet kan gå i å tillate romavlytting og andre inngripende metoder, uten at mange ville oppfatte prisen – i form av inngrep i den personlige sfære – som for høy.[23] Romavlytting måtte gis et «svært begrenset anvendelsesområde», skrev departementet.[24]

Omtrent 10 år senere ble likevel kravet om tilknytning til organisert kriminalitet ved bruk av romavlytting i drapssaker, fjernet. Departementet uttalte da at manglende metodetilgang ikke bør stå i veien for oppklaring.[25]

4.3. Dataavlesning

Krypteringsløsninger er tilgjengelig for alle, og gjør det vanskelig å utføre kommunikasjonskontroll og ransaking av innholdet på datamaskiner og smarttelefoner. Med dataavlesning, som ble innført i 2016, overvinnes krypteringshinderet.[26]

---

[17] Se Ot.prp. nr. 64 (1998–99) pkt. 8.3.1.4.
[18] Jf. Prop. 68 L (2015-2016) pkt. 1.3.
[19] Jf. høringsnotat av 8. november 1984.
[20] Jf. NOU 1997: 15 Etterforskingsmetoder for bekjempelse av kriminalitet.
[21] Jf. Ot.prp. nr. 64 (1998-1999) pkt. 11.2.6.
[22] Jf. strpl. §§ 216 m og 222 d.
[23] Jf. Ot.prp.nr.60 (2004-2005) s. 96 flg.
[24] Jf. Ot.prp.nr.60 (2004-2005) s. 99.
[25] Jf. Prop. 68 L (2015-2016) s. 138.
[26] Jf. lov av 17. juni 2016 nr. 54.

Begrepet «dataavlesning» er ikke et entydig teknologisk begrep, men innebærer i hovedsak at politiet kan hacke seg inn på personers PC eller mobiltelefon for å se hva som foregår der, på et tastatur eller på en skjerm – i sanntid. Kryptering er altså nytteløst.

Det var Metodekontrollutvalget som fikk oppdraget med å vurdere innføring av dataavlesning. Skjønt, konklusjonen var bestilt på forhånd; etter mandatet skulle utvalget «utrede og foreslå regler som tillater at politiet tar i bruk dataavlesing som metode».[27]

Metodekontrollutvalget foreslo dataavlesning kun som en fremgangsmåte for kommunikasjonskontroll og hemmelig ransaking.[28]

I høringsrunden var PST, NAST,[29] Kripos, Politidirektoratet, Oslo politidistrikt og Økokrim samstemte.[30] Dataavlesning burde brukes til mer enn bare å overvinne krypteringer ved bruk av eksisterende metoder. PST slo eksempelvis fast at ransaking, eventuelt gjentatt ransaking, ikke gir noen garanti for at relevante dokumenter avdekkes. De kan være borte når ransakingen skjer. Dataavlesning i sanntid er mer effektivt.

Politietatene fikk gjennomslag.

Dette er det grunn til å feste seg ved: Den opprinnelige hovedbegrunnelsen for å innføre dataavlesning, nemlig å overkomme krypteringshindre, ble forlatt. Formålsutglidningen skjedde denne gangen faktisk raskere enn lovbehandlingen. Teknologien gikk fra å være et hinder, til å bli en mulighet.

5. KONTROLL MED OVERVÅKNINGEN

5.1. Domstolskontroll

Domstolskontroll er lovgivers beroligende medisin når nye metoder innføres. Men dette er faktisk obligatorisk etter EMK. Vilkårlige inngrep skal hindres og det skal foretas en legalitetskontroll.

Men domstolskontrollen har sine svakheter:

Skjulte politimetoder er nettopp skjulte. Den det begjæres dataavlesning hos, vet ikke at det skjer.

Kontradiksjonsprinsippet er domstolenes viktigste verktøy for å opplyse en sak. Men her settes det til side. Den mistenkte kan ikke ta til motmæle. En domstolsbehandling som tilfredsstiller alminnelige krav til rettferdig rettergang, er utenfor rekkevidde.

Straffeprosessloven forsøker imidlertid å bringe en slags kontradiksjon inn i saken. Etter loven skal det oppnevnes en advokat for mistenkte.[31] Denne skal ivareta den mistenktes – og eventuelle tredjepersoners – interesser ved behandlingen av begjæringen om for eksempel avlytting. Advokaten

[27] Jf. NOU 2009: 15 s. 17 pkt. 1.3.
[28] Jf. NOU 2009: 15 s. 237 og 244.
[29] Det nasjonale statsadvokatembetet for bekjempelse av organisert og annen alvorlig kriminalitet.
[30] Jf. Prop. 68 L (2015-2016) s. 250-251.
[31] Jf. strpl. § 100 a.

kan imidlertid ikke ta kontakt med mistenkte – eller de berørte tredjepersonene – for å få opplysninger om saken.

Denne advokatrollen har mange navn. I straffeprosessloven omtales vedkommende som «offentlig advokat». I dagligtale kan vi støte på begreper som «skyggeadvokat» og «kjelleradvokat». Navnet skyggeadvokat har antakelig oppstått fordi mistenkte og dennes forsvarer bare kan ane tilstedeværelsen av advokaten – ved at denne tydeligvis har vært inne i saken tidligere. «Kjelleradvokat» kommer av at arbeidet fra tid til annen foregår i kjellere, avhengig av tinghusenes beskaffenhet.

Skyggeadvokaten får se dokumentene i papirformat på en skjermet arbeidsplass i tinghuset. Der står det også en PC med printer som skal benyttes. Ingen dokumenter skal tas med ut. Det er i utgangspunktet ingen muntlige forhandlinger.

Siden mistenkte ikke vet om bruken av tvangsmidlene, er advokatens rolle kanskje viktigere enn i de øvrige delene av straffeprosessen, skrev Metodekontrollutvalget.[32] Da er det et paradoks at advokatrollen i disse sakene samtidig har de dårligste rammevilkårene i straffeprosessen.

Selv om det er vanskelig å bedømme totalbildet i gjeldende statistikk, viser den klart at skyggeadvokatenes gjennomslagskraft er marginal. I 2016 ble det brukt kommunikasjonskontroll i 135 saker. I *to* saker avslo tingretten politiets begjæring. I begge sakene ble det gitt samtykke etter anke.[33] Mens det i 2015 ikke var noen forsvareranker som nådde frem, var det én i 2016.

Tallene er et naturlig resultat av systemet.

Lund-kommisjonen tegnet i sin tid et dystert bilde av hvordan domstolskontrollen den gang fortonet seg.[34] Kommisjonen refererte følgende fra en samtale med tidligere overvåkningssjef Jostein Erstad:

> *«Generelt vil Erstad si at det var svært så lett, kanskje for lett, å få rettens medhold i begjæringer om telefonkontroll.»*

Lund-kommisjonen uttalte at det var samlet sett «ingen tvil» om at domstolene ikke hadde vært den rettssikkerhetsgaranti de var ment å være. Kommisjonen antok at forhørsrettens ukritiske holdninger hadde sammenheng med at *«dommeren lett vil mene at han har begrenset kunnskap om de faktiske forhold og ikke har den oversikt som skal til for å sette spørsmålstegn ved overvåkningstjenestens vurderinger»*.[35]

Jeg er bekymret for at problemene fortsatt er gjeldende. Hør bare hva Bergen tingrett skrev om overforbruket av varetektsfengsling i sin høringsuttalelse om den nye straffeprosessloven:

> *«Retten har en mistanke om at langvarige fengslinger ofte er mer oppbevaring enn av reell betydning for oppklaring av saken. Gjeldende regler er skjønnsmessige, avgjørelser blir i praksis truffet raskt og på begrenset grunnlag, og fengslingshyppigheten er høy, blant annet som følge*

[32] Jf. NOU 2009: 15 s. 133.
[33] Jf. Kontrollutvalget for kommunikasjonskontroll, Årsrapport 2016 s. 3-4.
[34] Jf. Rapport til Stortinget fra kommisjonen som ble oppnevnt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere («Lund-rapporten») s. 676.
[35] Jf. Rapport til Stortinget fra kommisjonen som ble oppnevnt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere («Lund-rapporten») s. 678.

av at den som treffer avgjørelsen er redd for å ødelegge oppklaring av saken, basert på en slik begrenset oversikt.»[36]

Det har formodningen mot seg at dette ikke også gjelder i saker om bruk av skjulte metoder, ikke minst i saker om forebygging av alvorlig kriminalitet.

Jeg ønsker ikke på noen måte å kritisere dommerne. Det jeg er redd for, er at vi har et system som setter dem i en umulig situasjon, på lik linje med skyggeadvokatene.

Hvor lett er det for en dommer å avvise en begjæring om telefonavlytting når PST sier det er grunn til å undersøke om noen forbereder en terrorhandling? Konsekvensene av et nei for mye, kan være katastrofale. Konsekvensene av et ja for mye, er mindre. Den mistenkte som etter å ha fått sitt privatliv overvåket i alle sine intime detaljer, og som viste seg å ikke planlegge noe galt, får sannsynligvis aldri kjennskap til hva som skjedde.

Politiet presenterer faktum i sakene, og begrunner sitt behov for å ta metoden i bruk. Definisjonsmakten ligger hos politiet, mens et uhåndterlig ansvar og umulige rammevilkår – ligger hos advokat og dommer.

Problemet blir ikke mindre av at domstolenes legalitetskontroll i stor grad foregår først etter at kommunikasjonskontrollen er igangsatt. Politiet har adgang til å iverksette hurtigoppkopling, hvilket skjer i hele 35 % av sakene.[37] Dette har sine plausible forklaringer, men forutgående domstolskontroll skjer altså bare når politiet mener det er tid til det.

Det er mulig å forbedre domstolskontrollen: Vi må få skyggeadvokaten ut av kjelleren og inn i rettssalen.

Metodekontrollutvalget foreslo en hovedregel om muntlige forhandlinger.

Til dette uttalte departementet at det vil kunne gjøre det enklere å få avklart uklare sider ved begjæringene, og senke terskelen for å fremme innsigelser mot dem. Departementet la likevel avgjørende vekt på at muntlige forhandlinger kan forsinke gjennomføringen av tvangsmidlene slik at metodenes effektivitet svekkes.[38] Forslaget ble derfor ikke fulgt opp. Rettssikkerheten måtte vike for effektivitet. En hovedregel om muntlige forhandlinger fremstår for meg som en åpenbar løsning for å bringe en mer effektiv kontradiksjon inn i saken. Sakene kan inntas i fengslingsturnusene til forsvarerne uten at særlig tid går til spille.

5.2. Etterfølgende kontroll

I tillegg til den forutgående domstolskontrollen, skjer det også en etterfølgende kontroll med om metodene faktisk brukes slik loven foreskriver. Kommunikasjonskontrollutvalget – eller KK-utvalget – kontrollerer metodebruken i straffeprosess-sporet, mens EOS-utvalget fører kontroll med PSTs forebyggende bruk av tvangsmidler.

[36] Jf. Bergen tingrett, Høring – NOU 2016: 24 Ny straffeprosesslov, 6. juni 2017 s. 5-6.
[37] Jf. Kontrollutvalget for kommunikasjonskontroll, Årsrapport 2016.
[38] Jf. Prop. 68 L (2015-2016) s. 65-66.

Kontrollen viser i hvilken grad metodene faktisk virker, i tillegg til hvor mye de brukes. Tidligere var omfanget av bruken av romavlytting gradert informasjon, men nå offentliggjøres dette. Det er positivt. Offentlig tilgjengelig informasjon er en forutsetning for demokratisk kontroll.

Når det gjelder informasjon om hvordan og i hvilket omfang dataavlesning skjer, er dette derimot gradert informasjon som ikke tas inn i rapportene.[39] Jeg håper man også her så snart som mulig finner anledning til å operere med åpenhet.

Etterkontrollen av dataavlesning er for øvrig problematisk. Det er lagt opp til at politiet skal føre protokoll over dataavlesningen. Denne vil bli det sentrale grunnlaget for KK-utvalgets vurderinger. Etter kommunikasjonskontrollforskriften skal blant annet opplysninger om hvilke typer data som er avlest, protokollføres.[40]

Når dataavlesning til slutt ble vedtatt som en metode for å se alt som foregår i en datamaskin, passer en slik protokollføring dårlig. Går det i det hele tatt an å protokollere surfing, streaming, dating, chatting, radio, Skype, netthandel, kalenderoppdateringer, plasseringsdata og spill? I sanntid? Det er den som gjennomfører dataavlesningen som vil måtte gjøre et utvalg – og bestemme hva som protokollføres. Og ved dataavlesning er det politiet selv som hacker seg inn, ingenting er kontrollerbart gjennom spor hos leverandører som Telenor og Telia. KK-utvalgets grunnlag vil ikke være fullverdig.

Jeg mener vi bør vente med å ta dataavlesning i bruk, eventuelt slutte å bruke metoden, til praktiske og effektive kontrollmidler foreligger. Det samme gjelder PSTs bruk av dataavlesning; heller ikke her har man et rammeverk som sikrer EOS-utvalget nok kunnskap om bruken.

Kontroll med overvåkningen er grunnleggende. Det fremhever også lovgiver når nye metoder innføres. Det forekommer faktisk regelbrudd. Vi vet at det har foregått ulovlig avlytting av samtaler mellom advokat og klient, og at opptakene ikke straks har blitt avbrutt og slettet,[41] men vi får ikke kjennskap til verdien for etterforskningen. Vi vet også at ulovlig bevismateriale er brukt ved domfellelser i Norge.[42]

Tidligere i år ble det kjent at PST hadde overvåket Bent Endresens advokatvirksomhet ulovlig. Dette er samfunnsskadelig. Når det blir kjent at PST ulovlig overvåker advokater, svekkes tilliten til at man kan oppsøke advokatbistand i fortrolighet. Dette handler om mer enn rettssikkerheten til den som PST har mistanker mot. Dette handler om en velfungerende rettspleie. Da jeg snakket med Endresen på telefon om saken, var det med en underlig følelse av at det var noen andre til stede. Men dette er ingenting i forhold til det Endresens klienter må ha følt da de fikk vite om det inntrufne. Hva hadde de – i sin feilslåtte tillit til at samtalen var fortrolig – fortalt til Endresen?

«Snakk ikke i telefonen med klienter som har alvorlige straffbare forhold knyttet til seg selv», konkluderte advokat Mette Yvonne Larsen på Advokatforeningens menneskerettsseminar tidligere i år.[43]

---

[39] Jf. Kontrollutvalget for kommunikasjonskontroll, Årsrapport 2016 s. 4.
[40] Se kommunikasjonskontrollforskriften §§ 7 og 16.
[41] Se for eksempel HR-2015-181-A.
[42] Se https://www.nrk.no/norge/fbi-hacking-brukt-som-bevis-i-norske-saker-1.13318151. Lastet ned 21. november 2017.
[43] D.v.s. 2017.

6. DET DIGITALE GRENSEFORSVAR

I februar 2016 nedsatte regjeringen Lysne II-utvalget for å utrede en eventuell tilgang for Etterretningstjenesten til kabelbasert digital kommunikasjon som krysser den norske landegrensen – et såkalt digitalt grenseforsvar – eller DGF. 99 prosent av all kommunikasjon inn og ut av Norge går gjennom disse kablene.[44] Seks måneder senere forelå utvalgets rapport på 89 sider som konkluderer med at DGF er nødvendig for nasjonens sikkerhet.[45]

Grenseforsvar høres tilforlatelig ut. Vi forsvarer jo våre grenser mot smugling av alkohol og narkotika, så hvorfor ikke også kontrollere data fra utlandet?

Det tilfeldig hvilke data som krysser landegrensen. Spørsmålet er ikke hvem som sender data til hvem, og hvor de befinner seg – men hvilke servere dataene må innom – og hvor disse befinner seg. Da vi sendte ut invitasjon til denne talen på e-post, gikk den kanskje via utlandet. E-posten velger minste motstands vei, med lysets hastighet. Og dataene du lagrer i skyen; befinner de seg alltid i Norge?

Gjennom DGF vil E-tjenesten lagre en enorm mengde informasjon, der bare en mikroskopisk andel er relevant for deres oppdrag. Regjeringen vil imidlertid ikke bruke begrepet «masseovervåkning» – som dette jo faktisk er. Og begrunnelsen? Igjen skal offentligheten beroliges med henvisning til høyst mangelfulle kontrollmekanismer.

Lysne II-utvalget foreslo nemlig at alle søk i den lagrede informasjonen må godkjennes av «DGF-domstolen» basert på klare kriterier hvor krav til nødvendighet og forholdsmessighet blir ivaretatt. DGF-domstolen skal etter forslaget bestå av et mindre antall dommere med *«grunnleggende forståelse for etterretningsfaget og innsikt i etterretningsvurderinger og trusselbildet som ligger til grunn for anmodninger om søk»*.[46] Utvalget erkjenner selv at det vil være en risiko for at dommerne etter hvert kan identifisere seg med tjenestens virke og oppgaver. Det gjør de etter mitt syn rett i – i tillegg til manglende kontradiksjon, vil man i disse sakene også få manglende uavhengighet.

EU-domstolen har i den såkalte Tele 2-dommen av 21. desember 2016 imidlertid gått mer kritisk til verks i tilsvarende spørsmål.[47]

Dommen er tydelig på at kommunikasjonsdata om enkeltmennesker bare kan lagres under forutsetning av at det eksisterer en sammenheng mellom dataene som lagres, og en konkret trussel mot den offentlige sikkerhet. Etter Advokatforeningens mening viser avgjørelsen at en generell og udifferensiert lagring av trafikk- og lokaliseringsdata ikke kan tillates – uansett hvor grunnleggende det enn er å

---

[44] Se https://www.vg.no/nyheter/innenriks/norsk-politikk/e-sjefen-frykter-dataangrep-mot-stortingsvalget/a/23903214/. Lastet ned 22. november 2017.
[45] Jf. Lysne II-utvalget, Digitalt grenseforsvar (DGF), 26. august 2016.
[46] Jf. Lysne II-utvalget, Digitalt grenseforsvar (DGF), 26. august 2016 pkt. 9.3.2.
[47] Forente saker C-2013/15 og C-698/15. Dommen slår fast at så vid datalagringslovgivning som innført av Sverige og Storbritannia – strider mot EUs kommunikasjonsverndirektiv og EUs Charter artikkel 7 om retten til privatliv og artikkel 8 om retten til personopplysningsvern. Se særlig avsnitt 103: http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A62015CJ0203.

bekjempe organisert kriminalitet og terrorisme. Vi kan vanskelig se hvordan forslaget til DGF skal kunne imøtekomme det vern av privatlivet som ligger i EMK artikkel 8 og i Grunnloven § 102.

7. AVSLUTNING

Det har så vidt jeg vet aldri vært en terrorhandling i Nord-Korea, og jeg vil tro at kriminaliteten er lav. Men jeg vil ikke bo der. USA og Europa har blitt rammet av terror flere ganger, men veldig mange ønsker å leve nettopp her.

Jeg startet denne talen med å si at de fleste vil prioritere livet foran privatlivet. Fullt så enkelt er det altså ikke.

Jeg sa også at privatliv og trygghet ligger i hver sin vektskål. Også dette er en sannhet med modifikasjoner, for retten til et privatliv åpner nok noen muligheter for terrorister og forbrytere – men denne retten er samtidig et vern mot overgrep fra en annen mektig aktør; nemlig staten selv.

Jo mer informasjon om borgerne vi lar staten samle, desto mer makt har den over oss alle.

Vi må ha overvåkning, men vi vi må også ha privatliv og personvern.

Initiativene til nye overvåkningsmetoder kommer fra de myndighetene som skal ta dem i bruk. Og det er disse som leverer premissene for lovgivers vurdering av om de skal innføres. De sitter på trusselvurderingene. Det er vanskelig å stå imot. Politikerne står tilsynelatende overfor den samme utfordring som dommerne: Man er redd for å ødelegge. Følgene av å si nei er potensielt katastrofale, følgene av å si ja mer vage. Man fjerner bare enda en liten bit av personvernet og privatlivet.

Dette skjer i en tid hvor sporene etter vår livsførsel aldri har vært flere og mer tilgjengelige.

På nært hold kan hver bit av personvernet og respekten for privatlivet, være vanskelig å se betydningen av. Men etter hvert som de fjernes, vil det store bildet endre seg.

I dag kan våre myndigheter hacke seg inn på en persons datamaskin i forebyggende øyemed – før en eventuell forberedelse til en eventuell straffbar handling har startet.[48] Før tolket vi Grunnloven slik at den oppstilte et forbud mot husransakelser unntatt i «kriminelle tilfeller». Nå tolker Stortinget den slik at ransakelser også er greit for å forebygge fremtidige «kriminelle tilfeller».[49]

Underveis har vi i tillegg vedtatt datalagringsdirektivet. Det ble aldri satt i kraft fordi EU-domstolen fastslo at det stred mot grunnleggende europeisk kommunikasjonsvern. Vi vurderer nå likevel å innføre tilsvarende i form av det digitale grenseforsvar.

Vet vi hva vi gir fra oss? Har utviklingen konsekvenser for vår egen lovlydige adferd? Kan vissheten om at noen kan lete frem opplysninger om hva vi gjør, hva vi ytrer og hva vi mener, hemme oss i vår rettmessige livsutfoldelse? Og hvis ikke oss – hva med andre; hva med outsiderne? Hva med journalistenes kilder og advokatens klienter? Og hva betyr dette for meningsdannelsen, opposisjonen

[48] Se politil. § 17 d, jf. strl. § 131 tredje ledd.
[49] Knf. Norges nasjonale institusjon for menneskerettigheter, *Årsmelding* Dokument 6 (2016-2017) s. 117.

og demokratiet? Når risikerer vi at vi har ofret det livet og demokratiet vi elsker – for å beskytte oss mot de handlinger vi frykter?

Dette vet vi ikke nok om.

EMK artikkel 8 og Grunnloven § 102 er vårt liberale grenseforsvar – vår rettsstatlige beredskapsplan som skal verne privatlivet, demokratiet og samfunnet. Slik vi kjenner det – og vil bevare det.

Privatlivet behøver en advokat. I et forsøk på å fylle den rollen for én kveld, fremmer Advokatforeningen følgende anbefalinger:

- Vi må ha forskning på nedkjølingseffekten.
- Vi behøver en utredning om personvernet på justisfeltet. Hva er status – hvor vil vi?
- I mellomtiden må vi innføre en hovedregel om muntlige forhandlinger i skyggeadvokat-sakene. Vi må verne om grunnleggende straffeprosessuelle prinsipper. Dataavlesning får vi vente med til vi har på plass et rammeverk som sikrer effektiv kontroll.
- Det digitale grenseforsvar vil representere et skritt inn i masseovervåkningens verden. Advokatforeningen støtter synet til flere tunge juridiske høringsinstanser, blant annet Stortingets egen nasjonale institusjon for menneskerettigheter – og anbefaler at DGF ikke innføres.