DET KONGELIGE
UTENRIKSDEPARTEMENT

Lysneutvalget
ved utvalgssekretær Ragnhild Castberg

Kopi: JD og FD

Deres ref.:	Vår ref.:	Dato:
	-	29.5.2015

Folkerettslige rammer for grenseoverskridende informasjonsinnhenting

Det vises til henvendelse av 10. mars d.å. fra sekretariatet for det digitale sårbarhetsutvalget (Lysneutvalget), hvor Utenriksdepartementets rettsavdeling bes om bistand til å utrede følgende punkt i utvalgets mandat:

«Utvalget skal beskrive de sentrale folkerettslige rammer for grenseoverskridende informasjonsinnhenting.»

Utenriksdepartementet merker seg at utvalget ifølge mandatet ikke skal vurdere konsekvensene for norsk rett av EU-domstolens avgjørelse i saken om datalagringsdirektivet. Dette direktivet blir derfor ikke berørt i departementets innspill nedenfor. I lys av utvalgets øvrige mandat, forstår vi med grenseoverskridende informasjonsinnhenting i det følgende for det første overvåkning og informasjonsinnsamling i det digitale rom foretatt av en stat med virkning i en annen stat, med eller uten den andre statens samtykke. Slik informasjonsinnhenting kan være rettet mot private eller mot andre stater/myndighetspersoner. Videre forstår vi grenseoverskridende informasjonsinnhenting som mottak av informasjon fra utenlandske myndigheter innenfor rammen av f.eks. internasjonalt gjensidig strafferettslig samarbeid eller etterretningssamarbeid. Eventuell etterfølgende bruk, lagring eller deling av den innhentede informasjonen reiser også rettslige problemstillinger.

Først vil vi behandle alminnelige folkerettslige skranker for grenseoverskridende informasjonsinnhenting, herunder først og fremst suverenitetsprinsippet (punkt 1). Deretter vil vi kort omtale begrensninger som følger av Wien-konvensjonen om diplomatisk samkvem (punkt 2). Overvåkning og informasjonsinnhenting må videre

Postadresse:
Postboks 8114 Dep
0032 Oslo

Kontoradresse:
7. juni plass 1
0251 Oslo

Bank innbetalinger:
7694.05.12618
Org. nr.:972417920

Telefon:
23 95 00 00
Telefaks:
23 95 00 99

Elin Widsteen
seniorrådgiver
post@mfa.no
www.regjeringen.no/ud

skje innenfor rammene av de internasjonale menneskerettighetene (punkt 3). Vi vil også omtale Europarådets konvensjon nr. 108 om personvern (punkt 4) og Europarådets konvensjon nr. 185 om datakriminalitet (punkt 5).

Den stadig økende digitaliseringen av samfunnet har medført nye folkerettslige problemstillinger. Det er enighet om at den alminnelige folkeretten i utgangspunktet kommer til anvendelse på overvåkning og informasjonsinnhenting i det digitale rom. Samtidig kan det være usikkerhet og diskusjon knyttet til hvilket resultat anvendelse av gjeldende folkerett vil få i konkrete saker. Dette er derfor et område hvor folkeretten fortsatt ikke nødvendigvis alltid gir klare svar og hvor den kan være under utvikling. Dessuten medfører den teknologiske utviklingen at det kan være uklart om en stat utfra de konkrete omstendighetene kan holdes ansvarlig for en bestemt handling eller unnlatelse, dvs. om staten har jurisdiksjon.

De ulike folkerettslige spørsmålene som gjennomgås nedenfor er bare i begrenset grad regulert i traktater. Når det gjelder avgjørelser fra internasjonale domstoler, finnes det noen, men de er hovedsakelig knyttet til menneskerettslige problemstillinger (punkt 3). Enkelte folkerettslige vurderinger kan gjøres ut fra statspraksis og alminnelige folkerettslige prinsipper. Det foreligger også uttalelser fra f.eks. FNs høykommissær for menneskerettigheter og resolusjoner fra FNs generalforsamling. Selv om den folkerettslige rettskildeverdien av disse er begrenset, får de omtale nedenfor (punkt 3), bl.a. i lys av utvalgets anmodning til Utenriksdepartementet om å gjennomgå de internasjonale fora der problemstillingene blir drøftet.

Omtalen av menneskerettighetsforpliktelser gis relativt sett en bred plass i det følgende. Disse anses særlig relevant for utvalgets arbeid, og på dette området i folkeretten finnes det flere internasjonale rettsavgjørelser, særlig fra Den europeiske menneskerettighetsdomstolen.

1. Alminnelige folkerettslige skranker for grenseoverskridende informasjonsinnhenting

Med unntak for visse avgrensede områder er det få eksempler på traktatfestede forbud mot utenlandsetterretning eller spionasje i fredstid. Man må derfor falle tilbake på alminnelige folkerettslige prinsipper, herunder først og fremst suverenitetsprinsippet, dvs. prinsippet om en stats suverene myndighet på sitt territorium. Av suverenitetsprinsippet utledes bl.a. forbudet mot innblanding i en annens stats indre anliggende på dets territorium. Den internasjonale domstolen i Haag uttalte i dom av 7. september 1927 i Lotus-saken (Frankrike mot Tyrkia): "*[T]he first and foremost restriction imposed by international law upon a State is that — failing the existence of a permissive rule to the contrary — it may not exercise its power in any form in the territory of another State*".

Det er sjelden at stater har påberopt at etterretningsvirksomhet utgjør folkerettsbrudd. Det foreligger heller ingen avgjørelser fra internasjonale domstoler eller tribunaler som konkluderer med at spionasje i seg selv utgjør en suverenitetskrenkelse. Statenes manglede vilje til å påberope seg folkerettsbrudd skyldes nok dels at stater har ansett det nødvendig å ivareta sin egen mulighet til å drive etterretningsvirksomhet i utlandet. Til dette bildet hører også at statene har kunnet straffeforfølge spioner under nasjonal jurisdiksjon, eller – dersom disse har hatt diplomatisk immunitet – erklære disse *persona non grata*, jf. Wien-konvensjonen om diplomatisk samkvem av 1961 art. 9 (punkt 2).

Det legges på denne bakgrunn til grunn at det ikke er internasjonal konsensus om at grenseoverskridende etterretningsvirksomhet, herunder i det digitale rom, som utelukkende består i informasjonsinnhenting, og som ikke forårsaker noen form for fysisk skade eller tap av funksjonalitet, i seg selv utgjør en suverenitetskrenkelse. Det kan imidlertid diskuteres, ikke minst i lys av den tekniske utviklingen, om det kan tenkes situasjoner der de negative konsekvenser f.eks. på en stats økonomi (industrispionasje) er av en slik art at handlingen vil kunne utgjøre et brudd på suverenitetsprinsippet. Hensikten med informasjonsinnhentingen, og hvordan denne er foretatt, vil også kunne ha betydning.

Det nevnes i denne forbindelse at *NATO Cooperative Cyber Defence Centre of Excellence*, med kontor i Tallinn, har invitert en uavhengig ekspertgruppe til å utarbeide en manual om anvendelsen av folkeretten i det digitale rom i fredstid (som en oppfølgning av den såkalte Tallinn-manualen 1.0 som gjelder anvendelse av folkeretten på digital krigføring). Tallinn-manual 2.0 forventes å ville kaste nærmere lys over suverenitetsprinsippets anvendelse i en digital kontekst.

2. Wien-konvensjonen om diplomatisk samkvem

Wien-konvensjonen om diplomatisk samkvem av 1961 fastsetter rapportering om forholdene i vertslandet som en av funksjonene for en diplomatisk stasjon, jf. artikkel 3 nr. 1 (bokstav d). Informasjonsinnhenting er da en forutsetning. Imidlertid fremgår det av samme bestemmelse at denne aktiviteten skal foregå ved lovlige midler («by all lawful means»). Videre fremgår det av artikkel 41 nr. 1 og nr. 3 at vertslandets lover skal følges, og at ambassadens lokaler ikke skal benyttes på en måte som er i strid med stasjonens funksjoner slik de er fastsatt i konvensjonen. Dette legger begrensninger på denne type aktivitet.

Vertslandet kan erklære en diplomat som uønsket, *persona non grata*, dersom den anser at disse bestemmelsene ikke respekteres, jf. artikkel 9 nr. 1.

Wien-konvensjonen har også bestemmelser som beskytter den diplomatiske stasjons lokaler, områder, arkiver og korrespondanse, og setter derved grenser for vertslandets aktivitet overfor stasjonen.

3. Menneskerettslige skranker for informasjonsinnhenting

3.1. Innledning

Overvåkning og informasjonsinnhenting kan først og fremst komme i strid med retten til respekt for privatliv og korrespondanse, som vil bli behandlet nærmere under punkt 3.2. nedenfor. Andre menneskerettigheter kan imidlertid også være relevante. Overvåkning av en journalist vil f.eks. kunne innebære både et inngrep i journalistens privatliv og i vedkommendes ytringsfrihet.[1] Forsamlingsfriheten kan også etter omstendighetene være berørt.

Når det gjelder grenseoverskridende informasjonsinnhenting, reiser det seg et tilleggsspørsmål om internasjonale menneskerettigheter kan påberopes mot den staten som har innhentet opplysningene, også av personer som befinner seg utenfor statens territorium. Tilsvarende spørsmål reiser seg når en stat innhenter opplysningene på eget territorium, men virkningen i form av inngrep i privatliv eller kommunikasjon skjer utenfor statens territorium. Dette er spørsmål om menneskerettighetenes ekstraterritorielle anvendelse og vil bli nærmere belyst under punkt 3.3.

Det foreligger omfattende rettspraksis fra EMD vedrørende retten til et privatliv. Vi antar at hemmelig overvåkning og informasjonsinnhenting av hensyn til nasjonal sikkerhet og kriminalitetsbekjempelse er særlig relevant i tilknytning til utvalgets mandat. Vi fokuserer derfor særlig på dette i det følgende. Av særlig interesse mht. de menneskerettslige rammene for hemmelig overvåkning og informasjonsinnhenting er EMDs avvisningsavgjørelse *Weber og Saravia mot Tyskland* av 29. juni 2006, hvor EMD vurderte tysk etterretningstjenestes myndighet til å drive såkalte strategisk overvåkning av nasjonale sikkerhetshensyn, så vel som bruk og videreformidling av informasjonen oppnådd på denne måten. Det vises også til dommen *Liberty m.fl. mot UK* av 1. juli 2008, hvor dagjeldende britisk lovgivning for overvåking av kommunikasjon ble funnet å være i strid med EMK, jf. også den senere frifinnelsesdommen *Kennedy mot UK* av 18. mai 2010. Av fremtidige avgjørelser nevnes *Big Brother Watch m.fl. mot UK* (klage nr. 58170/13 av 4. september 2013), som vil kunne kaste nærmere lys over rettstilstanden på dette området.

[1] Se f.eks. EMDs avgjørelse *Weber og Saravia mot Tyskland* (klage nr. 54934/00) av 29.6.2006.

3.2. Den europeiske menneskerettskonvensjonen art. 8 og FNs konvensjon om sivile og politiske rettigheter art. 17

Den europeiske menneskerettskonvensjonen (EMK) art. 8 og FNs konvensjon om sivile og politiske rettigheter (SP) art. 17 om rett til respekt for ens privatliv og korrespondanse er noe ulikt formulert:

EMK art. 8 lyder:

1. *Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.*
2. *Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.*

Mens SP art. 17 fastsetter at:

1. *Ingen må utsettes for vilkårlige eller ulovlige inngrep i privat- eller familieliv, hjem eller korrespondanse, eller ulovlige inngrep på ære eller omdømme.*
2. *Enhver har rett til lovens beskyttelse mot slike inngrep eller angrep.*

Praksis fra de to konvensjonenes overvåkningsorganer, henholdsvis Den europeiske menneskerettsdomstolen (EMD) og FNs menneskerettskomité, viser imidlertid at de nærmere vurderingstemaene etter de to bestemmelsene vil være sammenfallende. Vi vil derfor i det følgende forholde oss til EMK art. 8 og EMDs rettspraksis med mindre det skulle være særlig grunn til også å nevne FN-konvensjonen.

Hva utgjør et inngrep i ens privatliv eller korrespondanse?
Det følger av EMDs rettspraksis at alle typer korrespondanse vil være beskyttet av EMK art. 8, herunder e-post og andre typer elektronisk kommunikasjon, video-klipp og lydopptak og GPS-overvåkning. EMD har også lagt til grunn at ikke bare innsamling av innhold i kommunikasjon, men også av trafikkdata eller metadata (data om kommunikasjon) er et inngrep i privatlivet (se *Malone mot UK* av 2. august 1984, avsnitt 84). Videre utgjør ikke bare selve innsamlingen av kommunikasjon, men også senere lagring og bruk av personlige opplysninger et inngrep i privatlivet (se f.eks. *Leander mot Sverige* av 26. mars 1987, avsnitt 48). Deling av informasjonen som utvider gruppen med kjennskap til personlige opplysninger, utgjør et ytterligere selvstendig inngrep i privatlivet (*Weber og Saravia mot Tyskland*, avsnitt 79). Til og med selve eksistensen av lovgivning som tillater hemmelige overvåkning av kommunikasjon, kan utgjøre et inngrep i privatlivet, selv om klager selv ikke har vært overvåket (se *Weber og Saravia*, avsnitt 78 med videre henvisninger).

Ikke bare individer, men også selskaper er vernet av EMK artikkel 8, jf. EMDs dom *Societé Colas Est m.fl. mot Frankrike* av 16. april 2002. Når det gjelder hvilken type opplysninger som er beskyttet av EMK art. 8, har EMD sett hen til Europarådets personvernskonvensjons vide definisjon av personopplysninger, som er «enhver

opplysning som gjelder en bestemt eller identifiserbar enkeltperson» (se. f.eks. *Rotaru mot Romania* av 4. mai 2000 avsnitt 42-43).

Retten til privatliv er ikke absolutt

Inngrep i privatlivet kan imidlertid skje dersom det har sitt grunnlag i lov og kan anses nødvendig i et demokratisk samfunn av hensyn til et legitimt formål, jf. EMK art. 8 nr. 2. Legitime formål er iht. bestemmelsen nasjonal sikkerhet, offentlig trygghet, landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter eller friheter.

EMD fremhevet i sin første avgjørelse om hemmelig overvåkning, *Klass m.fl. mot Tyskland* av 6. september 1978, at moderne demokratiske samfunn er truet av svært sofistikerte former for spionasje og terrorisme og derfor under særlige omstendigheter må kunne være i stand til å gjennomføre hemmelig overvåkning av kommunikasjon for effektivt å bekjempe slike trusler (dommens avsnitt 48).

Inngrep må være i samsvar med loven

For at inngrep i privatlivet eller korrespondanse skal være tillatt, må det skje i samsvar med loven. Det følger av EMDs rettspraksis at dette innebærer at inngrepet må ha hjemmel i nasjonal lov som må oppfylle visse kvalitative krav. Lovgivningen må være tilstrekkelig tilgjengelig, sikre forutberegnelighet mht. under hvilke omstendigheter overvåkning kan skje, og være i tråd med rettsstatsprinsipper (jf. *Weber og Saravia* avsnitt 84).

EMD har lagt til grunn at selv om kravet om forutberegnelighet i konteksten hemmelig overvåkning selvfølgelig ikke kan bety at den overvåkede skal forhåndsinformere om overvåkningen, må lovgivningen ha klare og detaljerte regler om innsamling av kommunikasjon for å forebygge vilkårlighet. Det må herunder ikke åpnes opp for stor grad av diskresjonær myndighet for den utøvende makt eller domstolene, men trekkes opp klare rammer for skjønnsutøvelsen (se bl.a. *Malone* avsnitt 67-68 og *Weber og Saravia* avsnitt 93-94). I tillegg må et minimum av rettssikkerhetsgarantier være oppfylt for hemmelig overvåkning, jf. nærmere *Weber og Saravia* avsnitt 95:

«In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed…"

EMD har videre lagt til grunn at inngrep ikke bare må være i samsvar med nasjonal lovgivning, men også internasjonale offentligrettslige regler som staten er bundet av,

herunder folkerettens regler om staters suverenitet, jf. følgende uttalelse i *Weber og Saravia* avsnitt 87:

"The Court reiterates that the term "law" within the meaning of the Convention refers back to national law, including rules of public international law applicable in the State concerned (...). As regards allegations that a respondent State has violated international law by breaching the territorial sovereignty of a foreign State, the Court requires proof in the form of concordant inferences that the authorities of the respondent State have acted extraterritorially in a manner that is inconsistent with the sovereignty of the foreign State and therefore contrary to international law."

EMD kom i saken *Weber og Saravia* til at det ikke var bevist at den tyske lovgivningen vedrørende strategisk overvåkning, var blitt anvendt på en på en måte som kom i strid med en fremmed stats suverenitet, jf. avsnitt 88:

"The Court observes that the impugned provisions of the amended G 10 Act authorise the monitoring of international wireless telecommunications, that is, telecommunications which are not effected via fixed telephone lines but, for example, via satellite or radio relay links, and the use of data thus obtained. Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany. In the light of this, the Court finds that the applicants failed to provide proof in the form of concordant inferences that the German authorities, by enacting and applying strategic monitoring measures, have acted in a manner which interfered with the territorial sovereignty of foreign States as protected in public international law."

Inngrepet må være nødvendig i et demokratisk samfunn av hensyn til et legitimt formål

Dersom man kommer til at inngrepet er i samsvar med loven, blir spørsmålet om inngrepet også er nødvendig i et demokratisk samfunn pga. et legitimt hensyn (eller i FN-konvensjonens terminologi om inngrepet er vilkårlig).

EMDs rettspraksis viser at domstolen generelt sett har akseptert at overvåkning og informasjonsinnsamling har tilstrebet et legitimt formål, uten å dra statenes vurdering av dette i tvil. EMDs drøftelser har først og fremst dreid seg om overvåkingen og informasjonsinnhentingen kan anses «nødvendig i et demokratisk samfunn». For at inngrepet skal anses nødvendig i et demokratisk samfunn må det være *forholdsmessig* («proportional») i forhold til det legitime formålet som forfølges. Forholdsmessighetsvurderingen er en konkret skjønnsmessig vurdering hvor en rekke faktorer tas i betraktning. EMD har lagt til grunn at statene har en nokså vid skjønnsmargin når de skal foreta interesseavveiningen mellom retten til et privatliv og hensynet til å beskytte nasjonal sikkerhet. Se f.eks. avvisningsavgjørelsen *Weber og Saravia mot Tyskland* avsnitt 106 med videre henvisninger:

«[W]hen balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, it has consistently recognized that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security...».

Samtidig understreker domstolen samme sted at dette ikke betyr at statene har ubegrenset diskresjonær myndighet til å gjøre personer innen sin jurisdiksjon gjenstand for hemmelig overvåkning, og at interesseavveiningen vil avhenge av en konkret vurdering av alle sakens omstendigheter:

«Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate effective guarantees against abuse (...) . This assessment depends on all the circumstances of the case such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law...".

På grunn av at hemmelig overvåking ikke kan påklages, da den som overvåkes ikke er kjent med den, har EMD videre lagt til grunn at overvåkningen må være underlagt effektiv kontroll. Kontrollen bør normalt sett ligge til den dømmende myndighet, i alle fall i siste instans, da domstolene gir de beste garantier for uavhengighet og upartiskhet (jf. *Klass m. fl. mot Tysland* avsnitt 55-56 og *Kennedy mot UK* avsnitt 167). EMD har imidlertid lagt til grunn at fravær av rettslig kontroll ikke automatisk fører til brudd på EMK art 8. I *Klass m.fl.* fant EMD at en parlamentarisk komité med balansert politisk sammensetning og en uavhengig myndighetskommisjon som gjennomførte overvåkningen, var tilstrekkelig for å oppfylle kravet om effektiv, uavhengig og permanent kontroll. Det ble også lagt vekt på at en person som mistenkte at han var gjenstand for overvåkning, hadde klageadgang til kommisjonen, selv om denne adgangen bare forelå under særlige omstendigheter (se *Klass m. fl. mot Tyskland* avsnitt 56).

Lagring i lang tid av opplysninger innhentet gjennom overvåkning kan også anses som et uforholdsmessig inngrep, jf. *Segerstedt-Wiberg og andre mot Sverige* av 6. juni 2006. EMD kom til at oppbevaring gjennom lang tid av opplysninger om at noen hadde planlagt et bombeattentat, ikke var i strid med EMK art. 8, mens oppbevaring av informasjon vedr. deltakelse på et politisk møte i 1967 eller at en klager hadde planlagt å utøve voldelig motstand mot politiet under en demonstrasjon i 1969, ble ansett for å være uforholdsmessig, tatt i betraktning opplysningenes natur og deres alder.

Som det fremkommer foran vil videreformidling av innhentet informasjon utgjøre et selvstendig inngrep i privatlivet. Selv om selve innhentingen av informasjonen var forholdsmessig av hensyn til et legitimt formål, er det ikke dermed sagt at

videreformidling av informasjonen vil være det, enten informasjonen deles med andre nasjonale myndigheter eller med utenlandske myndigheter.

3.3. I hvilken grad kommer menneskerettighetene til anvendelse ved grenseoverskridende overvåkning og informasjonsinnhenting, jf. EMK art. 1 og SP art. 2 nr. 1?

For at en stat skal kunne holdes ansvarlig for handlinger eller unnlatelser som gir grunnlag for brudd på menneskerettskonvensjonene, er det et vilkår at staten må kunne anses å utøve jurisdiksjon, jf. EMK art. 1 og SP art. 2 nr. 1.

Hvor en stat overvåker noen som befinner seg på statens territorium, er det på det rene at staten kan bli holdt ansvarlig for menneskerettsstridige inngrep i vedkommendes privatliv, selv om dette skulle skje i form av grenseoverskridende informasjonsinnhenting. Men hvordan stiller jurisdiksjonsspørsmålet seg hvis informasjonsinnhentingen finner sted på statens territorium, men hvor den som overvåkes ikke befinner seg der (f.eks. hvor en stat henter ut opplysninger om personer i utlandet fra en fiberoptisk kabel som befinner seg på statens territorium eller i statens territorialfarvann)? Og hva hvis man fjerner seg enda lengre fra statens territorium, ved at den som er gjenstand for et inngrep i sitt privatliv ikke befinner seg på statens territorium og heller ikke statens inngrep skjer der (f.eks. hvor en stat hacker seg inn i PCen til noen i utlandet eller fanger opp vedkommendes e-post i et annet land)? I begge tilfeller har statens handling virkning utenfor statens territorium.

Spørsmålet om menneskerettighetenes ekstraterritorielle anvendelse var et vanskelig punkt under forhandlingene i 2013 og 2014 om FNs generalforsamlings resolusjon om retten til et privatliv i den digitale tidsalder, jf. nærmere nedenfor om denne. Iht. FNs konvensjon om sivile og politiske rettigheter art. 2 nr. 1 skal statene «respektere de rettigheter som anerkjennes i konvensjon, og sikre dem for alle som befinner seg på dens territorium og er undergitt dens jurisdiksjon» («within its territory and subject to its jurisdiction»). USAs offisielle holdning er at SP art. 2 nr. 1 inneholder to kumulative vilkår for jurisdiksjon, som begge må være oppfylt for at konvensjonen skal komme til anvendelse, og at menneskerettighetene derfor ikke kan komme til ekstraterritoriell anvendelse. Dette er et syn som ikke har støtte i internasjonal rettspraksis, og som Norge sammen med en rekke andre stater ikke deler. Norge er dessuten i tillegg bundet av EMK, som har en jurisdiksjonsbestemmelse som ikke refererer til territorium, bare til jurisdiksjon. Etter EMK art. 1 skal statspartene sikre enhver konvensjonens rettigheter og friheter «innen sitt myndighetsområde» («within their jurisdiction»). EMD har gitt EMK ekstraterritoriell anvendelse i en lang rekke saker under visse vilkår. Tilsvarende har FNs menneskerettskomité gjort med FNs konvensjon om sivile og politiske rettigheter. At menneskerettighetene derfor generelt sett, avhengig av de nærmere omstendighetene, *kan* komme til ekstraterritoriell anvendelse er etter vårt syn på det rene.

Også EMD har imidlertid lagt til grunn i sin rettspraksis at en stats jurisdiksjon etter EMK art. 1 først og fremst er territoriell, og at handlinger begått av en statspart som er utført på, eller som har virkninger utenfor en stats territorium, bare unntaksvis kan utgjøre utøvelse av jurisdiksjon etter EMK art. 1.[2] Om slike eksepsjonelle omstendigheter foreligger, må etter EMDs rettspraksis besluttes utfra de særlige omstendighetene i den foreliggende sak. EMD har i sin rettspraksis anerkjent en rekke slike eksepsjonelle omstendigheter som kan medføre jurisdiksjonsutøvelse utenfor en stats eget territorium.

For det første har EMD lagt til grunn at *statlige agenters utøvelse av myndighet og kontroll* («authority and control») utenfor eget territorium kan gi grunnlag for jurisdiksjon. (Se nærmere f.eks. *Al- Skeini m.fl. mot UK* av 7.7.2011 avsnitt 133-137). For det andre har EMD lagt til grunn at en stat kan ha ekstraterritoriell jurisdiksjon etter EMK art. 1 når staten utøver *effektiv kontroll over et område*. Den kontrollerende staten har i disse tilfeller ansvar for å sikre alle konvensjonsrettighetene staten er bundet av på det kontrollerte området. (Se nærmere f.eks. *Al-Skeini m.fl.* avsnitt 138-140.) FNs menneskerettskomité har lagt til grunn tilsvarende vurderingstema etter FN-konvensjonen om sivile og politiske rettigheter.[3]

EMD har så langt, så vidt vi er kjent med, ikke avsagt noen avgjørelse hvor domstolen tar uttrykkelig stilling til jurisdiksjonsspørsmålet i grenseoverskridende internettrelaterte saker eller om grenseoverskridende informasjonsinnhenting. Spørsmålet ble berørt i den ovennevnte saken *Weber and Saravia mot Tyskland* fra 2006, hvor klagerne klaget over at Tyskland hadde brutt deres konvensjonsrettigheter i forbindelse med overvåkning av telekommunikasjon fra deres telefonforbindelser i Uruguay. Tyskland argumenterte bl.a. med at «*the monitoring of telecommunications made from abroad, however, had to be qualified as an extraterritorial act. In accordance with the Court's decision in the case of Bankovic and Others v. Belgium and Others (...) the applicants therefore did not come within Germany's jurisdiction within the meaning of Article 1 of the Convention – a concept which was primarily territorial – on account of that act*". Domstolen fant det imidlertid ikke nødvendig å ta stilling til spørsmålet siden klagen uansett måtte avvises da domstolen fant at det ikke hadde funnet sted noe konvensjonsbrudd. I ovennevnte sak *Liberty m.fl. mot Storbritannia* fra 2008 ble Storbritannia domfelt for brudd på EMK art. 8 for overvåkning av samtaler mellom en britisk og to irske organisasjoner basert i henholdsvis London og Dublin. Kommunikasjonen frem og tilbake mellom Dublin og London ble fanget opp på «Capenhurst Electronic Test Facility» på britisk territorium. Det ble ikke anført av Storbritannia i saken at EMK ikke kom til anvendelse på saksforholdet for så vidt gjaldt de irske klagerne, og EMD reiste heller ikke spørsmålet av eget tiltak.

---

[2] Se f.eks. *Al- Skeini m.fl. mot UK* av 7.7.2011 avsnitt 131.

[3] Se FNs høykommissær for menneskerettigheters rapport om rett til privatliv i den digitale tidsalder av 30. juni 2014, avsnitt 32.

Hvor informasjonsinnhentingen skjer på en stats territorium, som i *Liberty m.fl.*, kan det argumenteres for jurisdiksjon på grunnlag av territorialprinsippet, selv om virkningen er ekstraterritoriell. Når det gjelder situasjoner hvor både informasjonsinnhentingen og virkningen av inngrepet i privatliv eller kommunikasjon skjer utenfor statens territorium, f.eks. hvor en stat hacker seg inn i PCen til noen eller fanger opp vedkommendes e-post i et annet land, vil det derimot være modellen med myndighet og kontroll over personer som er relevant. Samtidig kan det stilles spørsmål ved om det er noen grunn til å behandle de to situasjonene forskjellig. I begge tilfeller er virkningen av menneskerettsinngrepet ekstraterritoriell.

Det er uklart hvordan EMD vil forholde seg til kriteriene effektiv kontroll over et område eller myndighet og kontroll over personer i fremtidige saker om grenseoverskridende overvåkning og informasjonsinnhenting dersom spørsmålet kommer på spissen, evt. om domstolen kan komme til at det kan tenkes andre typer av eksepsjonelle omstendigheter som kan nødvendiggjøre og berettige ekstraterritoriell jurisdiksjon enn det som er dekket av disse to vurderingstemaene.

I denne forbindelse synes bl.a. følgende uttalelse i EMDs avgjørelse *Ben El Mahi mot Danmark* (klage nr. 5853/06) av 11.12.2006 relevant, hvor EMD begrunner de unntakene fra territorialprinsippet som domstolen har fastsatt gjennom sin rettspraksis:

"Accountability in such situations stems from the fact that Article 1 cannot be interpreted so as to allow a State Party to perpetrate violations of the Convention on the territory of another State which it would not be permitted to perpetrate on its own territory."

Hvis man skulle konkludere med at EMK art. 8 ikke kan komme til ekstraterritoriell anvendelse på overvåkning eller informasjonsinnhenting, fordi staten ikke vil kunne anses å ha effektiv kontroll over området hvor vedkommende befinner seg, eller myndighet og kontroll over vedkommende, vil en stat med relativt enkle hjelpemidler og uten å pådra seg nevneverdige kostnader kunne begå omfattende konvensjonsbrudd utenfor sine grenser som ikke vil være tillatt etter konvensjonen på statens eget territorium. Det har også blitt argumentert med at dette ville kunne åpne for samarbeid om deling av etterretningsinformasjon mellom stater med sikte på å omgå statenes menneskerettsforpliktelser overfor personer på eget territorium. Det kan derfor argumenteres for at dette, etter omstendighetene, vil kunne gi et lite tilfredsstillende resultat, og utfordrer derfor EMDs og FNs menneskerettskomites hittil utviklede rettslige vurderingstema mht. ekstraterritoriell jurisdiksjon. På den annen side kan det imidlertid også argumenteres med at innhenting av informasjon om personer som befinner seg på et statskontrollert territorium eller som på annen måte er underlagt statens myndighet og (fysiske) kontroll, lettere kan brukes, herunder misbrukes, mot vedkommende av staten, enn når det gjelder informasjonsinnhenting rettet mot personer på andre staters territorium, og at EMDs gjeldende kriterier for ekstraterritoriell jurisdiksjon derfor er relevante og ikke bør strekkes for langt.

FNs høykommissær for menneskerettigheter omtaler spørsmålet om ekstraterritoriell anvendelse av SP art. 17 i rapport om retten til et privatliv av 30. juni 2014, utarbeidet på anmodning av FNs generalforsamling i resolusjon 68/167 om samme tema (se rapportens avsnitt 32-34). I rapportens avsnitt 34 uttaler høykommissæren:

«It follows that digital surveillance (....) may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country, then human rights protection must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or violates another State's sovereignty".

FNs generalforsamling uttrykte i enstemmige resolusjoner om rett til et privatliv i den digitale tidsalder av desember 2013 og desember 2014 (res. 68/167 og res. 69/166) at den var «*deeply concerned at the negative impact that surveillance and/or interception of communication, including extraterritorial (...), may have on the exercise and enjoyment of human rights*». Men statene klarte ikke å enes om tekst som reflekterte Høykommissærens uttalelser ovenfor.

Som belyst ovenfor er det betydelig usikkerhet knyttet til jurisdiksjonsspørsmålet ved grenseoverskridende overvåkning og informasjonsinnhenting, hvor den som overvåkes ikke befinner seg på statens territorium. Det forventes imidlertid at det etter hvert vil komme rettsavgjørelser som vil kaste lys over dette spørsmålet.

Vi finner avslutningsvis grunn til å understreke at selv om EMK art. 8 skulle komme til anvendelse på overvåkning av og informasjonsinnhenting om personer i utlandet, betyr selvfølgelig ikke dette at slik informasjonsinnhenting av sikkerhetshensyn ikke vil være tillatt. Dette vil beror på en nærmere forholdsmessighetsvurdering. Det kan ikke utelukkes at denne vurderingen vil kunne slå annerledes ut dersom det er tale om innhenting av informasjon relatert til eksterne trusler.

3.4. FN-resolusjonene om retten til et privatliv i den digitale tidsalder

Vi nevner også FNs generalforsamlings to resolusjoner om retten til et privatliv i den digitale tidsalder. Resolusjonene er ikke rettslig bindende, men kan anses å reflektere visse minstestandarder. Resolusjon 68/167 av 18. desember 2013 hadde først og fremst betydning ved at den innledet en internasjonal dialog om personvern i det digitale rom. Resolusjonen ga FNs høykommissær for menneskerettigheter i mandat å utarbeide en rapport om temaet, som forelå 30. juni 2014 og finnes her: http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

Høykommissærens rapport dannet så utgangspunktet for forhandlingene om en ny resolusjon på området, nr. 69/166, vedtatt av FNs generalforsamling 18. desember 2014. Som oppfølgning av Generalforsamlingens sistnevnte resolusjon, vedtok FNs menneskerettsråd 24. mars 2015 å oppnevne en spesialrapportør for personvern.

4. Europarådets personvernkonvensjon

Europarådets konvensjon nr. 108 av 28. januar 1981 om personvern i forbindelse med elektronisk databehandling av personopplysninger ble ratifisert av Norge 20. februar 1984. Konvensjonen er så langt ratifisert av 46 stater, hvorav én ikke-Europarådsstat (Uruguay). Det er den eneste internasjonale konvensjonen som gjelder behandling av personopplysninger, herunder som søker å regulere grenseoverskridende strømmer av data.

Konvensjonens formål, nedfelt i artikkel 1, er *«å sikre respekt for enhver enkeltpersons rettigheter og grunnleggende friheter og især retten til privatlivets fred på territoriet til enhver part, uten hensyn til statsborgerskap eller bopel, i forbindelse med elektronisk databehandling av personopplysninger som vedrører ham».*

I konvensjonens forklarende rapport understrekes det at de garantier konvensjonen gir, ikke kan begrenses til statens egne borgere eller personer med lovlig opphold i staten:

«The guarantees set out in the convention are extended to every individual regardless of nationality or residence. This provision is in accordance with the general principle of the Council of Europe and its member States with regard to the protection of individual rights. Clauses restricting data protection to a State's own nationals or legally resident aliens would be incompatible with the convention."

Konvensjonen definerer personopplysninger vidt: *«enhver opplysning som gjelder en bestemt eller identifiserbar enkeltperson»*, jf. konvensjonens art. 2 bokstav a.

Ved bearbeiding av denne type opplysninger ved elektronisk databehandling, skal de iht. konvensjonens art. 5:

«a) innsamles og bearbeides på rettferdig og lovlig vis;
b) lagres for bestemte og lovlige formål og ikke nyttes på en måte som er uforenlig med disse formål;
c) være adekvate, relevante og ikke for omfattende i relasjon til de formål de lagres til;
d) være nøyaktige og, der det er nødvendig, holdt a jour;
e) oppbevares på en måte som ikke gir anledning til å identifisere datasubjektene lenger enn nødvendig for det formål som disse opplysningene lagres til.»

Konvensjonen gir enhver rett til å vite om det eksisterer et elektronisk persondataregister, dets formål og få vite om og evt. korrigert eller slettet opplysninger

som er lagret i strid med konvensjonen, samt ha klageadgang dersom disse rettighetene ikke respekteres, jf. konvensjonens art. 8.

Konvensjonens art. 6 peker på kategorier av særlig sensitive opplysninger som skal nyte et særskilt vern:

«Personopplysninger som åpenbarer rasemessig opprinnelse, politiske oppfatninger samt religiøs eller annen tro, så vel som personopplysninger vedrørende helse eller seksualliv, kan ikke behandles elektronisk med mindre intern lovgivning gir tilstrekkelig vern. Det samme skal gjelde for personopplysninger som gjelder domfellelser for straffbare handlinger.»

Det kan gjøres unntak fra konvensjonens art. 5, 6 og 8, nevnt ovenfor, når dette er fastsatt i lov og er et nødvendig tiltak i et demokratisk samfunn av hensyn til a) beskyttelse av statens sikkerhet, offentlig sikkerhet, statens økonomiske interesser eller bekjempelse av kriminelle handlinger eller b) beskyttelse av datasubjektet eller andres rettigheter og friheter. Dette er mer eller mindre sammenfallende med ordlyden i EMK art. 8 nr. 2.

5. Europarådets konvensjon nr. 185 om datakriminalitet

Europarådets konvensjonen nr. 185 om datakriminalitet (Budapestkonvensjonen) ble ratifisert av Norge 30. juni 2006. Så langt har 39 Europarådsmedlemsstater og seks ikke-medlemsstater, deriblant USA og Japan, sluttet seg til konvensjonen. Partene til Budapestkonvensjonen har forpliktet seg til gjensidig strafferettslig samarbeid i saker vedrørende datakriminalitet, herunder til å bistå hverandre med innhenting av elektroniske bevis for datakriminalitet. Vi nøyer oss med å vise til konvensjonens kapitel III om strafferettslig samarbeid som i artiklene 25-34 gir nærmere og detaljerte regler om grenseoverskridende informasjonsinnhenting for dette formål.

Med vennlig hilsen

Martin Sørby
Avdelingsdirektør

Elin Widsteen
Seniorrådgiver