UiT Norges arktiske universitet

Det juridiske fakultet

Politiets adgang til ransaking og beslag i data på utenlandske servere

Håndhevelsesjurisdiksjon i kampen mot cyberkriminalitet

Victoria Nygård

Liten masteroppgave i rettsvitenskap JUR-3902, juni 2020

Innholdsfortegnelse

1 Innledning

1.1 Temaets aktualitet og hovedproblemstilling

Tema for avhandlingen er påtalemyndighetens jurisdiksjon i forbindelse med bevisinnhenting i straffesaker. Begrepet *«jurisdiksjon»* beskriver grensene for en stats juridiske myndighet til å vedta, anvende og håndheve lovregler overfor personer.[1] Denne avhandlingen fokuserer på myndigheten til å håndheve lovgivning, heretter kalt håndhevelsesjurisdiksjon.

Internett har blitt den grunnleggende infrastrukturen i samfunnet vårt, med mengder av datanett som er knyttet sammen. Begrepene som brukes for å betegne denne sammenknytningen er *«cyber»* eller *«cyberspace»*.[2] I dag finnes det knapt et område i samfunnslivet som er fri for datateknologi. De siste tiårene har den teknologiske utviklingen gått raskere enn myndighetene har hatt evne til å følge med. Dette har medført utfordringer på flere områder, herunder nye typer kriminalitet og spørsmål om personvern og internasjonale regler.

En stor del av kriminalitetsbildet har i dag blitt flyttet fra det fysiske samfunnet til internett.[3] Måten kriminelle bruker internett på har åpnet en skjult markedsplass for kjøp og salg av blant annet narkotika, hackingtjenester, våpen, prostitusjon, menneskehandel og overgrep mot barn. Ved hjelp av internett begås det digital utpressing, ran, tyveri og underslag hver eneste dag i Norge.[4] Denne type kriminalitet refereres ofte til som *«cyberkriminalitet»*.[5]

Dagens teknologi gjør det mulig for kriminelle å opptre i det skjulte ved hjelp av krypterte nettverk, ofte referert til som *«the dark web»*.[6] Ved hjelp av avanserte programvarer forblir brukerens identitet og plassering i verden ukjent, og overvåking fra etterforskende myndigheter blir nærmest umulig.[7] Landegrenser eksisterer ikke på internett, og kriminelle opptrer følgelig uten hensyn til slike. For påtalemyndigheten er derimot den klare hovedregel at myndigheten til å håndheve lovgivning er begrenset til eget territorium.[8]

---

[1] Lowe (2007) s. 171
[2] Schjølberg (2017) s. 17
[3] Sieber & Neubert (2016) s. 243
[4] Thon (2016)
[5] Sieber & Neubert (2016) s. 242
[6] Oerlemans (2017) s. 41-42
[7] Politiet (2019) s. 14
[8] Oerlemans (2017) s. 293

Problemet med internett og landegrenser melder seg ikke bare i forbindelse med cyberkriminalitet. Også den *«vanlige»* kriminaliteten vil med dagens teknologi i stor grad innebære bevis som er lagret *«i skyen»*, herunder både bilder, videoer, samtaler i sosiale medier og e-poster.[9] Kort fortalt innebærer lagring *«i skyen»* at personer og selskaper kjøper lagringsplass på eksterne servere hos en leverandør av såkalte skytjenester, eller at de bruker programmer som sendes og lagres via slike eksterne servere.[10] Med *eksterne* servere menes her at serveren som en brukers data lagres på, er lokalisert utenfor norsk territorium. Den staten som denne serveren befinner seg i vil i det følgende omtales som *serverstaten*.

Tidligere kunne påtalemyndigheten med hjemmel i straffeprosessloven[11] enkelt skaffe seg tilgang til, ransake og beslaglegge fysiske bevis, som for eksempel våpen, mobiltelefoner eller dokumenter fra en fysisk lagringsplass, enten i papirform eller fra en lokal datamaskin som materialet direkte var lagret på. I dag er vårt forhold til data og dokumenter langt mer avansert. Det meste befinner seg i dag *«i skyen»*, og dette innebærer i all hovedsak at materialet er lagret på en server utenfor norsk territorium.[12]

I en rapport fra Europakommisjonen fremholdes det at det i så mye som 85 % av dagens straffesaker er behov for elektroniske bevis. I to tredeler av disse sakene er materialet lagret via skytjenesteleverandører basert i en annen jurisdiksjon. Tallet på antall forespørsler om grenseoverskridende tilgang til data økte med 84 % i perioden 2013 til 2018.[13]

Spørsmålet om hvor norsk påtalemyndighet kan utøve håndheving av straffeloven[14] reguleres av straffeprosessloven § 4, som fastslår at loven gjelder *«med de begrensninger ...»* som er anerkjent i folkeretten eller følger av overenskomst med fremmed stat. Ordlyden tilsier at straffeprosessloven ikke kan anvendes i strid med folkeretten.

«Folkeretten» regulerer rettsforholdet mellom stater, i form av internasjonale avtaler, også kalt konvensjoner eller traktater, eller gjennom sedvanerett.[15] Den mest grunnleggende regelen i folkeretten er suverenitetsprinsippet som fastslår at enhver stat på eget territorium

---

[9] Sieber & Neubert (2016) s. 243
[10] Smith & Browne (2019) s. xiv
[11] Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker
[12] Sieber & Neubert (2016) s. 243
[13] Europakommisjonen (05.02.2019) s. 1
[14] Lov 20. mai 2005 nr. 28 om straff
[15] FN-sambandet (2019)

har fullt rådvelde både med tanke på lovgivning og håndhevelse.[16] At strafferettslige bevis befinner seg utenfor norsk territorium, innebærer derfor også at de som hovedregel befinner seg utenfor norsk håndhevelsesjurisdiksjon. Konsekvensene av dette er i dag tema for diskusjon blant jurister internasjonalt.[17]

I takt med digitaliseringen av samfunnet har disse folkerettslige spørsmålene vokst i aktualitet. Det er knyttet stor usikkerhet til hvilken plass internett og digitalt materiale skal ha i tilknytning til landegrenser og jurisdiksjon.[18] Spørsmålene er bare i begrenset grad regulert i traktater. Når det gjelder avgjørelser fra internasjonale domstoler finnes det noen, men disse er i all hovedsak knyttet til menneskerettslige problemstillinger som ikke vil berøres i denne avhandlingen.[19] Det er gjennomført internasjonale studier for å klarlegge problemet og finne forslag til løsninger.[20] Noen land har også vedtatt egne nasjonale lover i forsøk på å håndtere jurisdiksjonsproblemet på best mulig måte inntil en internasjonal konsensus er funnet.[21]

For norsk retts vedkommende er jurisdiksjonsspørsmålet i dag særlig aktuelt. I motsetning til mange andre stater har ikke Norge vedtatt noen lovbestemmelser som tar stilling til jurisdiksjonsproblemet ved bevisinnhenting fra servere i utlandet. Når slik bevisinnhenting til tross for uklare internasjonale regler gjennomføres, reises viktige spørsmål i tilknytning til serverstatens suverenitet. Et slikt bevisinnhentingstilfelle ble nylig bragt inn for Høyesterett.

Høyesterett behandlet i HR-2019-610-A (heretter *Tidal-saken* eller *Tidal-kjennelsen*) begjæring om ransaking hos et selskap for å få tilgang til data som selskapet hadde lagret på servere i utlandet. Høyesterett konkluderte med at beslaget ikke var en krenkelse av noen stats suverenitet. Det kan stilles spørsmål ved Høyesteretts premisser i forhold til folkeretten. Tidal-kjennelsen er per dags dato én av få autoritative norske rettskilder som berører jurisdiksjonsspørsmålet. Det finnes utover dette heller ikke mye norsk litteratur som foretar en dybdeanalyse av temaet basert på folkerettslige kilder. Problemstillingen er løftet frem av Jon Petter Rui i kjølvannet av Tidal-saken, i artikkelen «Høyesterett i skyen» i Lov og Rett nr. 5

[16] FN-sambandet (2019), Ruud & Ulfstein (2018) s. 198
[17] Om dette i avhandlingens kapittel 8 nedenfor
[18] Lysneutvalget (2015) s. 2
[19] Ibid.
[20] Se avhandlingens kapittel 7.9
[21] Se avhandlingens kapittel 7.3-7.8

(2019) hvor han presenterer sitt synspunkt. Det finnes også et svar på denne i Lov og Rett nr. 10 (2019) av Jørgen S. Skjold som har inntatt motsatt standpunkt.

Formålet med avhandlingen er å undersøke hvilken adgang etterforskende myndigheter har til å foreta ransaking og beslag i digitalt bevismateriale som er lagret i utlandet. Avhandlingens hovedproblemstilling er hvorvidt Høyesteretts kjennelse i Tidal-saken er i samsvar med folkeretten.

1.2 Metode og rettskilder

1.2.1 Avhandlingens metode

Masteroppgaven har et folkerettslig tema. For å belyse problemstillingen vil det være nødvendig å analysere de folkerettslige kilder som berører spørsmålet. En slik analyse foretas ved hjelp av folkerettslig metode. Videre vil det være hensiktsmessig å se hen til utenlandsk rett for å se hvordan andre land nasjonalt har håndtert problemet. Dette vil til slutt sammenlignes med norsk rett og Tidal-saken. En slik sammenligning gjøres ved hjelp av komparative metoder.

1.2.2 Folkerettslig metode

«Folkerett» er av Castberg definert som *«den del av retten som regulerer rettsforholdene mellom stater, i deres egenskap av sådanne»*.[22] *«I deres egenskap av sådanne»* sikter til det faktum at det i folkeretten ikke finnes noen overordnet lovgivningsmyndighet slik vi kjenner til i nasjonal rett.[23] Statene er bare bundet til de avtaler de selv har inngått og således akseptert som bindende for seg. [24] Et unntak fra dette er visse sedvanerettsregler, kalt *jus cogens*, som anses som så grunnleggende at de regnes for å utgjøre en tvingende norm innen folkeretten som er bindende for alle stater.[25]

1.2.3 Rettskilder i folkeretten

Statuttene for Den internasjonale domstol (heretter ICJ)[26] artikkel 38 lister opp relevante rettskilder ved løsning av folkerettslige spørsmål. Bestemmelsen er formelt bare bindende for rettsanvendelsen til domstolen, men den blir ansett for å gi et alminnelig uttrykk for

[22] Castberg (1948) s. 1, Ruud & Ulfstein (2018) s. 18
[23] Ruud & Ulfstein (2018) s. 22
[24] Ibid.
[25] Ibid. s. 73
[26] ICJ-statuttene (1945)

rettskildelæren i folkeretten.[27] Rekkefølgen i artikkelen innebærer ikke et hierarkisk forhold mellom rettskildene, og oppregningen er heller ikke uttømmende.[28]

ICJ-statuttene artikkel 38 fastsetter følgende:

> *«The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:*
> *a. international conventions, whether general or particular, establishing rules expressly recognized by the contesting States;*
> *b. international custom, as evidence of a general practice accepted as law;*
> *c. the general principles of law recognized by civilized nations;*
> *d. subject to the provisions of Article 59, judicial decisions and the teachings of the most highly publicists of the various nations, as subsidiary means for the determination of rules of law.»*

I tråd med bokstav a til c vil det i den folkerettslige analysen tas utgangspunkt i konvensjoner, sedvanerett og alminnelige rettsprinsipper som primære rettskilder. Subsidiært, der disse ikke gir tilstrekkelig svar, vil det sees hen til folkerettslig litteratur, jf. bokstav d.

1.2.4 Tolkning av folkerettslige forpliktelser

Ved tolkningen av konvensjonsforpliktelser er det naturlig å ta utgangspunkt i tolkningsprinsippene i Wien-konvensjonen om traktatretten.[29] Norge har ikke sluttet seg til konvensjonen, men den anses i stor grad å uttrykke folkerettslig sedvanerett.[30] Hovedbestemmelsen om traktattolking fremgår av artikkel 31 første ledd som lyder:

> *«A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose. »*

Dette innebærer at det skal tas utgangspunkt i traktatens ordlyd, og at den skal tolkes i lys av traktatens gjenstand og formål. Det skal søkes etter *«the ordinary meaning»* av ordlyden, og dette skal gjøres i *«good faith»*. Traktattolking bygger med andre ord på det grunnleggende

---

[27] Ruud & Ulfstein (2018) s. 71
[28] Ibid. s. 72-73
[29] Wien-konvensjonen (1969)
[30] Ruud & Ulfstein (2018) s. 86

prinsippet om at avtaler skal holdes, og den lojalitetsplikt dette innebærer. [31] En skal velge det tolkningsresultat som stemmer best overens med partenes felles intensjoner.[32]

1.2.5 Komparativ metode

Sammenlignende studier av norsk og utenlandsk rett kalles komparasjon.[33] Det finnes flere ulike komparative metoder. Jon Petter Rui redegjør i sin artikkel «Komparasjon innen strafferett og -prosess» for den struktursammenlignende metode, som går ut på å ta utgangspunkt i et faktisk problem og avklare hvordan ulike rettssystemer eller deler av rettssystemene forholder seg til problemet.[34] Det er en slik metode som vil ligge til grunn for sammenligningen i denne avhandlingen.

En fare ved komparative studier er at man ofte ikke er godt nok kjent med språket og den juridiske metoden i det fremmede rettssystemet til å kunne klarlegge rettsreglenes korrekte innhold eller funksjon.[35] Jon Petter Rui mener i denne sammenheng at det i mange tilfeller ikke er nødvendig å bygge fremstillingen på det fremmede rettssystemets primærkilder.[36] I de aller fleste tilfeller vil en grundig studie av juridisk litteratur i det fremmede rettssystemet være den beste fremgangsmåten for på trygt grunnlag å kunne fastslå hva som er gjeldende rett.[37] Dette synspunktet legges også til grunn for denne avhandlingen.

Det faktiske problemet det her tas utgangspunkt i er mangelen på klare, norske rettsregler vedrørende adgangen til å innhente bevis i tilfeller som det som lå til grunn for Tidal-saken. For å belyse dette vil det gjøres en undersøkelse av nederlandsk, belgisk, portugisisk, engelsk og amerikansk rett, samt det pågående lovarbeidet i EU.[38]

Når gjeldende rett i de nevnte rettssystemene er fastslått, vil det foretas en sammenligning der dette holdes opp mot norsk rett i lys av Tidal-saken.[39] Formålet er å identifisere likheter og forskjeller, samt å undersøke hvorfor det finnes slike.[40]

---

[31] Ruud & Ulfstein (2018) s. 95
[32] Ibid.
[33] Rui (2009) s. 434
[34] Ibid. s. 455
[35] Ibid. s. 451-454
[36] Ibid. s. 460
[37] Ibid. s. 461
[38] Se avhandlingens kapittel 7.3-7.8
[39] Se avhandlingens kapittel 9
[40] Rui (2009) s. 463

1.3 Videre fremstilling

Høyesteretts begrunnelse i Tidal-saken reiser flere spørsmål når den holdes opp mot folkerettslige kilder. Før det gås i dybden på analysen av disse spørsmålene, vil det være nødvendig å gi en presentasjon av fenomenet det her er tale om å vurdere opp mot folkeretten. Den videre fremstillingen vil derfor innledes med at det i kapittel 2 gis en redegjørelse for hva en server er, hva det innebærer at noe er lagret *«i skyen»*, og hva det vil si å ransake en server. Formålet er å gi leseren en forståelse av hvordan teknologien fungerer, og for hvordan den har betydning i det juridiske bildet. Deretter skal det i kapittel 3 gjøres rede for Tidal-sakens faktum, konklusjon og premisser.

Svaret på avhandlingens hovedproblemstilling beror på rekkevidden av det folkerettslige suverenitetsprinsippet. Det vil derfor være nødvendig med en alminnelig redegjørelse av suverenitetsprinsippet i kapittel 4. Det vil herunder bli gitt noen eksempler på tilfeller av suverenitetskrenkelse for å få satt situasjonen med serverransaking i et juridisk perspektiv.

I kapittel 5 begynner selve rettskildeanalysen. Det vil her tas utgangspunkt i de folkerettslige kilder som er presentert ovenfor i kapittel 1.2.3. I kapittel 5 undersøkes således traktatretten, med påfølgende undersøkelser av folkerettslig rettspraksis, sedvanerett og litteratur i kapitlene 6 til 8. På bakgrunn av disse er målet å danne et bilde av hvordan den internasjonale holdningen til problemet er i dag.

I kapittel 9 vil disse funnene holdes opp mot norsk rett i lys av Tidal-saken. Her vil det gis en konklusjon på avhandlingens hovedproblemstilling, sies noe om konsekvensene av uhjemlet serverransaking, samt knyttes noen bemerkninger *de lege ferenda* til dette.

2 Serverransaking – fenomenet

2.1 «Server»

Begrepet *«server»* kan defineres som *«store felles datamaskiner som har som mål å lagre, finne, prosessere og presentere store mengder data for hundrevis hvis ikke tusenvis av brukere»*.[41] En server har med andre ord som oppgave å levere tjenester til klienter som er

[41] Sander (2019)

koblet til den via et nettverk. En *«klient»* kan være en datamaskin, smarttelefon eller et program beregnet på å motta tjenester fra en bestemt type serverprogram.[42]

Internett kan på mange måter sammenlignes med et stort veinett. Alt fra smale veier (telelinjer) til de bredeste motorveier (høyhastighetslinjer). Langs veiene finner man privatpersoner, organisasjoner og bedrifter som tilbyr tjenester til de veifarende. Man kan for eksempel stoppe opp og lese informasjon, se på bilder og videoer, sende og motta meldinger, foreta banktjenester og hente post. Som reisende på internett bruker man en datamaskin med forskjellige programvarer som gjør det mulig å benytte de forskjellige tjenestene som tilbys. Programvaren på datamaskinen kalles *«klient»*, mens programvaren hos tjenesteyteren kalles *«tjener»* eller *«server»*. [43]

Det kan grovt sett skilles mellom to typer servere. Den første er applikasjonsservere som er satt opp for å levere en bestemt applikasjon (program) til brukeren, for eksempel Gmail, Facebook, Messenger, Snapchat, Instagram eller WhatsApp.[44] Den andre typen er filservere som er satt opp for å lagre og distribuere filer av ulike typer til brukerne i nettverket, for eksempel brukerens dokumenter, bilder og videofiler.[45]

2.2 Skyrevolusjonen som konsekvens for etterforskingen

Digitaliseringen av samfunnet har ført til at vi i stadig økende grad benytter oss av tjenester på internett, fremfor i den fysiske verden.[46] I motsetning til tidligere får vi i dag posten vår på e-post og ikke i postkassen, vi fører i stor grad samtaler gjennom sosiale medier fremfor å ringe eller møte personer fysisk, vi betaler regninger i nettbanken istedenfor i den fysiske banken, og vi deler bilder og videoer via sosiale medier i stedet for å vise noen det ved fysisk møte.

Alle disse applikasjonene og tjenestene som vi benytter oss av i det daglige har en viktig ting til felles; de foregår via internett og er knyttet til store, eksterne servere der alle brukernes post, bilder, videoer og samtaler lagres.[47] En brukers data ligger således ikke lagret lokalt på dennes smarttelefon, nettbrett eller datamaskin. Informasjonen kan nås uansett hvor

[42] Liseter (2019)
[43] Bertheussen (2000) s. 15
[44] Sander (2019)
[45] Ibid.
[46] Smith & Browne (2019) s. 94
[47] Sander (2019)

vedkommende befinner seg i verden, så lenge man innehar nødvendig innloggingsinformasjon.[48] Det er dette fenomenet som refereres til som *«skyen»*.[49]

Hver gang vi sjekker noe på smarttelefonen, nettbrettet eller datamaskinen vår, om det så er e-post, sosiale medier eller nettbanken, så hentes informasjonen ut fra en server plassert i et stort datasenter.[50] Et datasenter er store bygninger eller samlinger av bygninger, som er hjemmet til flere hundre tusener av servere. Det er disse serverne som lagrer alle våre data.[51] Lagring og prosessering av data er altså ikke noe som foregår *«i skyen»* som navnet tilsier. Handlingene vi gjør skjer alltid via en spesifikk fysisk server i et datasenter som befinner seg på et spesifikt territorium.[52]

Et fenomen som har vokst sterkt frem i løpet av det siste tiåret er bruken av såkalte *«skytjenester»*. Skytjenester er en samlebetegnelse på alt fra prosessering av data og lagring, til programvarer som er tilgjengelig fra eksterne filservere tilknyttet internett.[53] Enklere forklart innebærer dette at en rekke selskaper, herunder Microsoft, Apple og Google tilbyr seg å ta vare på det du måtte ha av data som du trenger å oppbevare, slik at du slipper å lagre det lokalt på din datamaskin, nettbrett eller smarttelefon. På denne måten er dataene lagret og tilgjengelig selv om du skulle miste datamaskinen, nettbrettet eller mobiltelefonen din, eller dersom du er på reise og har glemt disse hjemme. Noen av de mest kjente tjenestene er iCloud, Microsoft OneDrive, DropBox og Google Drive.[54]

Filer og applikasjonsdata lagres som regel ikke bare i ett datasenter. Et selskap har ofte flere datasentre, gjerne i forskjellige land.[55] Dataene lagres ofte som speilkopi på servere på flere datasentre samtidig, for å hindre tap hvis noe skulle skje med et av sentrene, og de flyttes også mellom sentrene etter faste algoritmer.[56] Dette innebærer at en brukers data kan være lagret i flere ulike stater samtidig, eller skifte lagringsplass fra én stat til en annen på bare et millisekund.[57] Det kan også hende at plasseringen av dataene ikke er mulig å spore opp.[58]

---

[48] Koops & Goodwin (2014) s. 22
[49] Oerlemans (2017) s. 51, Smith & Browne (2019) s. xiv
[50] Smith & Browne (2019) s. xiv, Oerlemans (2017) s. 51
[51] Smith & Browne (2019) s. xv
[52] Sieber & Neubert (2016) s. 255
[53] Datatilsynet (2018)
[54] Singsaas (2016)
[55] Smith & Browne (2019) s. xviii
[56] Koops & Goodwin (2014) s. 22
[57] Sieber & Neubert (2016) s. 246-247
[58] Ibid.

Uansett hvor dataene måtte befinne seg, er de imidlertid alltid lagret på en fysisk server som er plassert fysisk på en stats territorium.[59] Skyleverandørene og eierne av applikasjonene vi bruker mest, er som regel store, utenlandske selskaper, og datasentrene befinner seg derfor også i all hovedsak utenfor norsk territorium.[60]

2.3 «Serverransaking»

At en så stor del av vårt dagligliv i dag foregår *«i skyen»*, innebærer at også en stor del av bevisbildet i straffesaker er flyttet til *«skyen»*.[61] Når politiet i sin etterforskning av straffesaker søker etter gjenstander eller opplysninger som kan tjene som bevis i saken, tas det ofte i bruk tvangsmidler for å spore opp og sikre disse.

Tvangsmidler er i norsk rett regulert i straffeprosesslovens fjerde del og defineres i lovforarbeidene som *«et foreløpig skritt i etterforskingen som kan ha til formål å sikre bevis, men som også kan ha andre formål: først og fremst å hindre gjentakelse eller å sikre at gjerningspersonen ikke unndrar seg straff»*.[62] Med andre ord kan tvangsmidler anses som en fellesbetegnelse på noen av de etterforskningsmetoder politiet bruker i sin straffesaksbehandling. En naturlig forståelse av begrepet *«tvangsmiddel»* tilsier videre at det er tale om metoder som kan gjennomføres mot siktedes vilje.

Som eksempler på tvangsmidler kan nevnes ransaking etter straffeprosessloven kapittel 15 og beslag etter kapittel 16. Med ransaking menes *«en undersøkelse politiet foretar for å lete etter bevis for en straffbar handling eller etter ting som kan beslaglegges, eller som det kan tas heftelse i»*.[63] Straffeprosessloven § 203 første ledd fastslår at *«ting som antas å ha betydning som bevis, kan beslaglegges inntil rettskraftig dom foreligger i saken»*. Ordlyden tilsier at gjenstander som kan inneholde opplysninger av betydning i en straffesak, kan inndras fra eieren og beholdes i politiets besittelse inntil saken er avgjort.

Serverransaking er etter dette når politiet fra siktedes datamaskin, smarttelefon eller nettbrett, eller ved hjelp av siktedes innloggingsinformasjon til et nettsted, foretar undersøkelser på serveren som informasjonen er lagret på, med det formål å lete etter bevis for en straffbar handling eller etter informasjon som kan beslaglegges. Politiet skaffer seg med andre ord

[59] Sieber & Neubert (2016) s. 255
[60] Ibid. s. 252
[61] Ibid. s. 243
[62] Ot.prp. nr. 64 (1998-1999) s. 16
[63] Fredriksen (2018) s. 196

tilgang til materiale som (ofte) er lagret på en server lokalisert i utlandet, via en datamaskin, et nettbrett eller en mobiltelefon i Norge. Det er nettopp dette fenomenet som reiser spørsmål i relasjon til folkeretten.

3 Kjennelsen i HR-2019-610-A (Tidal Music AS)

Den 28. mars 2019 avsa Høyesterett kjennelse i en sak mellom Økokrim og Tidal Music AS. Økokrim hadde i forbindelse med etterforskning av et mulig databedrageri begjært tredjemannsransaking hos Tidal Music AS, jf. strpl. § 192 tredje ledd nr. 3, for å få tilgang til datamateriale som selskapet hadde lagret på servere i utlandet.

Tredjemannsransaking er etter straffeprosessloven § 192 tredje ledd ransaking *«hos andre»*. Ordlyden tilsier at det i noen tilfeller kan foretas ransaking hos andre enn siktede selv. For eksempel kan dette være en arbeidsgiver eller venn av siktede, som selv anses uskyldig. Dette kan blant annet være aktuelt dersom det er særlig grunn til å anta at *«det der kan finnes bevis eller ting som kan beslaglegges ...»* Det var dette alternativet som var aktuelt i Tidal-saken.

Spørsmålet for Høyesterett var om Økokrim fra dataterminaler i Tidals kontorlokaler i Oslo kunne laste ned elektronisk materiale som selskapet hadde lagret i utlandet, eller om slik ransaking falt utenfor norske myndigheters jurisdiksjon.

Tidal Music AS anførte at ransakingen har virkning på et territorium hvor andre stater har eksklusiv tvangsmyndighet. Økokrim anførte at tvangsbruken ikke kunne være noe inngrep i en annen stats suverenitet idet politiet hadde lovlig tilgang til selskapets datasystemer fra dets kontorlokaler i Norge, og politiet bare var til stede på norsk territorium.

Høyesterett konkluderte med at beslaget ikke var en krenkelse av noen stats suverenitet, selv om materialet var lagret på servere lokalisert på fremmed territorium.[64] Det avgjørende for Høyesterett var at *«materialet gjøres tilgjengelig gjennom bruk av tvangsmidler overfor et norsk selskap med kontor i Norge»*, og at det ikke var snakk om at *«norske myndigheter på egenhånd trenger seg inn i materiale som ligger lagret i utlandet».*[65] Videre la Høyesterett vekt på at ransakingen bare ville gi tilgang til materiale som selskapet selv disponerte via den

[64] Kjennelsens avsnitt 71-72
[65] Kjennelsens avsnitt 67

utenlandske serveren og at materialet fortsatt ville være uendret og i behold på den utenlandske serveren etter beslaget.[66]

I sin rettskildeanalyse undersøkte førstvoterende først traktatretten, nærmere bestemt Cybercrime-konvensjonen. Det ble vist til at konvensjonen *«pålegger statene å iverksette nærmere angitte tiltak for å bekjempe datakriminalitet ...»*, men at *«ingen av konvensjonsbestemmelsene angår direkte et tilfelle som i saken her ...».*[67] Førstvoterende valgte derfor å ikke gå nærmere inn på konvensjonen.

Videre undersøkte førstvoterende det folkerettslige suverenitetsprinsippet, og uttalte:

> *«Det klare folkerettslige utgangspunktet er at statene bare kan utøve tvang på eget territorium. Tvangsjurisdiksjonen er eksklusiv; ingen stat kan anvende tvangsmidler på en annen stats territorium uten samtykke fra vedkommende stat. Norsk lovgivning er basert på dette. Det er eksempelvis på det rene at norsk politi og påtalemyndighet ikke kan foreta pågripelser utenlands eller ransake et hus i et annet land. I slike tilfeller er rettshåndhevende myndigheter avhengig av bistand fra – eller avtaler med – andre land.»*[68]

Førstvoterende uttalte deretter at *«disse alminnelige utgangspunktene»* gir mindre veiledning når det gjelder ransaking og beslag av elektronisk lagret materiale som kan lagres *«i skyen»*.[69] Det ble vist til at det kan være nokså tilfeldig hvilken server en norsk brukers data lagres på, og til at lagringsstedet over tid kan endres uten at brukeren blir informert om det eller kan kontrollere det. Førstvoterende konkluderte med at

> *«[d]e rettslige spørsmål som den teknologiske utviklingen aktualiserer ved bruk av tvangsmidler rettet mot lagringssteder «i skyen» er lite avklart, både i norsk rett og internasjonalt»*.[70]

Videre undersøkte førstvoterende norsk praksis, og konstaterte at det ikke finnes noen avgjørelser fra Høyesterett som belyser grensen for norsk tvangsjurisdiksjon i et tilfelle som

---

[66] Kjennelsens avsnitt 69-70
[67] Kjennelsens avsnitt 36
[68] Kjennelsens avsnitt 40
[69] Kjennelsens avsnitt 41
[70] Kjennelsens avsnitt 42

dette. Det ble vist til NOU 1997:15 punkt 4.2.1.3 hvor det er lagt til grunn at *«det dreier seg om ransaking i Norge når tilgang til dataene oppnås fra en terminal som befinner seg i Norge»*. Etter metodeutvalgets oppfatning må det kunne undersøkes *«hvilke data som er tilgjengelig på den aktuelle terminal, uavhengig av om opplysningen er lagret i utlandet»*.[71] Førstvoterende fastslo at norsk praksis også på andre områder bygger på den samme tankegangen, for eksempel ved at kommunikasjonskontroll kan gjennomføres selv om den ene samtalepartneren viser seg å være i et annet land.[72]

Endelig undersøkte førstvoterende praksis fra andre land. Det ble for det første vist til svensk og dansk praksis, som har forskjellige synspunkter. Dansk Høyesterett tillot innhenting av opplysninger lagret på servere i utlandet, mens svensk rett bygde på at territorialprinsippet hindret politiet i å gå inn på internettbaserte kommunikasjons- eller lagringstjenester dersom leverandørens servere befinner seg utenfor Sverige.[73]

Når det gjaldt øvrige europeiske land nøyde førstvoterende seg med å vise til rapporter fra ekspertgrupper i Europarådet og EU-kommisjonen. Disse viste at *«det ikke er uvanlig at stater mener seg berettiget til å foreta en slik ransaking som i saken her, også om det er klart at materialet er lagret på en utenlandsk server.»*[74]

På bakgrunn av gjennomgangen av praksis konkluderte førstvoterende med at det ikke var etablert noen folkerettslig sedvane på området, og uttalte:

> *«Likevel er det av interesse at mange land i praksis synes å godta en slik ransaking som i saken her. Det er heller ikke opplyst noe om mellomstatlige reaksjoner knyttet til at et lands myndigheter gjennom tvangsmidler overfor rettssubjekter på eget territorium har fått tilgang til materiale lagret i en annen stat.»*[75]

Siden det verken fantes noen internasjonal konsensus, konvensjonsbestemmelser eller rettspraksis som kunne tjene til veiledning måtte Høyesterett på selvstendig grunnlag ta stilling til om bruk av tvangsmidler krenker en annen stats suverenitet. Førstvoterende tok

[71] Kjennelsens avsnitt 45
[72] Kjennelsens avsnitt 46
[73] Kjennelsens avsnitt 50-51
[74] Kjennelsens avsnitt 53
[75] Kjennelsens avsnitt 59

utgangspunkt i en overordnet vurdering av om den aktuelle ransakingen grep inn i en annen stats eksklusive tvangsjurisdiksjon på en slik måte at denne statens suverenitet ble krenket.[76]

Det kan stilles spørsmål ved Høyesteretts premisser for kjennelsen. Noen av de mest sentrale rettskildene Høyesterett er inne på, undersøkes kun overfladisk. Det finnes i tillegg flere relevante rettskilder som kan belyse andre sider ved spørsmålet som Høyesterett ikke eller bare i liten grad berører.

4 Allment om suverenitetsprinsippet

4.1 Håndhevelsesjurisdiksjon er territorielt begrenset

Suverenitetsprinsippet er det mest grunnleggende prinsippet i folkeretten.[77] Med *«prinsipp»* menes rettslige normer med høyt generalitetsnivå. Et *«grunnleggende»* prinsipp utgjør det rettslige utgangspunktet som de positive lovbestemmelsene på et felt bygger på, eller bygger videre på. Tilføyes ordet *«overordnet»* siktes det til at prinsippet har særlig stor vekt som rettslig argument.[78] Suverenitetsprinsippet er et slikt overordnet prinsipp.[79]

Suverenitetsprinsippet går ut på at alle stater er suverene og ikke underkastet noen annen vilje enn sin egen.[80] Prinsippet forklarer hvorfor folkeretten blir skapt og håndhevd av stater, og hvorfor statene står fritt til å velge hvilke avtaler de vil slutte seg til.[81] Som en naturlig følge av dette gjelder et allmenngyldig forbud mot å intervenere i andre staters interne anliggender. Dette intervensjonsforbudet anses i dag som en *jus cogens*-regel innen folkeretten.[82] «*Jus cogens*» er betegnelsen på regler som anses ufravikelig. Sedvanerett er normalt fravikelig og kan fravikes ved avtale. Jus cogens-regler kan stater derimot ikke avtale seg bort ifra.[83] Eksistensen av jus cogens-regler og det faktum at de er ufravikelig, er forutsatt i Wien-konvensjonen om traktatretten artikkel 53 og 64, som fastslår at en traktat som fraviker en *jus cogens*-regel er ugyldig.[84]

---

[76] Kjennelsens avsnitt 61 flg.
[77] FN-sambandet (2019), Ruud & Ulfstein (2018) s. 198
[78] Kjelby (2019) s. 115 med videre henvisninger, FN-sambandet (2019)
[79] FN-sambandet (2019)
[80] Ruud & Ulfstein (2018) s. 21
[81] FN-sambandet (2019)
[82] Ruud & Ulfstein (2018) s. 72 og s. 198, Cassese (2005) s. 202
[83] Ruud & Ulfstein (2018) s. 73
[84] Wien-konvensjonen (1969)

Den viktigste konsekvensen av suverenitetsprinsippet er territoriell integritet. Det vil si at enhver stat på eget territorium har fullt rådvelde, både med tanke på lovgivning og håndhevelse. Fordi suverenitet innebærer frihet til å styre innenfor egne grenser, innebærer det også en tilsvarende rett til å ekskludere andre aktører fra sitt territorium.[85] I hvilken grad stater kan utøve jurisdiksjon over aktiviteter på andre staters territorium stiller seg forskjellig for håndhevelsesjurisdiksjon og andre former for jurisdiksjon. Utøvelse av tvang, herunder håndhevelse av lovregler, på andre staters territorium er utelukket, med mindre det foreligger samtykke fra den annen stat.[86] Stater har derimot adgang til å gjøre lovgivningen sin gjeldende for handlinger foretatt i utlandet, men må da avvente håndheving til overtrederen befinner seg på statens eget territorium eller til samtykke foreligger.[87]

Hva som ligger i territoriell integritet er nærmere presisert av ICJ i Lotus-saken (Frankrike mot Tyrkia).[88] Saken gjaldt spørsmål om håndhevelsesjurisdiksjon etter en kollisjon mellom det franske fartøyet Lotus som var på vei til Konstantinopel (i dag Istanbul)[89] og det tyrkiske fartøyet Boz-Kourt. Kollisjonen skjedde i internasjonalt farvann og åtte tyrkiske statsborgere omkom. Da Lotus senere ankom Konstantinopel innledet tyrkiske myndigheter straffeforfølgelse mot kapteinen på Lotus som senere endte i domfellelse for uaktsomt drap. Spørsmålet for ICJ var om Tyrkia hadde opptrådt i strid med folkeretten, noe flertallet svarte benektende på. Flertallet mente at en kollisjon med et tyrkisk skip måtte anses for å tilsvare en skade på tyrkisk territorium, og dermed gi grunnlag for jurisdiksjon.[90] I sin beskrivelse av territoriell suverenitet uttalte domstolen følgende:

> *"The first and foremost restriction imposed by international law upon a State is that – failing existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention."*[91]

[85] Skodvin (2014)
[86] Ruud & Ulfstein (2018) s. 147
[87] Ibid.
[88] France v. Turkey (1927)
[89] Durovic-Andic (2019)
[90] Ruud & Ulfstein (2018) s. 148
[91] France v. Turkey (1927) s. 18

Dette er i dag det anerkjente utgangspunktet i folkeretten hva gjelder grenseoverskridende etterforskninger. Dette innebærer at etterforskende myndigheter ikke kan etterforske på fremmed territorium uten hjemmel i avtale, enten stående eller ad hoc.[92]

4.2 Suverenitetskrenkelse

Spørsmålet i denne avhandlingen er i hvilken grad suverenitetsprinsippet begrenser adgangen til å gjennomføre ransaking og beslag på servere plassert utenfor norsk territorium. Det er med andre ord et spørsmål om suverenitetsprinsippets rekkevidde. Som Høyesterett konstaterte i Tidal-saken, er spørsmålet uavklart autoritativt, både i nasjonal og internasjonal rett. En hensiktsmessig måte å tilnærme seg spørsmålet på, er først å klarlegge noen sikre eksempler på suverenitetskrenkende håndhevelseshandlinger for slik å få plassert problemet i et juridisk perspektiv.

Uhjemlet fysisk tilstedeværelse på en annen stats territorium vil i de fleste tilfeller være tilstrekkelig til å konkludere med at håndhevelseshandlingen foregår utenfor den håndhevende statens jurisdiksjon.[93] Dette innebærer at det vil kunne konstateres suverenitetskrenkelse dersom håndhevende myndigheter fra stat A uten særskilt hjemmel reiser til stat B og foretar ransaking eller pågripelse på dennes territorium. Slike handlinger ligger i kjernen av intervensjonsforbudet.[94] På den annen side kan en ikke utelukke suverenitetskrenkelse alene av den grunn at myndighetspersoner fra stat A ikke fysisk befinner seg på stat Bs territorium. En slik konklusjon vil overse problemet med ny teknologi og digital bevisinnhenting.

Stater er avskåret fra å håndheve sin lovgivning på andre staters territorium uten særskilt hjemmel, og retten til å utøve tvang hører til kjernen av territorialhøyheten.[95] Utøving av tvangsmidler må derfor anses fullstendig utelukket uten samtykke og må således anses som en krenkelse av suverenitetsprinsippet dersom det gjøres uhjemlet.

At bruk av tvangsmidler er utelukket i fravær av en hjemmel innebærer at det også vil foreligge en suverenitetskrenkelse i tilfeller hvor myndighetene i stat A får en person i stat B til å sette opp kameraovervåking eller avlyttingsutstyr på en adresse i stat B. Her har ikke

[92] Ruud & Ulfstein (2018) s.199, Crawford (2012) s. 478-479, Oerlemans (2017) s. 57, Sieber & Neubert (2016) s. 253, Koops & Goodwin (2014) s. 19
[93] Sieber & Neubert (2016) s. 255, Skjold (2019) s. 622
[94] Ruud & Ulfstein (2018) s. 145, Crawford (2012) s. 479
[95] Ruud & Ulfstein (2018) s. 145

myndighetspersoner fra stat A hatt noen fysisk tilknytning til stat Bs territorium, men det er likevel ikke tvilsomt at handlingen er ulovlig.

Like åpenbar er ikke situasjonen med grenseoverskridende datatilgang. Spørsmålet er som Høyesterett påpekte i Tidal-saken lite avklart, både i norsk rett og internasjonalt.[96] Det kan derfor ikke gis noen sikre utgangspunkter for hva som vil måtte anses som en suverenitetskrenkelse i slike tilfeller, men det kan derimot gis eksempler på tilfeller av digital bevisinnhenting som ganske sikkert *ikke* vil innebære noen suverenitetskrenkelse.

Et tilfelle hvor det ikke kan sies å eksistere noen territoriell kobling mellom etterforskingen av en straffesak og fremmed stats territorium, er der etterforskingen utelukkende skjer utenfor en fremmed stat.[97] Det vil si innenfor grensene til den etterforskende stat, i internasjonalt farvann eller internasjonalt luftrom. Et eksempel på dette er der etterforskende myndigheter beslaglegger siktedes datamaskin innenfor sitt eget statlige territorium, og datamaskinen inneholder informasjon som vanligvis er lagret på en utenlandsk server, men som er lastet ned lokalt av den private brukeren.[98] Det vil si at den private brukeren selv har flyttet materialet fra *«skyen»* til sin lokale datamaskin. I slike tilfeller vil ikke en påfølgende inndragning av materialet utgjøre en krenkelse av suvereniteten til staten materialet opprinnelig var lagret i. Her er det eieren av dataene og ikke håndhevende myndigheter som har flyttet materialet.[99]

Ransakingen hos Tidal Music AS innebar at Økokrim fra selskapets terminaler i Norge lastet ned materiale som Tidal hadde lagret på servere i USA. Det var med andre ord ikke tale om inngripen gjennom fysisk tilstedeværelse på amerikansk territorium. Heller var det ikke tale om materiale som var nedlastet av Tidal selv og lagret lokalt på deres datamaskiner. Situasjonen med serverransaking befinner seg således et sted imellom den sikre grensen for suverenitetskrenkelse, og den nedre grensen hvor aktiviteten anses lovlig etter folkeretten.

5 Traktatretten

5.1 The Budapest Convention on Cybercrime

Som følge av globaliseringen og økningen av grenseoverskridende kriminalitet er det etablert samarbeidsprosedyrer i konvensjoner om gjensidig juridisk samarbeid. Disse prosedyrene har

[96] HR-2019-610-A avsnitt 42
[97] Sieber & Neubert (2016) s. 261
[98] Ibid.
[99] Ibid.

videre blitt justert og forsøkt tilpasset de digitale etterforskningsmetodene som i dag brukes i etterforskingen av kriminalitet.[100] Som eksempler på slike konvensjoner kan nevnes Europarådets konvensjon om datakriminalitet av 23. november 2001 (The Budapest Convention on Cybercrime, heretter Cybercrime-konvensjonen), The 2010 Arab Convention on Combating Information Technology Offences og The Common Market for Eastern and Southern Africa Cyber Security Model Bill 2011.

Den desidert viktigste konvensjonen for spørsmålet i denne avhandlingen er Cybercrime-konvensjonen, og avhandlingen vil derfor begrense seg til å omtale denne. Konvensjonen er den første internasjonale avtalen om forbrytelser begått via internett, og er ratifisert av mer enn 70 stater, herunder både Norge og USA.[101] Partene har gjennom ratifikasjonen forpliktet seg til gjensidig strafferettslig samarbeid i saker om datakriminalitet. Europarådet har videre en egen komité[102] som konstant følger utviklingen og holder konvensjonen oppdatert i form av protokoller, veiledningsnotater og konferanser. Dette gjør konvensjonen særlig verdifull sammenlignet med andre lignende konvensjoner i dag.[103]

Hovedformålet med konvensjonen er etter fortalen å innføre en felles kriminalpolitikk rettet mot å beskytte samfunnet mot cyberkriminalitet ved å vedta og harmonisere lovgivning og fremme internasjonalt samarbeid.[104] I den forklarende rapporten som ble utarbeidet sammen med konvensjonen fremheves det at harmonisering av straffebud vil lette bekjempelsen av datakriminalitet både nasjonalt og internasjonalt. Risikoen for jurisdiksjoner med lavere standard, såkalte *«data havens»,* vil således også reduseres. Det internasjonale samarbeidet vil bli styrket ved utveksling av erfaringer med andre stater. Dernest vil harmonisering av nasjonale straffebestemmelser muliggjøre utlevering av lovbrytere statene imellom.[105]

Straffebestemmelsene i konvensjonens artikkel 2 til 10 fastsetter minstekrav til gjennomføringen av konvensjonen i nasjonal rett. Artiklene pålegger medlemsstatene å kriminalisere en rekke oppgitte forhold, herunder datarelatert forfalskning, svindel og

[100] Sieber & Neubert (2016) s. 245-246
[101] Europarådet (2020)
[102] Cybercrime Convention Comittee (T-CY)
[103] Sieber & Neubert (2016) s. 265
[104] Se konvensjonens fortale
[105] NOU 2003:27 Lovtiltak mot datakriminalitet s. 13

forseelser relatert til barnepornografi. Statene kan for øvrig selv velge å opprettholde eller vedta straffebestemmelser som er mer vidtgående enn konvensjonens bestemmelser.[106]

De prosessuelle bestemmelsene i artikkel 14 til 22 pålegger medlemsstatene å treffe nødvendige rettslige og faktiske tiltak for å sikre at konvensjonens prosessuelle bestemmelser blir gjennomført. Statene forpliktes videre til å sørge for at tiltakene som iverksettes er underlagt nasjonale rettssikkerhetsgarantier (*«safeguards»*), og statene skal ved gjennomføringen av konvensjonen respektere internasjonale menneskerettighetsinstrumenter, jf. artikkel 15.

5.2 Om internasjonalt samarbeid og jurisdiksjon

Ved fremforhandlingen av konvensjonen var deltakerstatene enige om at det ikke skulle utarbeides et særskilt regime for gjensidig bistand i konvensjonen. I stedet skal statene anvende eksisterende regimer for gjensidig samarbeid med tillegg av de spesielle mekanismene som er etablert i Cybercrime-konvensjonen.[107]

De eksisterende regimer det refereres til er blant annet Europarådskonvensjon 13. desember 1957 om utlevering av lovbrytere og Europarådskonvensjon 20. april 1959 om gjensidig hjelp i straffesaker.[108] Cybercrime-konvensjonen artikkel 23 til 35 fastsetter utover dette supplerende bestemmelser om internasjonalt samarbeid. Det angis her generelle prinsipper for samarbeid, samt særskilte mekanismer for blant annet tilgang til og sikring av lagrede data og avdekking av datatrafikk i sanntid.[109]

Cybercrime-konvensjonen artikkel 23 angir grunnleggende prinsipper knyttet til internasjonalt samarbeid. For det første fastsetter bestemmelsen at partene *«shall co-operate with each other ... to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence»*. Videre skal statene i sitt samarbeid anvende *«relevant international instruments on international co-operation in criminal matters»*. Dette tilsier at konvensjonens bestemmelser om internasjonalt samarbeid

[106] NOU 2003:27 Lovtiltak mot datakriminalitet s. 13
[107] NOU 2003:27 Lovtiltak mot datakriminalitet s. 53
[108] Ibid.
[109] Ibid.

ikke erstatter bestemmelser i andre internasjonale instrumenter, men skal bidra til å styrke et allerede eksisterende samarbeid.

Artikkel 25 fastsetter generelle prinsipper for gjensidig bistand. Her pålegges statene å *«afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence»*. Partene må derfor *«adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35»*. Partene kan *«in urgent circumstances»* sende anmodninger om rettslig bistand ved hjelp av *«expedited means of communication»*, herunder faks og e-post. Den anmodede part *«shall accept and respond to the request by any such expedited means of communication»*.

Artikkel 27 angir fremgangsmåter ved anmodning om gjensidig bistand når det ikke foreligger andre internasjonale avtaler, eller når partene til tross for at det foreligger slik avtale, likevel velger å anvende artikkel 27. Artikkelen bestemmer blant annet at hver part skal utpeke *«a central authority or authorities responsible for sending and answering requests for mutual legal assistance»*.

Videre finnes det i artikkel 27 regler om utsettelse eller avslag på anmodning om bistand. Dette kan blant annet gjøres dersom den anmodede part mener at gjennomføringen vil kunne krenke dens suverenitet eller andre vesentlige interesser, eller dersom gjennomføring vil kunne skade egen etterforsking av forholdet.

Artiklene 29 til 31 fastsetter regler for anmodning om hurtig sikring av elektroniske data som er lagret på territoriet til den annen part, om hurtig utlevering av slike sikrede data og om anmodning om ransaking eller liknende tilgang, beslag, forvaring eller avdekking av data som er lagret på en annen parts territorium.

Hensynet til tempo og effektivitet er tydelig vektlagt ved at hver stat etter artikkel 35 forutsettes å opprettholde *«a point of contact available on twenty-four hour, seven-day-a-week basis»* for å sikre omgående hjelp til etterforskning og bevisinnhenting. Konvensjonen stiller også krav til at de ansatte på kontaktpunktet har nødvendig kompetanse og er tilstrekkelig teknisk utstyrt. De skal kunne bistå med tekniske råd, sørge for bevissikring, innhente bevis, oppspore gjerningspersoner med videre. At konvensjonen åpner for

kommunikasjon via faks og e-post i hastetilfeller, er også en vesentlig lettelse i samarbeidet.[110]

Konvensjonen etablerer med andre ord et detaljert og helhetlig system for internasjonalt samarbeid på området. Det fokuseres gjennomgående på effektivisering, modernisering og harmonisering av lovgivningen i de stater som tiltrer den. [111] Konvensjonen representerer således et viktig skritt i retning av et bedre internasjonalt samarbeid.

5.3 Artikkel 32 – *«Trans-border access to stored computer data with consent or where publicly available»*

Artikkel 32 gir regler om grenseoverskridende tilgang til lagrede, elektroniske data, med samtykke fra bruker eller når de er offentlig tilgjengelige. Bestemmelsen angir tilfeller hvor en part *«without the authorization of another Party»* kan skaffe seg tilgang til data.

For det første kan en part skaffe seg tilgang til *«publicly available (open source) stored computer data»* uavhengig av hvor dataene befinner seg geografisk, jf. bokstav a. Ordlyden tilsier at politiet i én stat ikke trenger samtykke for å innhente informasjon som kan skaffes gjennom et åpent internettsøk.

At man ved utformingen av konvensjonen fant grunn til å presisere at åpne søk skulle være tillatt, kan tolkes dithen at også slike søk i utgangspunktet anses som en håndhevelseshandling som krever samtykke, men at slike likevel aksepteres.

Når data er offentlig tilgjengelig for alle, uavhengig av hvor de befinner seg i verden, kan det argumenteres for at dataenes lokalisasjon ikke kan anses beskyttelsesverdig i jurisdiksjonssammenheng.[112] Det må i slike tilfeller antas at eieren av dataene ikke har noe imot at de blir lest av andre. Serverstaten har da ingen grunn til å tro at borgerens individuelle rettigheter blir krenket, og følgelig ingen grunn til å beskytte dem fra inngripen utenfra. Av den grunn dekker begrepet *«publicly available»* også data som bare kan nås etter å ha fullført en form for registrering på nettsiden og data som bare kan nås etter forutsetning om betaling;

[110] Sunde (2002) s. 99
[111] Ibid.
[112] Sieber & /Neubert (2016) s. 266

felles er at alle som vil, kan nå materialet. Det samme gjelder offentlige samtaler i chatterom og informasjon fra åpne profiler på sosiale medier.[113]

Av den forklarende rapporten til artikkel 32 fremgår det at det etter at konvensjonen trådte i kraft ikke har oppstått noen problemer eller spørsmål vedrørende artikkel 32 bokstav a, og at det er *«commonly understood that law enforcement officials may access any data that the public may access, and for this purpose subscribe to or register for services available to the public»*.[114] Uttalelsen kan tolkes dithen at det i dag foreligger en felles internasjonal rettsoppfatning om at det kan søkes i offentlig tilgjengelige data i straffeforfølgningsøyemed uten samtykke fra serverstaten.

Det andre tilfellet hvor samtykke ikke kreves, er når en via et datasystem på eget territorium kan skaffe seg tilgang til eller motta elektroniske data som fysisk befinner seg i en annen stat, *«if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system»*, jf. bokstav b. Ordlyden tilsier at det må innhentes et lovlig og frivillig samtykke. Frivillighetskriteriet tilsier at politiet ikke kan bruke innloggingsinformasjon som er ervervet gjennom ransaking til å logge seg inn på brukerens PC og slik skaffe seg tilgang til data. Personen eller selskapet det gjelder må selv, på frivillig basis – det vil si uten tvang – utlevere informasjonen til politiet. Hvis slikt samtykke ikke foreligger, må serverstaten anmodes om bistand. En slik tolkning er også lagt til grunn i den forklarende rapporten til bestemmelsen.[115]

Artikkel 32 bokstav b refererer til *«stored computer data located in another Party»*. Dette tilsier at bestemmelsen er anvendelig i tilfeller hvor dataenes lokalisasjon er kjent. Det er i den forklarende rapporten fastslått at artikkel 32 bokstav b ikke gjelder i tilfeller der de aktuelle dataene ikke er lagret i en av medlemsstatene og heller ikke når det usikkert hvor dataene er lagret. Det følger videre at

> *«… in situations where it is unknown whether, or not certain that, data are stored in another Party, Parties may need to evaluate themselves the legitimacy of a search or*

[113] Sieber & /Neubert (2016) s. 266
[114] T-CY guidance note # 3 (2014) side 3
[115] Ibid. s. 6

other type of access in the light of domestic law, relevant international law principles or considerations of international relations.»[116]

Dette innebærer at stater, i tilfeller hvor datamaterialets lokalisasjon er usikker eller ukjent, selv må bestemme legitimiteten av et grenseoverskridende søk.[117]

Artikkel 32 gir partene tillatelse til å *«access»* data. Ordlyden tilsier at det er tillatt å finne frem til data i de gitte tilfellene, uten å si noe mer om hva som er tillatelig utover dette. Dette reiser spørsmål om hjemmelen også inkluderer kopiering, beslaglegging, endring eller sletting av materialet. Formålet med artikkel 32 er ifølge «Explanatory Report to the Convention on Cybercrime» å etablere en adgang for stater til å kunne bruke data i strafferettslige etterforskinger, herunder å bruke dem som bevis, uten å måtte gå gjennom prosedyrene for gjensidig bistand.[118] Hvis stater ikke skulle hatt lov til på en eller annen måte å tilegne seg dataene de fant i samsvar med artikkel 32 ville bestemmelsens formål ha feilet. Det må derfor antas at i alle fall kopiering av slike data er tillatt under begrepet *«access»*.[119]

6 Folkerettslig rettspraksis

Utenom Lotus-saken[120] som fastslår at stater ikke kan bruke tvang på andre staters territorium, finnes det lite relevant rettspraksis for spørsmålet om suverenitet og digital bevisinnhenting.

Voldgiftssaken *«The Trail Smelter»* fra 1941 kan gi veiledning. I saken ble Canada holdt erstatningsansvarlig for skader påført amerikansk jord etter luftforurensing fra et smelteverk. Den internasjonale voldgiftsdomstolen kom til at folkeretten inneholder et forbud mot å volde betydelig skade på andre staters territorium:

«[...] no State has the right to use or permit the use of its territory in such manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence.»[121]

---

[116] T-CY guidance note # 3 (2014) s. 6
[117] Om dette i avhandlingens kapittel 8
[118] Europarådet (2001) punktene 253 og 293
[119] Sieber & Neubert (2016) s. 268
[120] Om denne i kapittel 4 ovenfor.
[121] America v. Canada (1938)

Selv om saken ikke har direkte overføringsverdi til spørsmålet om suverenitetskrenkelse ved håndhevelseshandlinger utført i cyberspace, viser den at en stats territorielle integritet kan krenkes til tross for manglende fysisk tilstedeværelse på dets territorium fra den skadevoldende staten. En slik forståelse er også lagt til grunn i folkerettslig litteratur. Ulrich Sieber og Carl-Wendelin Neubert presiserer blant annet at:

> *«Public international law deems it irrelevant that a law enforcement officer conducting an investigation is not physically located on foreign soil: Ever since the famous Trail Smelter Arbitration, it has been an accepted principle in international law that acts attributable to a State that are conducted from the territory of one State but that take effect within the territory of another State infringe the sovereignty of the affected State.»*[122]

Om man ser Lotus-saken og The Trail Smelter-saken i sammenheng kan det argumenteres for at stater også er avskåret fra tvangsbruk som ikke krever fysisk tilstedeværelse på et annet territorium, noe som vil være tilfellet ved ransaking av utenlandske servere. Med dagens teknologi kan etterforskningsskritt som tidligere krevde fysisk tilstedeværelse, gjennomføres ensidig på et territorium fra et annet. De samme hensyn som begrunner suverenitetskrenkelse ved fysisk tilstedeværelse bør således gjøre seg gjeldende også for slike etterforskningsskritt. En slik dynamisk tolkning er også lagt til grunn i folkerettslig litteratur.[123]

7 Sedvanerett

7.1 Folkerettslig sedvane består av to elementer

Folkerettslig sedvanerett består av to elementer. Det må for det første kunne påvises en *«general practice»* (statspraksis), og denne må være *«accepted as law»* (*opinio juris*, om dette i kapittel 7.9 nedenfor), jf. ICJ-statuttene artikkel 38 (1) bokstav b. Ordlyden tilsier at det må foreligge en samsvarende praksis blant statene, og at statene må anse praksisen som en juridisk plikt.

Det kreves også at statspraksisen må ha foregått over en viss tid for å gi grunnlag for sedvanerett. ICJ uttalte i Nordsjø-saken (1969)[124] at en konvensjon kan gi grunnlag for en

[122] Sieber & Neubert (2016) s. 257
[123] Sieber & Neubert (2016) s. 257 med videre henvisninger, Koops & Goodwin (2014) s. 19
[124] Nordsjøsaken (1969) på s. 42

sedvanerettsregel *«even without the passage of any considerable period of time»*.[125] Dette tilsier at det ikke finnes noen absolutt tidsfrist, men at vurderingen av om en sedvanerettsregel er dannet, må bero på en skjønnsmessig helhetsvurdering.

Ved bedømmelsen av statspraksis er alle uttrykk for statenes rettsoppfatning relevante. Det kan for eksempel være lovgivning, håndhevelse eller avgjørelser av nasjonale domstoler. En viktig del av statspraksis er også kollektive handlinger fra statene i form av inngåelse av rettssettende traktater eller vedtak i internasjonale organisasjoner som således gir uttrykk for en felles rettsoppfatning. For at en praksis skal anses som sedvanerett etter ICJ-statuttene, må praksisen følges av et betydelig antall stater. Dette er i Fiskerijurisdiksjonssaken[126] fra 1974 uttrykt som et krav om *«widespread acceptance»*.[127] Dette tilsier at praksisen i alle fall må følges av et flertall stater.

7.2 Metodiske utfordringer

Å utrede et spørsmål om dannelse av folkerettslig sedvanerett krever en hel del mer kildeanalyse enn det er mulig å få til i et delkapittel i en liten masteravhandling. Det har blitt gjennomført omfattende internasjonale undersøkelser uten at det er funnet noen konsensus. Som det vil fremgå i det følgende er det bevist at flere stater i praksis bruker ensidig grenseoverskridende datatilgang som etterforskningsmetode, men vilkårene for bruken av det og begrunnelsene for det er for varierte til at det kan sies å ligge noen *«general practice»*.[128]

Formålet i dette delkapittelet er med andre ord ikke å kunne svaret *«ja»* eller *«nei»* på et spørsmål om folkerettslig sedvane er dannet, men heller å kunne gi et overordnet bilde av hvordan det internasjonale samfunnet per i dag forholder seg til problemet.

I det følgende vil lovgivningen i Belgia, Nederland, Portugal, England, USA og EU undersøkes. Formålet er å se hvilke likheter og ulikheter som finnes i lovverkene, og undersøke om det finnes noen felles rettsoppfatning rundt jurisdiksjonsproblemet. Rettspraksis fra landene vil også berøres der det finnes relevante dommer.

Som forklart i delkapittel 1.2.5 er ofte den beste fremgangsmåten for på trygt grunnlag å fastslå gjeldende rett i et annet rettssystem, å bygge på juridisk litteratur fra det aktuelle

[125] Ruud & Ulfstein (2018) s. 78-79
[126] United Kingdom v. Iceland (1974) på s. 26
[127] Ruud & Ulfstein (2018) s. 77-78
[128] Se UNODC (2013) s. 219, Sieber & Neubert (2016) s. 283

rettssystemet. På den måten kan misforståelser begrunnet i manglende kunnskap om språk og juridisk metode unngås. Fremstillingen under bygger på rapporter fra Cybercrime-komitéen, informasjonssider fra myndighetene i de respektive statene, juridisk litteratur, og for EUs del deres egne rapporter om lovarbeidet.

7.3 Statspraksis i Belgia

Belgia vedtok i 2000 en ny artikkel 88 i Belgian Criminal Code of Procedure (BCCP). Bestemmelsen gir etterforskende dommer hjemmel til, når det foretas søk i datasystemer, å utvide søket til også å omfatte andre datasystemer selv om de er lokalisert i en annen stat.[129]

Det oppstilles tre vilkår for beslutning om utvidet søk. Søket må for det første være nødvendig for å komme til bunns i etterforskingen. For det andre må andre etterforskningsmetoder anses utjenlige, for eksempel dersom det er nærliggende risiko for at bevisene vil gå tapt; noe som oftest vil være oppfylt i nettkriminalitetssaker idet bevis lett kan flyttes eller ødelegges.[130] Endelig må dommeren begrense søket til de delene av datasystemet som brukerne av det opprinnelige systemet har tilgang til, for eksempel dersom politiet får tilgang til et annet datasystem ved hjelp av innloggingsinformasjonen til siktede. Innloggingen definerer i så tilfelle begrensningen i tilgangen.[131] Etter at slikt søk er utført, stiller bestemmelsen krav om at personen som eier eller er ansvarlig for datasystemet må notifiseres dersom vedkommende lar seg identifisere.[132]

Den mest innovative delen av BCCP artikkel 88 ligger i det siste avsnittet i paragraf 3, som stadfester at når det oppdagede datamaterialet viser seg å være lagret utenfor belgisk territorium, kan dataene bare kopieres, ikke endres eller slettes. Når dette er tilfellet skal etterforskende dommer informere justisdepartementet slik at justisministeren notifiserer staten det gjelder, dersom det lar seg gjøre å lokalisere hvor dataene er lagret.[133] En slik bestemmelse synes å bygge på det synspunkt at det ikke kan gjøres skade på en annen stats territorium, og er således i samsvar med de kilder som ovenfor er undersøkt.

BCCP fokuserer altså ikke på hvor dataene er lagret, men på hvor de er tilgjengelige fra. Bare når det via datamaskiner eller innloggingsinformasjon på belgisk territorium er mulig å skaffe

[129] T-CY (2012) *s. 32 punkt 160-163*
[130] Ibid. s. 32 punkt 164
[131] Ibid. s. 32 punkt 165
[132] Ibid. s. 33 punkt 166
[133] Ibid. s. 33 punkt 167-168

tilgang til data på utenlandske servere, er ransaking tillatt. Det er således ikke tale om å hacke seg inn på utenlandske servere. En slik tilgang er viktig for å spare dyrebar tid i etterforskingen ved å unngå å tape bevis i påvente av saksbehandling i forbindelse med bistandsanmodninger. Dessuten er det ofte ikke mulig å lokalisere hvor dataene er lagret.[134]

Belgias syn på grenseoverskridende tilgang til data fremkommer også i rettspraksis fra landet. I en sak for belgisk høyesterett i 2011 ble skytjenesteleverandøren Yahoo! Inc. ilagt en bot på 44 000 euro for ikke å ha samarbeidet med etterforskende myndigheter i Belgia i en etterforsking av svindel begått via epostkontoer driftet av Yahoo! Inc.[135]

Det amerikanskregistrerte selskapet ble i saken bedt om å oppgi IP-adresser tilknyttet e-postkontoene til de mistenkte, men nektet å etterkomme pålegget.[136] Yahoo! Inc. mente at Belgia ved pålegget utøvde ekstraterritoriell håndheving av sin lovgivning. Det var i domstolene stor usikkerhet rundt om Belgia kunne håndheve sin lovgivning overfor selskapet i et tilfelle som dette.[137] Ankedomstolen og Høyesterett konkluderte med at anklager om ekstraterritorialitet bare kunne aksepteres dersom det hadde vært en anmodning om overlevering av data eller gjenstander som var lokalisert i USA, og som ikke hadde noen territoriell forbindelse til Belgia. Siden Yahoo! Inc. tilbydde sine tjenester til belgiske borgere, hadde en viktig rolle i belgisk økonomi, brukte et belgisk domenenavn ('www.yahoo.be') og hadde nettsider på belgisk språk, var de tilknyttet belgisk territorium på en slik måte at Belgia hadde jurisdiksjon til å håndheve sin lovgivning overfor dem.[138]

Dommen er i litteraturen kritisert for å ha ignorert skillet mellom jurisdiksjon til å vedta lovgivning og jurisdiksjon til å håndheve lovgivning. Selv om belgiske myndigheter er autorisert til å vedta lovgivning overfor utenlandske selskaper som opererer i Belgia, betyr det ikke uten videre at de har samme myndighet til å håndheve lovgivningen sin overfor dem. Yahoo! Inc. hadde ingen lokaler eller ansatte i Belgia. I prinsippet var det dermed ikke tale om et selskap på belgisk territorium.[139]

---

[134] T-CY (2012) s. 33 punkt 167-172
[135] Belgian Yahoo Case (2015)
[136] Oerlemans (2017) s. 313
[137] L'Ecluse & D'hulst (2016)
[138] Oerlemans (2017) s. 313, L'Ecluse & D'hulst (2016)
[139] Oerlemans (2017) s. 313 med videre henvisninger

7.4 Statspraksis i Nederland

Nederland vedtok i 2006 nye bestemmelser i sin straffeprosesslov, Dutch Code of Criminal Procedure (DCCP), for å oppfylle Cybercrime-konvensjonen. Når det gjelder datasøk i etterforskingsøyemed er artikkel 125 og 126 de mest relevante.[140]

Artikkel 125 gir blant annet hjemmel til å undersøke datamaskiner i forbindelse med ransaking av hus eller andre lokaler. Slike søk gjelder imidlertid bare for alvorlig kriminalitet med høye strafferammer og på nederlandsk territorium. Søket må skje på stedet i forbindelse med ransakingen, med mindre den rettmessige eieren av dataene godkjenner et etterfølgende søk eller etterforskende dommer begjærer innloggingsinformasjon utlevert.[141]

Artikkel 126 tillater innenfor visse grenser innhenting av informasjon som er formidlet via en datamaskin tilkoblet internett. Også dette gjelder bare på nederlandsk territorium. Denne etterforskningsmetoden kan imidlertid ikke brukes til å spore opp lagret informasjon. Det antas derfor at denne metoden ikke kan brukes til å skaffe informasjon om for eksempel et passord som er nødvendig for å få tilgang til krypterte data.[142]

Når det gjelder søk på systemer utenfor Nederland, følger det eksplisitt av den forklarende rapporten til the Dutch Cyber Crime Act at dette ikke er tillatt; det kan bare gjøres gjennom metoder som følger av folkeretten. I praksis innebærer altså dette at en da må benytte seg av mutual legal assistance og prosedyrene i Cybercrime-konvensjonen. [143]

Det nederlandske aktorembetet etterspurte lenge etterforskningsmetoder som ga mulighet til å etterforske på tvers av landegrenser. I mangel på dette har det i praksis vært flere operasjoner der det nederlandske aktoratet har forsøkt å gjennomføre innovative etterforskinger over landegrensene innenfor eksisterende juridiske rammer. Blant de mest kjente kan nevnes Bredolab-saken fra 2010 og Descartes-saken fra 2011. Felles for disse sakene er at politiet brukte hacking som etterforskningsmetode. Det nederlandske parlamentet stilte som følge av dette spørsmål ved lovligheten av politiets arbeid.[144]

---

[140] T-CY (2012) *s. 33 punkt 173*
[141] Ibid.
[142] T-CY (2012) s. 34 punkt. 173-174
[143] Ibid.
[144] Oerlemans (2017) s. 259

I Bredolab-saken lyktes det nederlandske myndigheter å ta kontroll over og bekjempe et stort botnet.[145] Gjennom botnetet, som var av utenlandsk opprinnelse, hadde siktede infisert mer enn 30 millioner datamaskiner over hele verden og stjålet konfidensiell finansiell informasjon.[146] Infrastrukturen i botnetet var kompleks og besto av flere krypterte servere som var lokalisert hos en nederlandsk leverandør av skytjenester. Plasseringen av botnetet og samarbeidsviljen til skytjenesteleverandøren gjorde det mulig for nederlandske etterforskere å foreta et søk i leverandørens systemer og således ta over botnetet ved å hacke flere av serverne. Det ble deretter sendt ut en melding til alle infiserte datamaskiner med melding om viruset og oppfordring om å få renset datamaskinene.[147] Den siktede ble lokalisert i Armenia og straffeforfulgt av myndighetene der.[148]

I Descartes-saken lyktes det nederlandske myndigheter, gjennom hacking, å få kontroll over fire servere skjult gjennom TOR (The Onion Router)[149] som var vert for grovt voldelig overgrepsmateriale av barn.[150] Det ble tatt digitale kopier av materialet for å bruke som bevis i straffesaken før det ble ødelagt og erstattet med logoen til det nederlandske politiet. I tillegg ble det lagt igjen en advarende melding til brukerne av disse nettsidene om at sidene var under etterforsking av nederlandsk politi, og at brukerne ved å søke tilgang til materialet risikerte straffeforfølgning.[151]

På tross av bred internasjonal publikasjon møtte ikke nederlandske myndigheter noen protester fra det internasjonale samfunnet. Uten muligheter til å etterforske på tvers av landegrenser ville ikke politiet klare å holde følge med utviklingen av kriminaliteten og således fange opp alvorlige kriminelle forhold.[152] Motivert av suksessen med Bredolab- og Descartes-sakene, og trolig inspirert av den belgiske BCCP artikkel 88, ble det i 2013 derfor

---

[145] Et «botnet» er et nettverk av datamaskiner infisert av ondsinnede programvarer, for eksempel datavirus eller spyware. Disse maskinene kobles til en eller flere styrende servere hvor de får tildelt oppgaver, i dette tilfellet servere styrt av den siktede, jf. Oerlemans (2017) s. 259
[146] The Guardian (2010)
[147] Oerlemans (2017) s. 259
[148] The Guardian (2010)
[149] TOR er en programvare som gir personer mulighet til å bruke internett helt anonymt, og gir også mulighet til å nå materiale på servere som bare kan nås gjennom TOR, jf. Oerlemans (2017) s. 40
[150] T-CY (2012) *35 pkt. 182-183*
[151] Ibid.
[152] Koops & Goodwin (2014) s. 84

fremlagt et lovforslag som gav nederlandske myndigheter bedre verktøy i kampen mot internettrelatert kriminalitet.[153]

The Computer Crime Act III trådte i kraft 1. mars 2019 og gir etterforskende myndigheter hjemmel til gjennom hacking å skaffe seg tilgang til systemer fra en annen datamaskin uten eierens kunnskap, herunder også til å kopiere og ødelegge data.[154] Slik hjemmel foreligger, under forutsetning av at en rekke vilkår er oppfylt, i tilfeller hvor siktede benytter seg av skytjenester eller anonymiserende tjenester og dataenes lokalisasjon er ukjent. Dersom plasseringen av dataene er kjent, må myndighetene falle tilbake på mutual legal assistance-systemet.[155]

Hjemmelen til å bruke hacking som etterforskningsmetode er betinget av flere vilkår. For det første må saken gjelde et hastetilfelle som nødvendiggjør bruken av hacking. For det andre må begjæringen behandles av en domstol. Endelig kreves det at lovbruddet utgjør et alvorlig brudd på rettsordenen, som etter loven innebærer at det må være tale om lovbrudd med strafferamme på åtte år eller mer, eller at det gjelder et av lovbruddene som myndighetene har utpekt.[156] Eksempler på slike er besittelse av barnepornografi, rekruttering til terrorisme, deltakelse i organisert kriminalitet, svindel og hvitvasking av penger.[157]

7.5 Statspraksis i Portugal

Portugal vedtok i september 2009 The Portuguese Law on Cybercrime som inneholder regler om innhenting av elektroniske bevis. Lovens artikkel 15 gir etterforskende myndigheter hjemmel til, når det under etterforskingen er nødvendig for bevisbildet i saken eller for å finne sannheten, å innhente spesifikke data som er lagret i et spesifikt datasystem. Videre følger at når det er grunn til å tro at informasjonen som søkes er lagret i et annet datasystem, kan det også skaffes tilgang til disse når slik tilgang er tilgjengelig fra det opprinnelige datasystemet. Dette gjelder også data på systemer utenfor portugisiske grenser.[158]

Lovens artikkel 16 regulerer adgangen til å beslaglegge slike grenseoverskridende data. Etter kjennelse fra en domstol kan data beslaglegges enten ved å ta beslag i den fysiske enheten

---

[153] Koops & Goodwin (2014) s. 84
[154] Governments of Netherlands (2019), T-CY (2012) punkt 179
[155] Oerlemans (2017) s. 341
[156] Simmons Simmons (2019), Oerlemans (2017) s. 341
[157] Simmons Simmons (2019), Governments of Netherlands (2019)
[158] T-CY (2012) s. 37-38

dataene er lagret på, ved å kopiere dem eller ved å slette eller blokkere tilgangen til dataene. Loven ligner således den nederlandske loven ved å gå langt i adgangen til å ta beslag.[159]

7.6 Statspraksis i USA

The Microsoft Ireland case ga i februar 2018 amerikansk høyesterett en ny type problemstilling: Ville en ransakelsesordre gitt i medhold av The 1986 Stored Communication Act (SCA) hjemle ransaking av e-poster og andre kommunikasjonsplattformer som var eid og kontrollert av et amerikanskbasert selskap, men som var lagret på servere lokalisert utenfor USA?[160]

Saken gjaldt en ransakelsesordre i forbindelse med en narkotikarelatert etterforsking. Microsoft nektet å utlevere informasjonen ettersom dataene var lagret på en server i Irland. Selskapet mente av den grunn at spørsmålet måtte rettes irske myndigheter.[161]

Amerikanske myndigheter anførte at siden Microsoft var et amerikansk selskap måtte de overholde amerikansk lov, selv om informasjonen i dette tilfellet var lagret i et annet land. Det ble argumentert for at man ofte ikke vet hvor dataene er lagret og at anmodning om bistand således kunne være umulig. Videre kunne en rettstilstand der etterforskende myndigheter er avskåret fra å ransake og beslaglegge materiale som er lagret i utlandet medføre at kriminelle bevisst lagret dataene sine utenfor amerikanske grenser for å avskjære myndighetenes tilgang. Dette ville medføre et stort rettssikkerhetsbrudd.[162]

Microsoft advarte mot en tilstand der alle land i verden fritt kunne kreve tilgang til data av interesse. Dette ville ifølge Microsoft gi en internasjonal fritt-for-alle-tilstand som ville lede til uenigheter og dessuten medføre store brudd på personvernrettigheter. Microsoft mente at lovverket trengte oppdatering, men at saken var en problemstilling for lovgiver og ikke domstolene.[163]

Etter flere års forhandlinger i retten om hva som var riktig, slapp domstolen å ta endelig stilling til problemet da en ny lov ble vedtatt i samsvar med regjeringens anførsler i saken.

---

[159] T-CY (2012) s. 37-38
[160] Daskal (2018) s. 9
[161] Dustin (2018)
[162] Dustin (2018), Daskal (2018) s. 10
[163] Daskal (2018) s. 10

The Cloud Act står for *Clarifying Lawful Overseas Use of Data* og innebærer en oppdatering av den eksisterende SCA-loven ved å regulere rekkevidden av USAs ransakelsesmyndighet og utenlandske myndigheters adgang til å søke tilgang til data lagret i USA.[164] Kort fortalt pålegger loven amerikanske tjenesteleverandører å gi tilgang til alt de måtte ha av data i sin besittelse eller kontroll, uavhengig av om dataene er lagret utenfor amerikanske grenser. Dette innebærer at amerikanske myndigheter nå har hjemmel til å kreve utlevert alt av data fra Microsoft, uavhengig av hvor dataene befinner seg.[165]

Selv om loven gir myndighetene rett til ensidig å kreve utlevert data, er det likevel som hovedregel påkrevd at USA må ha en underliggende avtale med den aktuelle staten om utlevering. For å være gyldig må avtalen oppfylle visse krav, blant annet at den utenlandske regjeringen gir betryggende garantier for personvern og vedtar minimeringsprosedyrer.[166]

Loven er kritisert av det internasjonale samfunnet, herunder flere personvernorganisasjoner. For det første inneholder loven en unntaksregel som hjemler ensidig innhenting av data til tross for manglende avtale med, eller enkeltstående samtykke fra aktuelle utenlandske myndigheter.[167] Dette gjelder i situasjoner hvor samtykke ikke kan innhentes, for eksempel på grunn av motstrid mellom landenes nasjonale rett. I slike tilfeller kan data likevel innhentes etter kjennelse fra en domstol som må ta stilling til en rekke forskjellige faktorer. Blant annet plasseringen og nasjonaliteten til personen det søkes informasjon om, viktigheten av informasjonen for USAs etterforsking, samt muligheten for effektiv tilgang til bevisene på alternative måter.[168]

Slik motstrid i nasjonal rett som likevel kan gi USA rett til ensidig tilgang til data utgjør den andre hovedlinjen i kritikken mot The Cloud Act. Loven gir som nevnt ikke bare USA adgang til å få utlevert data fra amerikanskregistrerte selskaper. Den gjelder også motsatt, og lar utenlandske myndigheter innhente data om egne borgere dersom de bruker en amerikansk skytjenesteleverandør. Dette innebærer at dersom en brukers informasjon er lagret via et

[164] Dustin (2018), Daskal (2018) s. 11
[165] Daskal (2018) s. 13
[166] US Congress (2017-2018), Daskal (2018) s. 13, se også kapittel 7.7 om avtalen mellom USA og England
[167] Daskal (2018) s. 11
[168] Daskal (2018) s. 11

amerikansk selskap, så kan det være eksponert for myndigheter fra hele verden, selv om man tror man er beskyttet av EUs GDPR-regelverk eller nasjonale lover.[169]

GDPR er EUs nye personvernforordning og står for *General Data Protection Regulation*. Formålet er å styrke personvernet overfor privatpersoner. I hovedsak dreier det seg om innstramminger knyttet til innsamling, bruk og oppbevaring av personopplysninger for alle virksomheter i EU og EØS-land. Forordningen gir blant annet regler om at personopplysninger bare skal brukes til formålet de er innsamlet for, regler om sletting og overføring av personopplysninger, samt krav til samtykke.[170]

Regelverket setter begrensninger for når data lokalisert innenfor EU kan overføres ut av EU. Artikkel 48 spesifiserer at slik overføring bare kan skje basert på en internasjonal avtale, som for eksempel en traktat om mutual legal assistance. Foreligger ingen slik avtale finnes det likevel unntak i artikkel 49 i tilfeller hvor overføring er *«necessary for important reasons of public interest»* eller der det er nødvendig på grunn av *«compelling legitimate interests»*. Brudd på regelverket kan medføre bøter på inntil 20 millioner euro eller fire prosent av bedriftens totale omsetning.[171]

The Cloud Act gjelder som nevnt for amerikanske selskaper og statsborgere som er innenfor amerikansk jurisdiksjon – også dersom deres data er lagret utenfor amerikansk territorium. Dette kan medføre konflikt mellom The Cloud Act og GDPR idet sistnevnte også gjelder for amerikanske statsborgere som er innenfor Europa, eller hvis data brukes til forretningsvirksomhet i Europa. Et selskap lokalisert i Europa vil derfor kunne bryte med GDPR hvis de overleverer amerikanske personers data til etterforskende myndigheter i USA i forbindelse med straffeforfølgning. Det kan med andre ord oppstå en interessekonflikt hvis et norsk selskap har ansatt en amerikansk statsborger der The Cloud Act krever utlevering av dennes informasjon.[172]

[169] Dustin (2018) og Daskal s. 12
[170] EU (2018), Skarning (2019)
[171] Daskal s. 12, EU (2018)
[172] Beck-Olsen (2019)

The Cloud Act representerer uansett en viktig brikke i rettsutviklingen i relasjon til etterforskning av internettrelatert kriminalitet, idet de største skytjenesteleverandørene i verden i dag er amerikanskregistrerte selskaper.[173]

7.7 Statspraksis i England

Den 12. februar 2019 ble The Crime (Overseas Production Orders) Act vedtatt. Loven gir håndhevende myndigheter hjemmel til, etter kjennelse fra en domstol, å ensidig innhente data som er lagret elektronisk på servere i utlandet. Slik bevisinnhenting kan skje når beviset anses å være av betydning i etterforskning av alvorlig kriminalitet.[174]

Den 3. oktober 2019 signerte USA og England en avtale om grenseoverskridende datatilgang fra tjenesteleverandører.[175] Avtalen er den første bilaterale avtalen under amerikanske Cloud Act. Avtalen pålegger begge parter å fjerne alle barrierer i sitt nasjonale lovverk slik at rettshåndhevende myndigheter i begge stater kan innhente data direkte fra tjenesteleverandører lokalisert i den andre staten. Med andre ord vil USA være unntatt fra restriksjonene i den engelske loven som ellers ekskluderer andre statlige myndigheter fra å skaffe tilgang til data direkte fra tjenesteleverandører i England, og motsatt.[176]

Den gjensidige datatilgangen gjelder imidlertid ikke ubegrenset. For det første stilles det etter avtalen krav til at ethvert krav om datatilgang må være *«for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution»* of a *«Serious Crime, including terrorist activity.»* Avtalen definerer dette som lovbrudd som kan straffes med minimum tre års fengsel, se avtalens artikkel 1.5, 1.14 og 4.1.[177]

Videre stilles det krav om at ordren må rettes mot spesifikke brukerkontoer og således identifisere en *«specific person, account, address, personal device, or any other specific identifier.»*, se artikkel 4.5. Avtalen kan med andre ord ikke brukes til å skaffe generell informasjon om personer eller grupper av personer. [178]

---

[173] Herunder Apple, Microsoft og Google, se for øvrig Europakommisjonen (05.02.2019) s. 4
[174] Thomson m.fl. (2019)
[175] Agreement U.S. and U.K. (2019)
[176] Covington & Burling LLP (2019)
[177] Ibid.
[178] Covington & Burling LLP (2019)

Hver av partene skal videre utpeke en myndighet som skal gjennomgå anmodningene og bekrefte at kravet er lovlig og oppfyller avtalen før det kan overføres til tjenesteleverandøren, se artikkel 5.7. Dersom en av partene anmoder tilgang til data om en person som med rimelig grunn antas å være lokalisert i et tredjepartsland, det vil si utenfor USA og England, må den utpekte myndigheten i den stat som utsteder kravet varsle myndighetene i tredjepartslandet, se artikkel 5.10.[179]

Det oppstilles videre prosedyrer for å minimere bruk og lagring av informasjon om personer fra den andre stat som utilsiktet har blitt ervervet gjennom anmodning etter avtalen, se artikkel 7.2. Videre er partene avskåret fra muligheten til å overføre data de erverver gjennom avtalen, til et tredjeland uten samtykke fra den part som dataene er mottatt fra, se artikkel 8.2.[180]

7.8 Praksis i EU

Det har siden 2003 eksistert avtale om gjensidig samarbeid mellom EU og USA med det formål å sikre et effektivt samarbeid med hensyn til innhenting av digitale bevis. Avtalen trådte i kraft i 2010, og en felles gjennomgang av den ble gjennomført i 2016. Partene konkluderte da med at avtalen er verdifull i samarbeidet mellom statene, men at det bør arbeides ytterligere for å forbedre samarbeidet.[181]

Selv om avtalen i prinsippet var bra, ble det påpekt som problematisk at prosedyrene var for ineffektive med en gjennomsnittlig responstid på 10 måneder. Siden amerikansk lov tillot amerikanskregistrerte selskaper å utlevere informasjon direkte til EU-stater, ble EU-statene oppfordret til å rette anmodninger direkte til tjenesteleverandørene istedenfor til amerikanske myndigheter. En svakhet med loven var imidlertid at et slikt samarbeid var frivillig fra tjenesteleverandørens side. Systemet var således ikke optimalt. Dette gjaldt også motsatt vei, for det tilfellet at amerikanske myndigheter ba om data fra tjenesteleverandører i EU, idet mange europeiske land har nasjonale lovhjemler som forbyr tjenesteleverandører å svare direkte på forespørsler fra utenlandske myndigheter.[182]

[179] Covington & Burling LLP (2019)
[180] Ibid.
[181] Europakommisjonen (05.02.2019) s. 1
[182] Europakommisjonen (05.02.2019) s. 1-2

På bakgrunn av disse utfordringer, fremla Europakommisjonen 17. april 2018 forslag om nye regler for å gjøre det enklere og mer effektivt å innhente elektroniske bevis i forbindelse med etterforsking og påtale av straffesaker.[183] Lovforslaget tar sikte på å etablere et harmonisert regelverk for EU-statene og forskynde prosessen med innhenting av elektroniske bevis i EU.[184]

Regelverket vil for det første opprette en europeisk produksjonsordre (*«production order»*) som gjør det mulig for rettslige myndigheter å kreve elektroniske bevis direkte fra en tjenesteleverandør eller sin juridiske representant i en annen medlemsstat. Disse vil være forpliktet til å svare i løpet av ti dager, og innen seks timer i nødstilfeller, sammenlignet med opptil 120 dager for den eksisterende europeiske etterforskningsordren eller gjennomsnittlig 10 måneder for ordinær mutual legal assistance-prosedyrer.[185] For å gjøre dette enklere og mer effektivt pålegges alle tjenesteleverandører å utpeke én representant for seg i unionen. For det andre vil det opprettes en europeisk bevaringsordre (*«preservation order»*) som gir rettslige myndigheter hjemmel til å be tjenesteleverandør eller dens representant i en annen medlemsstat om å bevare spesifikke data med tanke på senere forespørsel om utlevering.[186] Det legges med andre ord opp til et likt system i EU som det vi ser i amerikanske Cloud Act og i avtalen mellom USA og England.

Regelverket vil innebære strenge sikkerhetsgarantier for grunnleggende rettigheter, herunder personvernrettigheter. Alle tjenesteleverandører vil nå være underlagt det samme regelverket. Dette vil gi klarhet i gjeldende regler og sikre bedre rettssikkerhet for tjenesteleverandører og brukere av tjenestene. Lovforslaget er et resultat av en to år lang prosess som følge av sterk etterspørsel fra medlemsstater og næringslivet.[187] I forlengelsen av dette forhandles det om en ny, gjensidig avtale mellom EU og USA om utlevering av elektroniske bevis som vil få forrang foran Cybercrime-konvensjonen. Avtalen vil løse problemene knyttet til manglende effektivitet i samarbeidet ved begge veier å tillate direkte samarbeid med tjenesteleverandører som vil ha plikt til å utlevere informasjon.[188]

---

[183] Europakommisjonen (2018) «explanatory memorandum» punkt 1
[184] Europakommisjonen (05.02.2019) s. 3
[185] Europakommisjonen (2019)
[186] Europakommisjonen (2019)
[187] Europakommisjonen (2019)
[188] Europakommisjonen (05.02.2019) s. 4

7.9 Opinio juris

7.9.1 Innledning

Etter artikkel 38 (1) bokstav b i Statuttene for ICJ kreves det at statspraksisen må skje på grunnlag av en overbevisning om at det staten gjør, nødvendiggjøres av en rettsregel, for at den skal anses som sedvanerett (*opinio juris)*. Det finnes mange eksempler på statspraksis som stater ikke føler seg juridisk forpliktet til, og som derfor er å anse som statspraksis uten *opinio juris*. Det må med andre ord skilles mellom det statene gjør ut fra praktisk og politisk hensiktsmessighet, og hva som gjøres ut fra rettslig nødvendighet.[189]

Spørsmålet i dette delkapittelet er om statspraksisen som er undersøkt ovenfor er gjort i overbevisning om at praksisen nødvendiggjøres av en rettsregel. Mer konkret er spørsmålet om statene anser praksisen nødvendiggjort av suverenitetsprinsippet.

7.9.2 UNODC – Comprehensive Study on Cybercrime

FN publiserte i februar 2013 en omfattende studie av problemet med cyberkriminalitet. Formålet var å undersøke alternativer for å styrke eksisterende, og foreslå nye nasjonale og internasjonale juridiske løsninger på jurisdiksjonsproblemet. Studien inneholder en omfattende undersøkelse av cyberkriminalitet, med innspill fra medlemsstatene, det internasjonale samfunnet og den private sektor, og inkluderer utveksling av informasjon om nasjonal lovgivning, praksis, teknisk assistanse og internasjonalt samarbeid.[190]

I forbindelse med informasjonsinnhenting i studien, ble en rekke land i Afrika, Amerika, Asia, Oseania og Europa spurt om sin bruk av grenseoverskridende tilgang til data som etterforskingsverktøy, og om hvorvidt slik tilgang fra utenlandske rettshåndhevende myndigheter var tillatt.[191]

Når det gjaldt bruken av grenseoverskridende datatilgang som etterforskningsmetode, rapporterte rundt 20 prosent av landene i Amerika, Asia og Oseania at de hadde utført slike tiltak, enten i forbindelse med etterforsking av cyberkriminalitet eller andre forbrytelser. Blant landene i Afrika svarte 40 prosent at de brukte det, og i Europa var tallet hele 50 prosent. Den høyere prosentandelen i Afrika og Europa skyldes trolig innflytelsen fra Cybercrime-

[189] Ruud & Ulfstein (2018) s. 79
[190] UNODC (2013)
[191] Ibid. s. 219

konvensjonen og The 2011 COMESA Cyber Security Model Bill. Mange av landene presiserte at de kun brukte tiltaket etter å ha fått godkjenning fra serverstaten. Landene som svarte at de ikke brukte tiltaket regelmessig, oppga blant annet manglende regelverk som grunnen til det.[192]

Til tross for at mange stater svarte at de brukte grenseoverskridende datatilgang som etterforskningsmetode var praksisen og vilkårene for den for variert til at studien kunne dokumentere noen generell praksis.[193]

Når det gjaldt lovligheten av utenlandske myndigheters tilgang til data eller datasystemer hos dem selv, svarte rundt to tredjedeler av statene at tiltaket er ulovlig uten avtale. Mange av landene som svarte at de tillot det presiserte at dette bare var tillatt med hjemmel i Cybercrime-konvensjonen. Noen land rapporterte at tiltaket var tillatt i nødsituasjoner, ved trussel mot nasjonal sikkerhet eller hvis det var umulig å lokalisere hvor datamaterialet fysisk var lagret.[194]

Samlet sett kan studien tas til inntekt for at et stort antall av verdens stater anser ensidig grenseoverskridende datatilgang som ulovlig, men at noen tar slike tiltak i bruk til tross for ulovligheten, i mangel på noen internasjonal konsensus og effektivt regelverk. Studien er også tatt til inntekt for et slikt standpunkt i litteraturen.[195]

7.9.3 Cybercrime-konvensjonen

Ved å ratifisere Cybercrime-konvensjonen har medlemsstatene samtykket i at suvereniteten deres ikke krenkes i de to tilfellene hvor artikkel 32 hjemler tilgang til data uten å følge prosedyrene i artikkel 29 følgende. Sett i kontekst fremstår bestemmelsen som et unntak fra plikten til å følge samarbeidsprosedyrene. Dette tilsier at i tilfeller hvor dataene ikke er offentlig tilgjengelig eller hvor frivillig samtykke fra eieren av dataene ikke er gitt, så må etterforskende myndigheter rette seg etter samarbeidsprosedyrene i konvensjonen.

[192] UNODC (2013) s. 219
[193] Sieber & Neubert (2016) s. 283
[194] UNODC (2013) s. 220
[195] Sieber & Neubert (2016) s. 255 og s. 262

Selv ikke i hastetilfeller tillater konvensjonen tilgang til data uten samtykke eller bistand. I slike tilfeller henvises medlemsstatene i stedet til å ta i bruk mer uformelle kommunikasjonsmidler som e-post og faks for å få fortgang i prosessen, jf. artikkel 25.

Samlet sett tilsier dette at den herskende oppfatning blant de 75 medlemsstatene er at elektronisk bevisinnhenting uten samtykke er folkerettsstridig etter suverenitetsprinsippet og at det således var nødvendig å etablere regler og prosedyrer for samarbeid slik at etterforskende myndigheter i forskjellige stater får skaffet nødvendige bevis.

På den annen side er konvensjonen etablert med det formål å fremme internasjonalt samarbeid ved etterforskning av internettrelatert kriminalitet.[196] Det kan således også tenkes at konvensjonen ikke er laget under forutsetning om at den var nødvendiggjort av suverenitetsprinsippet, men at den derimot bare var ment å forenkle samarbeidet statene imellom. Her må det imidlertid innvendes at å etablere og ratifisere en slik traktat ville ha fremstått som meningsløst dersom medlemsstatene mente at ensidig tilgang til data var uproblematisk. Å be om bistand eller samtykke må i seg selv anses unødvendig dersom ensidig tilgang ikke er suverenitetskrenkende. Det fremstår således som åpenlyst at suverenitetsprinsippet ligger til grunn for det hele og at konvensjonen er et resultat av at statene anser det som nødvendig med en samarbeidsavtale på grunn av suverenitetsprinsippet.

Tilsvarende regler som i Cybercrime-konvensjonen er også å finne i The 2010 Arab Convention on Combating Information Technology Offences og The 2011 COMESA Cyber Security Model Bill. Disse er ratifisert av en rekke arabiske og afrikanske stater og viser at det er en bredere oppslutning rundt synspunktet om suverenitetskrenkelse foruten de 75 statene som har ratifisert Cybercrime-konvensjonen.

7.9.4 Vedtakelsen av nasjonale lover og avtaleinngåelse med annen stat

Undersøkelsen i kapittel 7.3-7.8 ovenfor viser at en rekke stater har vedtatt nasjonale lovhjemler for å regulere grenseoverskridende datatilgang. Alle de stater som der er nevnt, har til felles at de har ratifisert Cybercrime-konvensjonen. Dette i seg selv tilsier en grunnleggende oppfatning om at ensidig grenseoverskridende datatilgang er

[196] Kapittel 5.1 ovenfor

suverenitetskrenkende uten samtykke. Det kan således stilles spørsmål ved nasjonale lovhjemler som i strid med dette likevel gir hjemmel for ensidig innhenting av data.

Cybercrime-komitéen (T-CY) har i «Assessment Report: the Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime» fra 2013 funnet at gjennomsnittlig responstid på bistandsanmodninger etter konvensjonens system ligger på mellom seks og 24 måneder, i tillegg til at mange av anmodningene avvises.[197] Vedtakelsen av nasjonale lovhjemler om ensidig grenseoverskridende datatilgang må ses i lys av dette. Hensynet til å beskytte egne borgere mot kriminalitet, og til å ivareta siktedes rettssikkerhet og rett til en rettferdig rettergang etter Grunnloven § 95 og EMK artikkel 6, jf. menneskerettsloven § 3, jf. § 2,[198]må veie tyngre enn hensynet til serverstatens suverenitet, særlig må dette gjelde i tilfeller av alvorlig kriminalitet.

På bakgrunn av dette fremstår ikke de nasjonale lovhjemler som et uttrykk for at statene anser ensidig datatilgang som lovlig etter folkeretten. Lovhjemlene er reservert for tilfeller av alvorlig kriminalitet og stiller krav om nødvendighet, domstolsbehandling og fortløpende notifikasjon til serverstaten etter inngrepet. De aktuelle lovene synes således å bygge på en oppfatning om at slik inngripen på fremmed territorium er ulovlig, men at hensynet til etterforskingen av alvorlig kriminalitet må veie tyngre. Lovhjemlene er således utformet etter et subsidiært mønster og oppstiller rettssikkerhetsgarantier for serverstaten.

I forsøk på å løse problemet har det begynt å vokse frem flere nye bilaterale avtaler. Disse knytter seg særlig til USA og Cloud Act, idet de største skytjenesteleverandørene som i dag leverer tjenester over hele verden har sin base i USA. Ved å etablere et effektivt system hvor data kan kreves direkte fra tjenesteleverandøren, løser man problemet med lang responstid, og suvereniteten til serverstaten ivaretas ved å ha en avtale liggende i bunn.

At et stort antall av verdens stater har inngått traktater i forsøk på å regulere og løse problemet, tyder på at ensidig grenseoverskridende datatilgang synes å være i strid med suverenitetsprinsippet. Skulle det motsatte legges til grunn hadde vedtakelsen av lovhjemler og inngåelse av traktater ha fremstått som meningsløst.

---

[197] Sieber & Neubert (2016) s. 246
[198] Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett

8 Teori

8.1 Spørsmålet om suverenitetskrenkelse

Det finnes til dels ulike oppfatninger i litteraturen knyttet til spørsmålet om grenseoverskridende datatilgang i relasjon til suverenitetsprinsippet. Teorien er likevel i hovedsak samstemt om at slik tilgang i noen tilfeller er suverenitetskrenkende. Ulikhetene knytter seg til hvor den nedre grensen for suverenitetskrenkelse går.

Anna Maria Osula redegjør for dette i sin artikkel «Transborder access and territorial sovereignty». Hun skiller mellom to hovedsynspunkter. Det første bygger på den strenge tolkningen i Lotus-saken som fastslår at all utøvelse av jurisdiksjon på fremmed territorium er å anse som suverenitetskrenkende,[199] og at ransaking og beslag av utenlandske servere således er ulovlig uten særskilt hjemmel. Dette gjelder selv om den virtuelle tilstedeværelsen ikke vil forårsake noen skade eller konsekvenser for den berørte statens nettverk. Et slikt synspunkt har blitt lagt til grunn av en rekke folkerettslige forfattere. Ulempen med en så streng tolkning er at det da foretas tusenvis av suverenitetskrenkende handlinger verden over, hver eneste dag.[200]

Bert Jaap Koops og Morag Goodwin foretar i sin artikkel «Cyberspace, the cloud, and cross-border criminal investigation – The limits and possibilities of international law» en omfattende analyse av rettstilstanden for grenseoverskridende tilgang til datasystemer. De oppsummerer på side 61 gjeldende rett som følger:

> *«[T]he most solid view on what international law permits is that accessing data that are, or later turn out to be, stored on a server located in the territory of another state constitutes a breach of the territorial integrity of that state and thus constitutes a wrongful act (...) except where sovereign consent has been formally given»*

Jan-Jaap Oerlemans gir i sin artikkel «Investigating Cybercrime» uttrykk for det samme når han på side 338-339 skriver at

> *«When law enforcement officials conduct a search remotely on a computer that is located in another State, the territorial sovereignty of the affected State may be*

[199] Om dette i avhandlingens kapittel 4
[200] Osula (2015) s. 726 med videre henvisninger

infringed if no permission has been obtains and no authorising treaty basis is available. »

Også Ulrich Sieber og Carl-Wendelin Neubert legger til grunn et slikt synspunkt når de på side 262 i sin artikkel «Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty» fastslår at

«… nearly all types of transborder criminal investigations undertaken via the internet constitute sovereign acts in another country and as such infringe that country's sovereignty.» På side 251 fastslår de at dette er det herskende syn blant forfattere av folkerettslig litteratur, men at *"[the] view that unilateral transborder investigations in cyberspace do not infringe territorial sovereignty can also be found, but it is rare.»*

Det andre hovedsynspunktet Osula redegjør for, bygger på en antakelse om at ikke alle grenseoverskridende handlinger i relasjon til datatilgang utgjør en suverenitetskrenkelse. De som støtter dette synspunktet argumenterer for at handlingen ikke kan anses som en suverenitetskrenkelse med mindre handlingen medfører skade på den berørte statens nettverk, for eksempel hvis dataene endres eller slettes fra den aktuelle serveren. Ulempen med en slik løsning er at den lett vil kunne misbrukes, og resultere i en fritt for alle-tilstand på internett ved at myndigheter vil ha tilgang til data på servere i alle land, forutsatt at materialet ikke slettes.[201]

Osula oppsummerer med å konstatere at folkeretten fortsatt er uklar på dette punkt, men at det ser ut til at klare internasjonale regler er å foretrekke fremfor den usikkerheten som preger verdenssamfunnet i dag. Osula fremholder at dette bevises gjennom det faktum at stater i stadig økende grad streber for å få spørsmålet regulert, det være seg gjennom traktater eller nasjonal lovgivning. Avslutningsvis uttaler hun at

«[t]ese examples ... may exemplify a belief that transborder access is indeed perceived as violating international law, and thus requires codifying circumstances that would preclude the wrongfulness of such acts.»[202]

En slik konklusjon harmonerer godt med de funn som er gjort i de foregående kapitler.

---

[201] Osula (2015) side 726 med videre henvisninger
[202] Ibid. s. 726

8.2 Offentlig tilgjengelige data og *«loss of location»*-data

Juridisk litteratur innenfor folkeretten er samstemt om at det finnes to situasjoner hvor det må gjøres unntak fra utgangspunktet om at ensidig grenseoverskridende datatilgang er suverenitetskrenkende. Dette er for det første i tilfeller hvor dataene er offentlig tilgjengelige. Det er i dag enighet om at slik datatilgang er lovlig ikke bare etter Cybercrime-konvensjonen artikkel 32 litra a, The 2010 Arab Convention on Combating Information Technology Offences artikkel 40 og The 2011 COMESA Cyber Security Model Bill artikkel 49, men også i henhold til folkerettslig sedvanerett.[203]

Det andre tilfellet gjelder situasjoner hvor det ikke er mulig å finne dataenes lokalisasjon. Disse tilfellene refereres i teorien til som *«loss of location»* eller *«loss of knowledge of location»*. Europarådets Cybercrime-komité (T-CY) har om dette uttalt at territoriell suverenitet ikke krenkes i disse tilfeller fordi territorialprinsippet ikke kan gjøre seg gjeldende når man ikke vet hvilket territorium de er lagret på.[204] En slik forståelse synes også å være lagt til grunn i nasjonal praksis blant flere stater når de i sine nasjonale lover tillater sine myndigheter å skaffe grenseoverskridende tilgang til data uten samtykke fra den berørte staten i tilfeller hvor dataenes lokalisasjon er ukjent.[205]

Ulrich Sieber og Carl-Wendelin Neubert skriver om dette at et slikt synspunkt kan begrunnes i en antakelse om at serverstatens suverene interesser i å beskytte dataene er minimal eller ikke-eksisterende i *«loss of location»*-tilfeller:

> *«If data accessed by State A are stored on a system located in State B (randomly, due to sophisticated algorithms and dynamic data management systems following the allocation of free data storage space in the cloud, or due to re-routing of data through a transnational botnet in a concealment effort), then State B's relationship towards and legal interests in the protection of the data stored in its territory appear to be merely 'virtual'.»*[206]

Med andre ord begrunnes mangelen på territoriell suverenitet først og fremst i at forholdet mellom dataene og territoriet de lagret på er tilfeldig. For eksempel kan dette være når data

---

[203] Sieber & Neubert (2016) s. 259
[204] T-CY (2012) s. 27 punkt 134
[205] Sieber & Neubert (2016) s. 259
[206] Ibid. s. 260

bare passerer gjennom tilfeldig utvalgte TOR-servere for å unngå å bli sporet. Dessuten vil serverstatens suverene interesser i slike tilfeller bare være en antakelse, idet man ikke vet hvor dataene faktisk befinner seg. For det andre kan mangelen på territoriell suverenitet begrunnes i selve mangelen på kunnskap. En stat som ikke har kunnskap om at dataene befinner seg på deres territorium, kan lite trolig ha noen interesse i å beskytte dem.[207]

På den annen side kan det ikke hevdes at en suverenitetskrenkelse ikke har funnet sted bare fordi den berørte staten ikke har kunnskap om krenkelsen. Rent faktisk befinner datamaterialet seg på noens territorium når datatilgangen finner sted.[208] De uttalelser som er tilgjengelig fra stater i relasjon til suverenitetsspørsmålet, tar ikke hensyn til *«loss of location»* når de svarer at slik tilgang er ulovlig. Det kan således argumenteres for at suverenitetskrenkelser kan finne sted til tross for mangel på kunnskap.[209]

Uavhengig av hvilket standpunkt som tas, må det innvendes at slike tilfeller trolig ikke er et stort problem i praksis. Når verken etterforskende stat eller serverstaten vet hvor dataene befinner seg på handlingstidspunktet kan det vanskelig tenkes at noen vil påberope seg krenkelse. Når man i slike tilfeller dessuten ikke vet hvem en bistandsanmodning skal rettes til, er ikke samarbeid praktisk mulig. Ensidig grenseoverskridende datatilgang må på denne bakgrunn kunne anses akseptabelt.

9 Konklusjoner

9.1 Innledning

De rettskilder som ovenfor er undersøkt viser at en alminnelig tolkning av suverenitetsprinsippet innebærer et forbud mot ensidig grenseoverskridende datatilgang. To tredjedeler av statene som besvarte FNs undersøkelse om cyberkriminalitet, svarte at slik aktivitet er ulovlig uten særskilt hjemmel. Et stort antall av verdens stater har som følge av dette inngått detaljerte traktater i forsøk på å få til et bedre samarbeid i relasjon til grenseoverskridende digital bevisinnhenting. Utgangspunktet etter disse traktatene er at statene skal forholde seg til gitte samarbeidsprosedyrer, og at samtykke fra serverstaten er et vilkår for datatilgang.

---

[207] Sieber & Neubert (2016) s. 260
[208] Ibid. s. 255
[209] Sieber & Neubert (2016) s. 260, Koops & Goodwin (2014) s. 66

Det har i praksis vist seg at slike traktater ikke tilfredsstiller etterforskende myndigheters behov for effektivitet. Gjennomsnittlig responstid på bistandsanmodninger etter dagens system ligger på mellom seks og 24 måneder, i tillegg til at mange anmodninger avvises.[210]

Et slikt system holder ikke mål i relasjon til etterforsking av straffesaker. Samfunnet har et ansvar for å beskytte egne borgere fra kriminalitet. Skulle man ha ventet i opp til 24 måneder på klarsignal for datatilgang ville viktige bevis ha gått tapt, idet slike med dagens teknologi kan endres og slettes på bare millisekunder. Etterforsking av digitale bevis krever således snarlig inngripen. Gjerningspersoner som er under politiets etterforsking har dessuten krav på en rettferdig rettergang, herunder endelig avgjørelse innen rimelig tid, jf. Grunnloven § 95 og EMK artikkel 6, jf. menneskerettsloven § 3, jf. § 2.

På grunn av mangelen på et tilfredsstillende system under dagens regelverk har et økende antall stater vedtatt nasjonale lovbestemmelser som hjemler ensidig grenseoverskridende datatilgang, og det har i tillegg blitt inngått flere nye traktater. Felles for et flertall av disse traktatene og lovene, er at legitimeringen av ensidig inngripen er reservert for tilfeller der det enten er alminnelig enighet om at tilgang ikke er suverenitetskrenkende, herunder ved offentlig tilgjengelige data, data nedlastet av privatperson og i tilfeller hvor dataenes lokalisasjon er ukjent.

De nasjonale lovverkene er konstruert som subsidiære hjemler og etter minste inngreps prinsipp. Noen tillater bare ensidig tilgang i tilfeller hvor dataenes lokalisasjon er ukjent,[211] mens andre går lenger og tillater slik tilgang til tross for kjent lokalisasjon, under forutsetning av at serverstaten notifiseres etter inngrepet.[212] Det stilles gjennomgående krav om tilfelle av alvorlig kriminalitet og at dataene er nødvendig for å komme til bunns i etterforskningen. Lovhjemlene synes således å bygge på nødrettsbetraktninger.

Høyesterett kom i Tidal-saken til at ransakingen av materialet lagret på servere i USA ikke var i strid med suverenitetsprinsippet. En slik konklusjon harmonerer dårlig med den analyse som ovenfor er foretatt, og det kan stilles spørsmål ved Høyesteretts rettslige argumentasjon. I det følgende skal det klarlegges hvordan norsk rett forholder seg til problemet sammenlignet med den statspraksis som ovenfor er undersøkt. Dette vil skje gjennom en konfrontasjon av

---

[210] Sieber & Neubert (2016) s. 246
[211] Nederland, se kapittel 7.4
[212] Belgia, se kapittel 7.3

Tidal-saken. Avhandlingens hovedproblemstilling vil herunder besvares. Deretter vil det knyttes noen bemerkninger til folkerettslige konsekvenser av uhjemlet ensidig grenseoverskridende datatilgang, og noen bemerkninger *de lege ferenda* til hva som i denne sammenheng bør gjøres for norsk retts vedkommende.

9.2 Sammenligning og konfrontasjon

I Tidal-saken innleder Høyesterett sin rettskildeanalyse med å se på den internrettslige hjemmelen for ransaking.[213] Straffeprosessloven § 192 gir som vist i kapittel 3 hjemmel for ransaking. Det som kan ransakes er blant annet siktedes og andres *«oppbevaringssted»*. Etter bestemmelsens ordlyd tilsier dette alle fysiske lagringssteder. Ordlyden gir heller ingen begrensninger med hensyn til hvor bevisene befinner seg. Høyesterett uttaler om dette i Tidal-saken at *«[d]ette kan omfatte et datanettverk, herunder en server som befinner seg i utlandet»*.[214]

Dersom vilkårene i strpl. § 192 er oppfylt, gir § 199a ved ransaking av et datasystem også hjemmel for å *«pålegge enhver som har befatning med datasystemet å gi nødvendige opplysninger for å gi tilgang til datasystemet.»* På denne måten er politiet i en etterforskning der beviser befinner seg på en utenlandsk server sikret tilgang til materialet, uavhengig av hvilken stat materialet fysisk befinner seg i.

Etter norsk rett har politiet således full adgang til å ransake og beslaglegge data lagret på servere i utlandet. Det finnes heller ingen bestemmelser som gir regler om at slik folkerettslig uhjemlet tilgang til data må begrenses til tilfeller av alvorlig kriminalitet hvor det for eksempel er fare for etterforskingen ved opphold, eller om at den berørte staten må notifiseres etter inngrepet. En slik ransakingshjemmel er derfor betenkelig i forhold til folkeretten, og står i kontrast til den statspraksis som er presentert i den foregående analysen. I disse staters lovgivning er det som nevnt oppstilt strenge vilkår og rettssikkerhetsgarantier, herunder krav om alvorlig kriminalitet, nødvendighet og notifisering. Dette viser at statene anerkjenner at handlingen er suverenitetskrenkende, og at hjemmelen er vedtatt på bakgrunn av nødrettsbetraktninger.

---

[213] Kjennelsens avsnitt 24 flg.
[214] Kjennelsens avsnitt 27

Videre i sin analyse tar Høyesterett for seg Cybercrime-konvensjonen.[215] Førstvoterende uttaler at artikkel 29 følgende pålegger statene å iverksette nærmere angitte tiltak for å bekjempe datakriminalitet, men at *«[k]onvensjonen fastsetter imidlertid bare minimumsforpliktelser for statene»*. Videre uttales at *«[i]ngen av konvensjonsbestemmelsene angår direkte et tilfelle som i saken her»*. En slik tolkning av konvensjonen er etter min oppfatning for kortfattet. Det kan i tillegg stilles spørsmål ved om den i det hele tatt er riktig.

Artiklene 29 til 34 fastsetter prosedyrer for gjensidig samarbeid om grenseoverskridende bevisinnhenting. Å følge disse prosedyrene når det er behov for nettopp slik grenseoverskridende bevisinnhenting må etter konvensjonens system kunne anses som en minimumsforpliktelse for medlemsstatene.

Tilfellet i Tidal-saken gjaldt tilgang til data som ikke var offentlig tilgjengelig, og som var skaffet til veie gjennom tvangsmessig tilgang til selskapets datamaskiner. Med andre ord var tilfellet ikke omfattet av konvensjonens artikkel 32 idet informasjonen ikke var offentlig tilgjengelig, og tilgangen var skaffet gjennom ransaking og ikke frivillig samtykke. En antitetisk tolking av bestemmelsen tilsier da at samarbeidsprosedyrene i artikkel 29 følgende skulle ha vært fulgt. Når en slik tolkning ikke legges til grunn blir resultatet at statene fritt kan velge om de vil følge konvensjonens prosedyrer eller ikke. I så tilfelle forfeiles konvensjonens formål.

Analysen av artikkel 32 i avhandlingens kapittel 5.3 viste at det i tilfeller hvor datamaterialets lokalisasjon er usikker eller ukjent, er opp til medlemsstatene selv å bestemme legitimiteten av et grenseoverskridende søk. Avhandlingens kapittel 8.2 viser at slik ensidig grenseoverskridende datatilgang i slike tilfeller anses lovlig. I Tidal-saken var det imidlertid kjent at materialet var lagret på servere i USA. Dette utgjør nok et argument for at samarbeidsprosedyrene skulle ha vært fulgt.

Videre går Høyesterett over til å diskutere anerkjente begrensninger i folkeretten, herunder suverenitetsprinsippet.[216] Som det er redegjort for ovenfor i kapittel 3, uttalte Høyesterett om dette at utgangspunktet er at ingen stat kan anvende tvangsmidler på en annen stats territorium uten samtykke fra vedkommende stat. Til tross for dette fant førstvoterende at dette gir

[215] Kjennelsens avsnitt 35-36
[216] Kjennelsens avsnitt 40

mindre veiledning når det gjelder ransaking og beslag av elektronisk lagret materiale som kan lagres *«i skyen»*.

Ransaking er etter straffeprosessloven et tvangsmiddel. Hovedregelen om at ransaking ikke uhjemlet kan foretas på en annen stats territorium, endrer ikke karakter alene av den grunn at ransakingen skjer på et datasystem. Ransaking av datasystemer krever samme hjemmelsgrunnlag som fysisk ransaking, og regelen bør således være den samme for begge.

Høyesterett bruker videre som argument at det ikke har vært problematisert om det kan gjennomføres kommunikasjonskontroll selv om den ene samtalepartneren viser seg å være i et annet land, og tilsvarende at det kan gis pålegg om utlevering av bevis i medhold av strpl. § 210 også dersom tingen befinner seg utenlands.[217]

Her må imidlertid innvendes at det i tilknytning til disse spørsmål er inngått traktater som blant annet bestemmer at det i noen tilfeller av kommunikasjonskontroll i utlandet ikke kreves at den berørte staten samtykker eller varsles om handlingen. Se om dette EUs konvensjon av 29. mai 2000 om gjensidig hjelp i straffesaker mellom Den europeiske unions medlemsstater med relevante tilleggsprotokoller.[218] Konvensjonens artikkel 20 regulerer situasjoner der en stat gjennomfører kommunikasjonskontroll av personer som befinner seg på en annen stats territorium. Bestemmelsen oppstiller en plikt til å varsle fremmed stat om kontrollen, men statene kan etter artikkel 20 nr. 7 avgi erklæring om at slikt varsel ikke er nødvendig.

At en slik avtaleregulering er etablert, tilsier at ensidig kommunikasjonskontroll av personer på fremmed territorium er suverenitetskrenkende, men at man i visse tilfeller likevel godtar det. En slik aksept for ensidig grenseoverskridende datatilgang finnes i dag kun for tilfeller av offentlig tilgjengelige data og der eieren av data frivillig har samtykket, jf. Cybercrime-konvensjonen artikkel 32. Utenom slike situasjoner krever konvensjonen at samarbeidsprosedyrene følges. Situasjonen blir således noe annerledes enn her, og kan ikke brukes som et direkte argument for en legitimering av ensidig datatilgang.

Høyesterett går deretter over til norsk praksis.[219] Det fantes før Tidal-saken ingen avgjørelser fra Høyesterett som kunne belyse spørsmålet. Høyesterett viser til NOU 1997:15 om

---

[217] Kjennelsens avsnitt 46
[218] 2000-konvensjonen
[219] Kjennelsens avsnitt 43 flg.

etterforskingsmetoder for bekjempelse av kriminalitet, og antar at det synspunkt som i den er lagt til grunn, har blitt fulgt i senere tid. I utredningen drøfter metodeutvalget lovligheten av ransaking av datamaskiner. De påpeker at det i slike situasjoner hyppig vil *«forekomme at man står i en situasjon hvor selve dataene er lagret fysisk på et annet sted enn der det ransakes»*. I den forbindelse *«kan det oppstå spørsmål om ikke politiets ransaking må regnes for å ha skjedd på et område som er underlagt et annet lands jurisdiksjon».* Det påpekes at en slik handling vil kunne være ulovlig i det land den foretas, og at slike handlinger tilligger det aktuelle lands rettshåndhevende myndigheter å utføre.

Metodeutvalget viser videre til at det på tidspunktet da utredningen ble skrevet, ble arbeidet internasjonalt med å løse denne typen problemstillinger og at *«inntil en slik konvensjon foreligger, må politi/påtalemyndighet utvise særdeles stor grad av forsiktighet ved ransaking i nettverk som spenner over flere land. I det øyeblikk man blir klar over at ransakingen har «passert» en landegrense, må den avsluttes og politiet i vedkommende land kontaktes»*. De oppsummerer at adgangen til å foreta ransaking i andre land *«selvsagt»* er undergitt folkerettslige begrensninger og i utgangspunktet er ulovlig dersom den ikke er hjemlet i særskilt avtale med vedkommende lands kompetente myndigheter. Et slikt synspunkt harmonerer godt med de rettskilder som er undersøkt i kapitlene ovenfor.

Det metodeutvalget deretter legger til grunn, og som også legges til grunn av Høyesterett i Tidal-saken, er at det problematiske er hvor grensen skal trekkes mellom hva som er å anse som ransaking i Norge og hva som er ransaking i utlandet. Det uttales at *«utgangspunktet [må] være at det dreier seg om ransaking i Norge når tilgang til dataene oppnås fra en terminal som befinner seg i Norge»*.[220] Utvalget sammenligner dette med reglene om vitneplikt og utlevering, som ikke avhenger av hvor de aktuelle opplysningene er lagret. Dette tilsier at så lenge politiet i Norge gjennom tvangsmidler kan skaffe materialet, så anses etterforskingen utelukkende å foregå på norsk territorium, dette til tross for om materialet fysisk er lagret på utenlandsk territorium. Dette harmonerer dårlig med slik rettstilstanden fremstår i dag.

[220] NOU 1997:15 punkt 4.2.1.3 og Tidal-kjennelsen avsnitt 45

For det første er det anerkjent i folkeretten at fysisk tilstedeværelse på den berørte statens territorium ikke kan stilles som et vilkår for suverenitetskrenkelse. Ulrich Sieber og Carl-Wendelin Neubert konstaterer i denne forbindelse at

> *«[t]he argument that the investigating State's agents perform their activity from within the confines of their home country and themselves never personally enter foreign territory also fails to refute the infringement of sovereignty caused by online criminal investigations of computer systems located in foreign territory. Public international law deems it irrelevant that a law enforcement officer conducting an investigation is not physically located on foreign soil ...»* [221]

For det andre ble utredningen skrevet i en tid hvor det rådet stor usikkerhet knyttet til rettstilstanden i relasjon til grenseoverskridende datatilgang. Bruken av skytjenester var på langt nær slik den er i dag. I 1997 fantes ikke smarttelefoner, nettbrett og applikasjoner. Samfunnet har gjennomgått en teknologisk revolusjon siden utredningen ble skrevet og rettsutviklingen har kommet langt. En utredning som denne kan med andre ord ikke anses å ha noen bemerkelsesverdig rettskildeverdi i dag. Det er i nyere tid etablert en rekke internasjonale konvensjoner som regulerer nettopp det spørsmål utvalget drøfter. I lys av samfunnsutviklingen de siste 20 årene og folkeretten for øvrig bør disse veie tyngst. En slik slutning harmonerer dessuten best med straffeprosessloven § 4.

Cybercrime-konvensjonen artikkel 32 bokstav b regulerer som nevnt tilfeller hvor det er innhentet lovlig og frivillig samtykke fra eieren av dataene. Som vist i kapittel 5.3 tilsier en antitetisk tolkning av bestemmelsen at i tilfeller hvor slikt samtykke ikke foreligger, skal samarbeidsprosedyrene i konvensjonen følges. Når Norge har ratifisert en konvensjon som åpenlyst bygger på det grunnlag at ensidig grenseoverskridende datatilgang er ulovlig og derfor må reguleres ved avtale, taler det sterkt i retning mot at ransaking ikke kan anses for å skje i Norge bare fordi dataene gjennom tvangsmidler kan oppnås fra en datamaskin i Norge. Dette begrunnes i naturen av dagens teknologi; hele problemet med grenseoverskridende datatilgang ligger jo nettopp i det faktum at man kan oppnå tilgang til data i et annet land fra eget territorium.

---

[221] Sieber & Neubert (2016) s. 257 med videre henvisninger

Som Høyesterett er inne på i avsnitt 30 i Tidal-saken er utgangspunktet at tvangsmidler bare kan brukes innenfor norske myndigheters jurisdiksjon, og straffeprosessloven gjelder som nevnt med de begrensninger som følger av folkeretten, jf. strpl. § 4. Dersom grenseoverskridende datatilgang er i strid med suverenitetsprinsippet innebærer dette at slik datatilgang faller utenfor ransakingshjemmelen i strpl. § 192. Norge ligger med andre ord langt bak resten av verden i lovgivningsarbeidet knyttet til grenseoverskridende datatilgang.

Høyesterett ser etter dette hen til praksis fra andre land, herunder vises det til en kjennelse fra dansk Højesteret som tillot ensidig grenseoverskridende tilgang og en svensk utredning som inntok motsatt standpunkt.[222] Videre vises det til internasjonal praksis, herunder rapporter fra ekspertgrupper i Europarådet og en arbeidsgruppe under EU-kommisjonen. Disse viste at det er en utbredt praksis for at etterforskende myndigheter ensidig skaffer tilgang til data som er lagret i utlandet.[223]

At en slik praksis finnes, er imidlertid også fastslått i FNs undersøkelse (UNODC) som det er redegjort for ovenfor i avhandlingens kapittel 7.9. Det som i den også er fastslått, er at to tredjedeler av statene som svarte, likevel anser slik tilgang som folkerettsstridig. Grunnen til at det er en praksis for ensidig grenseoverskridende datatilgang er med andre ord ikke fordi den anses som lovlig, men fordi det fortsatt mangler et effektivt regelverk. Det finnes i dag ingen folkerettslig sedvanerett tilknyttet problemet. Statspraksis i relasjon til dette har således begrenset rettskildemessig vekt, særlig må dette gjelde når det ikke finnes noen opinio juris rundt praksisen.

Av internasjonal litteratur begrenser Høyesterett seg til å vise til «Tallin Manual 2.0 on the International Law Applicable to Cyber Operations» fra 2017. Det Høyesterett fremhever fra denne er at det *«kan være vanskelig å avgjøre jurisdiksjonsspørsmålet «in the cyber context»* og at ekspertene i favør av å godta territorial jurisdiksjon blant annet legger vekt på om materialet *«is meant to be accessible from the State concerned»*.[224] Som vist i avhandlingens kapittel 8 foregår det i dag en diskusjon i litteraturen blant jurister internasjonalt. Det finnes ulike meninger, og blant noen av forfatterne legges argumenter som dette til grunn. Til tross for at det finnes slike meninger, finnes det likevel et stort antall forfattere som mener det

[222] Kjennelsens avsnitt 50 flg.
[223] Kjennelsens avsnitt 52 flg.
[224] Kjennelsens avsnitt 56

motsatte. Skal en slik mening tillegges vekt i utredningen av et juridisk spørsmål, må det i alle fall kreves at den samsvarer med andre autoritative og vektige kilder.

Høyesterett oppsummerer etter dette med å uttale at gjennomgangen viser at det ikke er etablert noen folkerettslig sedvane på området. Høyesterett anser det likevel som interessant at mange land i praksis *«synes å godta en slik ransaking som i saken her»* og at det ikke er opplyst om noen mellomstatlige reaksjoner knyttet til at et lands myndigheter gjennom tvangsmidler overfor rettssubjekter på eget territorium har fått tilgang til materiale lagret i en annen stat.[225]

Høyesteretts rettskildeanalyse i Tidal-saken bærer preg av at viktige rettskilder er unnlatt behandlet, eller kun er behandlet overfladisk. Dersom de kilder som i kapitlene 3 til 8 ovenfor hadde vært analysert grundig, er det nærliggende å tro at Høyesterett hadde blitt tvunget til å konkludere med at ransakingen av Tidals datasystemer var i strid med suverenitetsprinsippet. Høyesterett synes således å ha unngått viktige kilder for å unngå å komme til motsatt resultat.

Å konsekvent unngå de rettskilder som peker i motsatt retning av ønsket konklusjon fremstår som betenkelig. En mer akseptabel fremgangsmåte ville ha vært å anerkjenne at den norske hjemmelen for ransaking er problematisk i relasjon til folkeretten, og i stedet gjøre unntak av hensyn til en effektiv og praktikabel straffeforfølgning og rettssikkerhet. Dette er imidlertid ikke et spørsmål for Høyesterett å ta stilling til, men en lovgiveroppgave. Domstolen er likevel pliktig til å ta stilling til de rettsspørsmål som bringes inn for den, og Høyesteretts konklusjon kan således anses som den beste løsning i Tidal-saken.

Dersom Høyesterett hadde konkludert med at ransaking og beslag i Tidals datasystemer hadde vært i strid med folkeretten, ville det ha fått enorme konsekvenser for politiets straffesaksbehandling. Som nevnt i kapittel 1.1 er det i 85 % av dagens straffesaker behov for elektroniske bevis, og to tredeler av disse er lagret på servere i utlandet. Med andre ord ville en motsatt konklusjon i Tidal-saken ha satt en stopper for innhenting av digitale bevis i mer enn halvparten av politiets etterforskninger. Hensynet til samfunns- og rettssikkerhet må klart nok veie tyngst i denne sammenheng. I et rettspolitisk perspektiv levnes det således liten tvil rundt riktigheten av Høyesteretts konklusjon, selv om den må anses å stride mot folkeretten.

---

[225] Kjennelsens avsnitt 57 flg.

Konklusjonen på avhandlingens hovedproblemstilling er at Høyesteretts kjennelse i Tidal-saken ikke er i samsvar med folkeretten.

9.3 Konsekvenser av uhjemlet grenseoverskridende datatilgang

Som vist i den foregående analysen, kan det påvises en praksis for bruk av ensidig grenseoverskridende datatilgang som etterforskningsmetode til tross for en bred oppfatning om at slik aktivitet er ulovlig etter folkeretten.

Reaksjonene som risikeres fra andre stater ved slik uhjemlet aktivitet kan ikke generaliseres, men vil kunne bero på omstendighetene rundt og alvorligheten av inngrepet, samt tidligere konflikter mellom de aktuelle statene.[226]

Jan-Jaap Oerlemans viser til at stater trolig ikke er villig til å destabilisere verdensordenen ved å gå til væpnet angrep som ikke involverer *«'coercive' activities. Examples of coercive activities include (1) physical sabotage, (2) assassinations, and (3) abductions of individuals on another State's territory ...»*[227] Det er med andre ord lite trolig at ekstraterritoriell myndighetsutøvelse innenfor cyberdomenet vil kunne føre til en suverenitetskrenkelse som stiger til det nivået at stater vil havne i en væpnet konflikt. De reaksjoner som fremstår som sannsynlige er at den berørte stat vil kreve en unnskyldning med en innrømmelse av den folkerettsstridige handlingen og et løfte om ikke å utføre slik uhjemlet aktivitet igjen i fremtiden.[228]

Høyesterett påpekte i Tidal-saken at *«[d]et er heller ikke opplyst noe om mellomstatlige reaksjoner knyttet til at et lands myndigheter gjennom tvangsmidler overfor rettssubjekter på eget territorium har fått tilgang til materiale lagret i en annen stat.»* Det faktum at væpnet konflikt eller andre alvorlige reaksjoner er lite trolig som konsekvens av uhjemlet grenseoverskridende datatilgang kan likevel ikke tjene som argument for at slik aktivitet kan foretas. En slik oppførsel harmonerer dårlig med det samarbeidet som i dag utøves i verdenssamfunnet.

[226] Oerlemans (2017) s. 295
[227] Ibid. s. 295 med videre henvisninger
[228] Ibid. s. 296

9.4 Avsluttende bemerkninger *de lege ferenda*

Politiets behov for grenseoverskridende tilgang til data som er lagret via skytjenester er stort, og vil trolig fortsette å øke i omfang.[229] Andre land synes å prioritere strategier for bekjempelse av kriminalitet i det digitale rom høyt. Dette *«rommet»* er i sin natur internasjonalt, og samarbeid med andre land er således helt sentralt i kampen mot datakriminalitet.[230]

På bakgrunn av dette og den rettskildeanalyse som ovenfor er foretatt, foreligger en sterk oppfordring til lovgivende myndigheter i Norge om å ta grep. Når en stor del av øvrige stater i verden streber med å få på plass nasjonale lovhjemler og internasjonale avtaler fordi dagens ordning ikke holder mål, er det lite trolig at det vil aksepteres at Norge fortsetter med uhjemlet ransaking av servere plassert i utlandet. En slik opptreden gjenspeiler i liten grad den viktige rollen Norge har i verdenssamfunnet i dag. Norge er ansett som en av verdens sterkeste rettsstater, og bør av den grunn gå foran som et av foregangslandene i bekjempelsen av datakriminalitet.[231]

For det første bør det komme på plass en ny straffeprosessuell lovhjemmel for innhenting av elektroniske bevis som tar hensyn til dagens teknologi og folkeretten ved å oppstille strenge vilkår for ensidig grenseoverskridende datatilgang. På den måten vil Norge i likhet med de øvrige staters praksis som er undersøkt i kapittel 7 ovenfor, anerkjenne at slike handlinger er problematiske i relasjon til folkeretten og samtidig sikre serverstatens rettigheter i størst mulig grad.

For det andre bør Norge, for å redusere de situasjoner hvor det er behov for ensidig datatilgang, ta sikte på å ta del i den avtalen som i dag blir fremforhandlet mellom USA og EU. Avtalen er en viktig brikke i den internasjonale rettsutviklingen på området, og vil gi en vesentlig lettelse for det norske politiets arbeid ved at det kan innhentes informasjon direkte fra tjenesteleverandører i USA og EU. Det er nærliggende å tro at også flere stater i fremtiden vil følge etter og vedta lignende traktater, da naturen av dagens teknologi ikke tillater den saksbehandlingstid som kreves for å innhente samtykke fra serverstatens myndigheter.

---

[229] Politidirektoratet (2015) s. 143
[230] Ibid. s. 14 og 142
[231] Ibid. s. 14

Kildeliste

Lovregister

Norsk lovgivning

Grunnloven	17. mai 1814, Kongeriket Norges Grunnlov
Straffeprosessloven	Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker
Menneskerettsloven	Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett
Straffeloven	Lov 20. mai 2005 nr. 28 om straff

Andre lands lovgivning

The Cloud Act	The Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 1625, 115th Cong. div. V (2018)
BCCP	Criminal Procedure Code of the Kingdom of Belgium, 1808
DCCP	Dutch Code of Criminal Procedure, 15. januar 1921
England	The Crime (Overseas Production Orders) Act, 12. februar 2019
Portugal	The Portuguese law on Cybercrime, Law no. 109/2009, 15. september 2009

Lovgivning i EU

GDPR	The General Data Protection Regulation (EU) 2016/679 (GDPR), 4. mai 2016

Traktater

ICJ-statuttene (1945)	Statute of the International Court of Justice, 24. oktober 1945
EMK	Convention for the Protection of Human Rights and Fundamental Freedoms, Roma 4. november 1950
Wien-konvensjonen (1969)	Vienna Convention on the Law of Treaties, 23. mai 1969
2000-konvensjonen	EUs konvensjon av 29. mai 2000 om gjensidig hjelp i straffesaker mellom Den europeiske unions medlemsstater
Cybercrime-konvensjonen	Europarådets konvensjon om datakriminalitet – ETS nr. 185, Budapest, 23. november 2001
The 2010 Arab Convention	Arab Convention on Combating Technology Offences, Kairo, 21. desember 2010
COMESA	The Common Market for Eastern and Southern Africa Cyber Security Model Bill, oktober 2011
Cloud Act Agreement	Agreement between the Government of the United Kingdom of Great Britain and Nothern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington, 3. oktober 2019

Forarbeider

NOU 1997:15	Etterforskingsmetoder for bekjempelse av kriminalitet
NOU 2003:27	Lovtiltak mot datakriminalitet
Ot.prp. nr. 64 (1998-1999)	Om lov om endringer i straffeprosessloven og straffeloven m v (etterforskningsmetoder m v)

Rettspraksis

Norsk rettspraksis

HR-2019-610-A	Tidal

Internasjonal rettspraksis

France v. Turkey (1927)	The Case of the S.S. «Lotus» (France v. Turkey), September 7th 1927, PCIJ, Publications of the Permanent Court of Justice, Series A. – No. 10, 7. September 1927
America v. Canada (1938)	Trail Smelter (United States of America v. Canada) (1938/41) 3 RIAA, 1905
Nordsjøsaken (1969)	North Sea Continental Shelf, ICJ Reports 1969, s. 3
United Kingdom v. Iceland (1974)	Fisheries Jurisdiction (United Kingdom v. Iceland), ICJ Reports 1974, s. 3

Utenlandsk rettspraksis

Belgian Yahoo Case (2015)	Belgisk Høyesterett, 1. desember 2015, Nr. P.13.2082.N
Microsoft Ireland Case (2018)	United States v. Microsoft Corporation (*Microsoft Ireland*), No. 17-2, (17. april 2018)

Litteratur

Bertheussen (2000)	Bertheussen, Svein, *Internett i teori og praksis*, EDB-kunnskap, 2000
Cassese (2005)	Cassese, Antionio, *International Law,* Oxford University Press, 2. utgave, 2005

Castberg (1948)	Castberg, Frede, *Folkerett,* 2. utgave, Oslo 1948
Crawford (2012)	Crawford, James, *Brownlie's Principles of Public International Law,* Oxford University Press, 2012
Daskal (2018)	Daskal, Jennifer, «Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0», *Stanford Law Review Online*, Volume 71, 2018, s. 9-16
Fredriksen (2018)	Fredriksen, Steinar, *Innføring i straffeprosess*, Gyldendal, 4. utgave, 2018
Kjelby (2019)	Kjelby, Gert Johan, *Påtalerett*, Cappelen Damm Akademisk, 2. utgave, 2019
Koops & Goodwin (2014)	Koops, Bert-Jaap og Goodwin, Morag, *Cyberspace, the cloud, and cross-border criminal investigation: The limits and possibilities of international law,* Tilburg University, 2014
Lowe (2007)	Vaughan, Lowe, *International Law*, Oxford University Press, 2007
Oerlemans (2017)	Oerlemans, Jan-Jaap, *Investigating Cybercrime,* Amsterdam University Press, 2017
Osula (2015)	Osula, Anna-Maria, «Transborder access and territorial sovereignty», *Computer law & Security review 31,* 2015, s. 719-735
Rui (2009)	Rui, Jon Petter, «Komparasjon innen strafferett og -prosess», *Tidsskrift for strafferett nr. 4, 2009* s. 434-468, (lastet ned 29. januar 2020)
Rui (2019)	Rui, Jon Petter, «Høyesterett i «skyen», *Lov og Rett nr. 5, vol. 58, 2019 s. 261-262*

Ruud & Ulfstein (2018) — Ruud, Morten og Ulfstein, Geir, *Folkerett*, Universitetsforlaget, 5. utgave, 2018

Schjølberg (2017) — Schjølberg, Stein, *Cyberkriminalitet,* Universitetsforlaget, 2017

Sieber & Neubert (2016) — Sieber, Ulrich og Neubert, Carl-Wendelin, «Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty», *Max Planck Yearbook of United Nations Law,* 2016 s. 241-321

Skjold (2019) — Skjold, Jørgen S., «Suverenitet, jurisdiksjon og beslag i informasjon på server i utlandet – En kommentar til Høyesteretts kjennelse i Tidal-saken og Ruis kritikk», *Lov og Rett nr. 10,* vol. 58, 2019 s. 617-639

Smith & Browne (2019) — Smith, Brad og Browne, Carol Ann, *Tools and weapons: The promise and the peril of the digital age,* Penguin Press, 2019

Sunde (2002) — Sunde Inger Marie, «Convention on Cybercrime», *Tidsskrift for strafferett nr. 1,* 2002 s. 89-99

Nettdokumenter

Singsaas (2016) — Singsaas, Frode, *Hvilke skylagringstjeneste er best?*, 11.02.16, https://www.aftenposten.no/digital/i/b58Rjl/hvilken-skylagringstjeneste-er-best, (sist besøkt 10.02.20)

Beck-Olsen (2019) — Beck-Olsen, Aksel, *Cloud Act kan by på utfordringer for europeiske selskaper*, https://www.cw.no/artikkel/debatt/cloud-act-kan-pa-utfordringer-europeiske-selskaper (sist besøkt 14.04.20)

Covington & Burling LLP (2019) — Trisha Anderson, Alexander Berengaut, Jim Garland, Marty Hansen og Lisa Peets, «U.S. and U.K. Sign

CLOUD Act Agreement», 11.10.19 https://www.insideprivacy.com/surveillance-law-enforcement-access/10167/, (sist besøkt 23.05.20)

Datatilsynet (2018) — Datatilsynet, *Skytjenester*, 23.06.18 https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/skytjenester/, (sist besøkt 10.02.20)

Durovic-Andic (2019) — Durovic-Andic, Marina, *Konstantinopel*, 11.11.19, https://snl.no/Konstantinopel, (sist besøkt 24.03.20)

Dustin (2018) — Dustin, *Cloud Act: den nye loven i skyggen av GDPR*, 09.08.18 https://www.dustin.no/tjenester/kunnskapsbanken/archive/cloud-act-den-nye-loven-i-skyggen-av-gdpr/ (sist besøkt 12.04.20)

EU (2018) — «What is GDPR, the EU's new data protection law?», https://gdpr.eu/what-is-gdpr/ (sist besøkt 31.05.20)

Europakommisjonen (2018) — Europakommisjonen, «Proposal for a regulation of the european parliament and of the council on European Production and Presevation Orders for electronic evidence in criminal matters», 17. april 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN (sist besøkt 27.05.20)

Europakommisjonen (05.02.2019) — Europakommisjonen, «Recommandation for a Council Decision: Authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters», 05.02.19 https://ec.europa.eu/info/sites/info/files/recommendation

_council_decision_eu_us_e-evidence.pdf, (sist besøkt 22.05.20)

Europakommisjonen (2019) Europakommisjonen, «Internal EU rules: Proposal on e-evidence», https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en#internaleurulesproposaloneevidence (sist besøkt 28.05.20)

Europarådet (2001) Europarådet, *Explanatory Report to the Convention on Cybercrime*, 23.11.01, https://rm.coe.int/16800cce5b (sist besøkt 14.04.20)

Europarådet (2020) Europarådet, *Chart of signatures and ratifications of Treaty 185*, 11.05.20 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=YHHDQpOY, (sist besøkt 04.03.20)

FN-sambandet (2019) FN-sambandet, «Folkerett», 26.03.19 https://www.fn.no/Tema/Konflikt-og-fred/Folkerett, (sist besøkt 13.02.20)

Governments of Netherlands (2019) Goverments of Netherlands, *New law to help fight computer crime*, 28.02.19 https://www.government.nl/latest/news/2019/02/28/new-law-to-help-fight-computer-crime, (sist besøkt 07.04.20)

L'Ecluse & D'hulst (2016) L'Ecluse, Peter og D'hulst, Thibaut, *Belgium: Supreme Court Condemns Yahoo For Failure To Cooperate With Belgian Law Enforcement Officials*, 11.01.16 https://www.mondaq.com/CorporateCommercial-Law/456514/Supreme-Court-Condemns-Yahoo-For-Failure-To-Cooperate-With-Belgian-Law-Enforcement-Officials, (sist besøkt 08.04.20)

Liseter (2019)	Liseter, Ivar M., *server*, 06.12.19 https://snl.no/server, (sist besøkt 10.02.20)
Lysneutvalget (2015)	Det kongelige utenriksdepartementet, «Folkerettslige rammer for grenseoverskridende informasjonsinnhenting», 29.05.15 https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/2.pdf, (sist besøkt 30.03.20)
Politidirektoratet (2015)	Politidirektoratet, «Overordnet nasjonal strategi for bekjempelse av datakriminalitet (Datakrimstrategien)», 12. mai 2015, https://www.regjeringen.no/contentassets/4d2ba37bf2ae4cc9ac39afdf20a2f41b/datakrimstrategi_2015.pdf (sist besøkt 01.06.20)
Politiet (2019)	Politiet, Kripos, «Seksuell utnyttelse av barn og unge over internett», mars 2019 https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/seksuelle-overgrep-mot-barn/seksuell-utnyttelse-av-barn-over-internett.pdf, (sist besøkt 26.05.20)
Skarning (2019)	Skarning, Nicolay, *«Personvern (GDPR) på arbeidsplassen»*, 23.11.19 https://www.jusstorget.no/personvern-gdpr-pa-arbeidsplassen/ (sist besøkt 30.05.20)
Skodvin (2014)	Skodvin, Knut Einar, *Territorialprinsippet – folkerett*, 21.03.14 https://snl.no/territorialprinsippet_-_folkerett, (sist besøkt 10.04.20)
Sander (2019)	Sander, Kjetil, *Nettverksserver (server, også kalt tjener)*, 19.11.19 https://estudie.no/nettverksserver/, (sist besøkt 10.02.20)

Simmons + Simmons (2019)	Simmons + Simmons, *Pioneering Dutch Computer Crime Act III entered into force*, 01.03.19 https://www.simmons-simmons.com/en/publications/ck0bi70lg7kew0b94qi4inld1/280219-pioneering-dutch-computer-crime-act-iii-entered-into-force, (sist besøkt 07.04.20)
T-CY	https://www.coe.int/en/web/cybercrime/tcy
T-CY (2012)	Cybercrime Convention Committee (T-CY) Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, «Transborder access and jurisdiction: What are the options?» https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8 (sist besøkt 12.04.20)
T-CY guidance note # 3 (2014)	Cybercrime Convention Committee (T-CY), *T-CY Guidance note # 3 Transborder access to data (Article 32)*, 02.03.12.14 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a, (sist besøkt 01.04.20)
The Guardian (2010)	Halliday, Josh, *Suspected Bredolab worm mastermind arrested in Armenia*, 26.10.10 https://www.theguardian.com/technology/2010/oct/26/bredolab-worm-suspect-arrested-armenia, (sist besøkt 07.04.20)
Thomson m.fl. (2019)	Thomson Charles, Ludlam Joanna, Peddie Jonathan, Grimmer Tristan, Garfield Henry og Gesinde Yindi, «UK Introduces Crime (Overseas Production Orders) Act 2019 – Extension of the SFO's Evidence Gathering Powers», 26.06.19, https://globalcompliancenews.com/uk-introduces-crime-

overseas-production-orders-act-2019-extension-sfo-evidence-gathering-powers-20190506/ (sist besøkt 20.05.20)

Thon (2016) — Roar Thon, «Dette er et ran!», Sikkerhetsbloggen, Nasjonal sikkerhetsmyndighet (NSM), 1. juli 2016, https://www.nsm.stat.no/blogg/dette-er-et-ran/ (sist besøkt 27.05.20)

US Congress (2017-2018) — 115th Congress, *H.R.4943 – CLOUD Act*, https://www.congress.gov/bill/115th-congress/house-bill/4943 (sist besøkt 14.04.20)

UNODC (2013) — United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-CRP05/Comprehensive_study_on_cybercrime.pdf side ix (sist besøkt 26.02.20)