Digital bevisinnhenting utenfor Norge

En vurdering av handlingsrommet til å innhente digitale bevis lagret i utlandet gjennom tvangshandlinger på norsk territorium

Kandidatnummer: 52

Antall ord: 14553

JUS399 Masteroppgave

Det juridiske fakultet

UNIVERSITETET I BERGEN

10. mai 2024

Innholdsfortegnelse

1 Innledning

1.1 Problemstilling og aktualitet

Denne oppgaven vurderer hvilket handlingsrom norsk politi har til å innhente digitale bevis lagret utenfor Norge, ved bruk av norske tvangsmidler i utlandet uten å samarbeide med lokale myndigheter i andre jurisdiksjoner. Det sentrale spørsmålet er hvilket handlingsrom norske myndigheter har når informasjonen en har tvangshjemmel til etter norsk lov er lagret på servere i utlandet, samtidig som informasjonen er tilgjengelig fra Norge.

Kartlegging av tilgangen til innhenting av digitale bevis på tvers av landegrenser er et dagsaktuelt tema som blir viktigere med økt digitalisering. Etter hvert som kriminelle tar i bruk digitale løsninger er det naturlig at bevis for alminnelige forbrytelser som for eksempel salg av narkotika, bedrageri og seksuelle overgrep også blir digitale.[1] Tidligere kunne politiet følge kriminelles kommunikasjon ved å lese brev eller overhøre samtaler. Nå er digitale plattformer som sosiale medier og skylagringstjenester kilde til sentrale bevis som samtalelogger, søkehistorikk, trafikkdata og personopplysninger. Dersom viktige bevis enkelt kan innhentes digitalt, kan tilgang til digitale plattformer bli et sentralt verktøy for politiet i etterforskningen av kriminalitet.

Suverenitetsprinsippet innebærer at den enkelte nasjonalstat har retten til data som befinner seg i egen jurisdiksjon.[2] Det innebærer en risiko for at norske etterforskere kan mangle hjemmel til å innhente bevis lagret i utlandet. Derfor er det sentralt at den rettslige utviklingen følger digitaliseringen, og legger til rette for effektiv rettshåndhevelse.

Digitale bevis har andre egenskaper enn tradisjonelle analoge bevis. Analoge bevis er ofte knyttet til et bestemt sted, for eksempel ved at et regnskap oppbevares på et kontor eller vitner er bosatt i et område. I den digitale verden er ikke bevis like stedsbestemt. Noe av formålet og fordelen med internett, skylagring og sosiale medier er at hvem som helst kan bruke

[1] Økokrim. (2023) *Bedrageri - et samfunnsproblem*. Hentet fra: https://img8.custompublish.com/getfile.php/5180722.2528.qaamznluipnjsl/Bedrageri+-+et+samfunnsproblem.pdf?return=www.okokrim.no (Lest: 06.03.2024) s. 7

[2] Currie, R. J. (2017). *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?* Canadian Yearbook of International Law, 54, 63–97. Hentet fra: https://doi.org/10.1017/cyl.2017.7 (Lest: 05.03.2024) s. 69-74

tjenestene fra hvor som helst i verden. Data må også sikres mot dataangrep og skade ved blant annet sikkerhetskopiering. Dette oppnås ved at data lagres på flere steder og helst i ulike verdensdeler for å sikre at brukerens opplevelse er den samme uavhengig av hvor man befinner seg. Denne praksisen gjør, i motsetning til tradisjonelle fysiske bevis, som brev, at bevismateriale knyttet til en forbrytelse begått i Norge av norsk statsborger kan befinne seg lagret på ulike servere i mange forskjellige land.[3] I enkelte tilfeller er dataen så spredt at det er vanskelig å vite sikkert hvor dataen befinner seg. Dette fenomenet kalles «loss of location» (LOC).[4]

Norske myndigheter er avhengige av å innhente bevis som er lagret utenfor norsk territorium for å sikre effektiv etterforskning av straffbare forhold. Straffeprosessloven av 1981 inneholder hjemler som åpner for og kontrollerer hvordan data kan benyttes i etterforskning.[5] Digitale bevis kan være lagret hvor som helst i verden og da blir det i tillegg til straffeprosessloven også sentralt hvordan internasjonal rett stiller seg til grenseoverskridende datainnhenting, og om etablerte rettslige prinsipper, som suverenitet og jurisdiksjonslæren, setter grenser for effektiv rettshåndhevelse.

1.2 Jurisdiksjon og suverenitet setter rammer for nasjonalt handlingsrom

For at myndigheter skal kunne utøve tvang overfor noe eller noen må de ha jurisdiksjon til tvangsbruken. Det er tre typer jurisdiksjon som er aktuelle for å kartlegge det folkerettslige handlingsrommet for stater: Lovgivningsjurisdiksjon, strafferettslig jurisdiksjon og håndhevelsesjurisdiksjon. Lovgivningsjurisdiksjon gir regler for hvor og for hvem et lands lover gjelder, og strafferettslig jurisdiksjon gir regler for når en stat har jurisdiksjon over en straffbar handling. [6] Denne oppgaven omhandler håndhevelsesjurisdiksjon som er retten til å håndheve et lands lover ved hjelp av tvang. Dette innebærer etterforskning av kriminelle

[3] Pulse Technology. «Cloud Storage: Where is my data actually stored?», 26. juni 2023 Hentet fra: https://www.pulsetechnology.com/blog/cloud-storage-where-is-my-data-actually-stored (Lest: 06.03.2024)
[4] Economic Crime Division. (2010) *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?* Council of Europe. Hentet fra: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df (Lest: 06.03.2024) s. 5
[5] Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven/strpl.) §§ 192, 203 og 210
[6] Currie (2017) s. 69-74

forhold, gjennomføring av rettsak og ileggelse av straff. [7] Oppgaven forutsetter derfor at Norge har strafferettslig jurisdiksjon over forholdet som etterforskes.

Reglene for staters jurisdiksjon er både hjemlet av og begrenset av suverenitets- og territorialprinsippet. I Norge vurderte Høyesterett om digital bevisinnhenting på tvers av landegrenser krenker suverenitetsprinsippet i HR-2019-610-A (Tidal-saken). Rettsspørsmålet ble aktuelt i forbindelse med anken av kjennelsen som tillot tredjemannsransakelse av dataterminalene til Tidal Music AS (Tidal).[8] Høyesterett forkastet anken med begrunnelsen at ransakelse av data lagret på utenlandske servere ikke utgjorde brudd på folkeretten.[9] I kjølvannet av Tidal-saken har det oppstått diskusjon i det juridiske fagmiljøet. Kjennelsen møtte blant annet kritikk av professor Jon Petter Rui og politiadvokat Victoria Nygård. Kritikken kan så tvil om kjennelsens prejudikatverdi og rettstilstanden i Norge, med hensyn til å innhente digitale bevis på tvers av landegrenser.[10] Dette blir nærmere diskutert under punkt 3.3 og 3.4.

Spørsmålet om lovligheten av grenseoverskridende digital bevisinnhenting har ikke kommet på spissen fremfor internasjonale domstoler. Den tradisjonelle forståelsen av suverenitets- og territorialprinsippet fremgår av Lotus-saken, hvor den internasjonale domstolen (ICJ) stadfestet at en stat ikke har håndhevelsesjurisdiksjon utenfor eget territorium, med mindre det foreligger et eksplisitt unntak.[11] Det kan illustreres ved at dersom et brev om en bombetrussel i Norge blir sendt til Belgia, så er det ikke adgang for norsk politi til fysisk å ta seg inn i Belgia for å beslaglegge brevet.

Neste spørsmål er om retten til beslag endrer seg om brevet er en e-post som er lagret på en server i Belgia, men tilgjengelig fra en PC i Norge. Da er det ingen fysisk utøvelse av tvangsjurisdiksjon i Belgia. I voldgiftssaken Trail Smelter som omhandlet luftforurensning som drev over fra Canada til USA ble det fastslått at «no State has the right to use or permit

[7] Currie (2017) s. s. 69-74
[8] HR-2019-610-A avsnitt 1-3
[9] HR-2019-610-A avsnitt 71-72
[10] Rui, J. P. (2019). *Høyesterett i «skyen»*. Lov og rett, 58(5), 261–262. Hentet fra: https://doi.org/10.18261/issn.1504-3061-2019-05-01 (Lest: 19.02.2024); Nygård, V. S. (2021). *Politiets adgang til ransaking og beslag i data på utenlandske servere.* Tidsskrift for strafferett, 21(2), 140–160. Hentet fra: https://doi.org/10.18261/issn.0809-9537-2021-02-03 s. 140-141 (Lest: 20.02.2024); Skjold, J. S. (2019). *Suverenitet, jurisdiksjon og beslag i informasjon på server i utlandet: En kommentar til Høyesteretts kjennelse i Tidal-saken og Ruis kritikk.* Lov og rett, 58(10), 617–639. Hentet fra: https://doi.org/10.18261/issn.1504-3061-2019-10-03 (Lest: 20.02.2024)
[11] 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 section 45

the use of its territory in such a manner as to cause injury […] when the case is of serious consequence».[12] Sammenholdes Trail Smelter og Lotus gir sakene uttrykk for at myndighetsutøvelse kan krenke en annen stats suverenitet uten fysisk tilstedeværelse. Det avgjørende er om myndighetsutøvelsen påvirker et annet territorium og virkningen må anses å være alvorlig. Her gis det åpning for at ekstraterritoriell bevisinnhenting kan være i strid med suverenitetsprinsippet selv om etterforskningen ikke krever fysisk tilstedeværelse i annet lands jurisdiksjon. Dette er også premisset for oppgavens problemstilling.

1.3 Avgrensning og oppbygning av oppgaven

Oppgaven avgrenser mot tilfeller der beviset er innhentet ved samarbeid med lokale myndigheter eller frivillig overlevering fra tredjepart. Heller ikke offentlig informasjon lagret på servere i utlandet vil behandles. Begrunnelsen for dette er at oppgaven omhandler tvangsmidler utført av norske tjenestemenn på norsk jord, noe som forutsetter at bevisinnhenting må være gjennomført ved tvangsmiddel etter norsk lov.[13]

Videre forutsettes det at vilkårene for å bruke tvangsmidler som ransakelse, beslag ol. i straffeprosessloven er oppfylt fordi oppgavens fokus er på suverenitetsprinsippet, og ikke på vilkårene for å bruke tvangsmidler ved bruk av digitale bevis. Først avklares begreper og forskningsspørsmålet avgrenses ytterligere. Deretter gjøres en analyse av rettstilstanden i Norge i lys av straffeprosessloven, Tidal-saken og den etterfølgende kritikken. Videre vurderes rettstilstanden for digital bevisinnhenting i folkeretten. Avslutningsvis vil den norske og internasjonale rettstilstanden sammenlignes, og forfatteren kommer med noen rettspolitiske betraktninger knyttet til rettstilstanden.

[12] Trail Smelter (United States of America v. Canada) (1938/41) 3 RIAA, 1905. s. 1965
[13] NOU 1997: 15 Om etterforskingsmetoder for bekjempelse av kriminalitet — Delinnstilling II punkt 4.2.1.3

2 Begrepsavklaring

Det er vanskelig å ta stilling til digitalisering og digitale bevis uten litt bakgrunnsinformasjon om internett. Internett kan defineres som «et globalt system av datamaskiner, smarttelefoner og andre digitale enheter som er koblet sammen gjennom et kommunikasjonsnett».[14] Det er altså flere datasystemer som består av mange enheter som er koblet sammen til å kommunisere i et verdensomspennende omfang (WWW – World Wide Web). Internett gjør det mulig å utveksle data, men hadde i seg selv hatt liten verdi uten de ulike aktørene som tilbyr tjenester på nettet.[15] Internett benevnes også som «cyberspace», og når det begås kriminelle handlinger på nett kalles det «cybercrime». Kriminaliteten diskutert i denne oppgaven skiller seg fra «cybercrime» ettersom det ikke er handlinger som er begått på internett som er sentralt, men alle kriminelle handlinger som etterlater digitale bevis – herunder «cybercrime».

Tjenestene på nettet er mange, men i denne oppgaven er det mest aktuelle sosiale medier og tjenester som tilbyr skylagring. Sosiale medier er medieplattformer som tillater kommunikasjon og deling av informasjon på internett.[16] Noen av plattformene har offentlig innhold, mens andre kun har privat innhold, eller en kombinasjon. For mange er sosiale medier viktige kommunikasjonsplattformer som til dels erstatter tradisjonell telefonbruk. Informasjonen på profilene og plattformeiers sikkerhetskopier, ofte benevnt som informasjon i «skyen», kan derfor være viktig i etterforskning av ulike kriminelle handlinger.

Skylagring defineres som «et lagringsmedium lokalisert på en ekstern server driftet av en ekstern leverandør».[17] Den eksterne serveren som lagringsplass kalles ofte «skyen» (the cloud) fordi en viktig egenskap ved skylagring er at det lagrede materialet kan hentes frem raskt uansett hvor en befinner seg.[18] Det er vanlig å lagre filer, e-poster, bilder etc. i skyen. Det er mange tjenester som bruker skylagring, blant annet sosiale medier. Når vi bruker

[14] Øverby, H. «Internett» i Store Norske Leksikon, 1. oktober 2021. Hentet fra: https://snl.no/internett (Lest: 06.03.2024)
[15] Øverby (2021)
[16] Enli, G. «Sosiale medier» i Store Norske Leksikon, 06.02.2023. Hentet fra: https://snl.no/sosiale_medier (Lest: 13.02.2024)
[17] Nätt T. H. «Skylagring» i Store Norske Leksikon, 8. desember 2023. Hentet fra: https://snl.no/skylagring (Lest: 06.03.2024)
[18] Nätt (2023)

begrepet skylagringstjenester siktes det gjerne til bedrifter som eier og styrer eksterne servere som selger skylagring. Kjøpere av skytjenester kan velge mellom ulike lagringsmodeller som gir differensierte muligheter for særtilpasning av sikkerhetsnivå. Det omtales ofte som offentlige, private eller hybride løsninger for lagring. Dette skillet diskuteres ikke videre da skylagringsmetoden ikke innvirker på retten til bevisinnhenting av data utover hvor serveren er plassert.

På sosiale medier og i skylagringstjenester både deles og skapes data. Definisjonen av «data» er informasjon i et ubestemt format som kan behandles og brukes til det vi ønsker. Data kan være både analog og digital, og det er først når en behandler data at data blir informativ.[19] I denne oppgaven brukes «data» om informasjon som er lagret digitalt. Når data i utlandet innhentes i forbindelse med etterforskning av et straffbart forhold kan det kalles ekstraterritoriell bevisinnhenting. Det kan være innhenting av både analoge og digitale bevis som befinner seg utenfor landets grenser. I denne oppgaven brukes begrepet om innhenting av digitale bevis lagret på servere i utlandet uten samarbeid med myndighetene i landet der dataene er lagret.

Ekstraterritoriell bevisinnhenting kan utføres på ulike måter basert på dataens lokasjon og tilgjengelighet. Metodene diskutert i denne oppgaven er der informasjonen er offentlig tilgjengelig, der myndighetene benytter mistenktes egen innlogging eller når myndighetene «hacker» seg til informasjon. «Hacking» er ikke entydig i dagligtalen.[20] I denne oppgaven brukes «hacking» om situasjoner hvor politiet gjør innbrudd i en database for å innhente databevis.

Ved bevisinnhenting skilles det mellom «subscriber data», «traffic data» og «content data». De to sistnevnte kategoriene har en glidende overgang og det er vanlig å ikke operere med et skarpt skille. «Subscriber data» er informasjon som kan identifisere en bruker med en IP-adresse eller motsatt. «Traffic data» gir informasjon om operasjonssystemet og kommunikasjon mellom enheter. «Content data» er det innholdet brukeren har skapt eller sett på for eksempel e-poster, filmer og andre filer.[21] Det er sentralt å skille mellom data som

[19] Nätt, T. H. «Data» i Store Norske Leksikon, 22.10.2022. Hentet fra: https://snl.no/data (Lest: 13.02.2024)
[20] Nätt, T. H. «Hacking» i Store Norske Leksikon, 07.02.2024. Hentet fra: https://snl.no/hacking (Lest: 27.03.2024)
[21] Transborder Group of the Cybercrime Convention Committee Cloud Evidence Group (Cloud group) (2016) Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY. Council of Europe. Hentet fra: https://rm.coe.int/16806a495e (05.04.2024) s. 12

allerede eksisterer og kan gjenfinnes i et datasystem, versus data som innhentes i sanntid.[22] Bevisinnhentingshjemlene i straffeprosessloven trekker også dette skillet.[23] Ved innhenting i sanntid er det for databevis en flytende overgang mellom avlytting og ransakelse.[24]

For å begrense oppgavens omfang forutsettes det at dataene allerede er lagret. Oppgaven tar for seg handlingsrommet for ransakelse, beslag og utleveringspålegg etter strpl. §§ 192, 206 og 210.

[22] Cloud group (2016) s. 12
[23] Se for eksempel strpl. §§ 192, 206, 210 sammenlignet med strpl. §§ 216 o og 216 m
[24] Ekaas, I., D*ataavlesning som etterforskningsmetode: En rettslig analyse av straffeprosessloven § 216 o*, Universitetet i Bergen, 01. juni 2017, Hentet fra: https://bora.uib.no/bora-xmlui/bitstream/handle/1956/16227/Jus399_V17_208.pdf?sequence=1&isAllowed=y (Lest: 13.02.2024) s. 13

3 Rettstilstanden i Norge

3.1 Lovverk og forarbeider

Reglene for når og hvordan norske tjenestemenn kan innhente bevis er i hovedsak regulert i straffeprosessloven. Grensen mellom norsk rett og folkeretten trekkes i strpl. § 4 som gir uttrykk for at reglene i loven «gjelder med de begrensninger som er anerkjent i folkeretten eller følger av overenskomst med fremmed stat». Ordlyden tilsier ikke at folkeretten gjelder direkte som norsk rett. Folkeretten er likevel bestemmende for norske bevisinnhentingsregler i den forstand at straffeprosessloven ikke kan være i strid med Norges internasjonale forpliktelser. Suverenitetsprinsippet aktualiseres derfor ved innhenting av bevis utenfor norsk territorium. Det er neppe kontroversielt å påstå at innhenting av analoge bevis utenfor norsk territorium vil krenke suverenitetsprinsippet. Avgjørende for den norske rettstilstanden er om det er grunn til å behandle digitale bevis annerledes enn analoge bevis.

Et eksempel på analog bevisbehandling er der en norsk bil blir stjålet av en norsk statsborger i Norge og så kjørt til Sverige. Norsk politi vil ikke kunne krysse grensen inn i Sverige og beslaglegge bilen etter strpl. § 203 uten å krenke svensk suverenitet, selv om Norge har strafferettslig jurisdiksjon over lovbruddet, ettersom Sverige har eksklusiv håndhevelsesjurisdiksjon. Den veletablerte rettstilstanden tilsier at politiet måtte benyttet etablerte ordninger om internasjonalt rettslig politi- og påtalesamarbeid (rettsanmodninger). For å avgjøre om det er grunn til å behandle digitale bevis annerledes er første vurdering om straffeprosessloven legger opp til en forskjellsbehandling mellom digitale og analoge bevis.

Digitale bevis kan innhentes ved ransakelse, beslag og utleveringspålegg etter straffeprosesslovens kapittel 15 og 16. Her finner en i hovedsak eldre bestemmelser hvor begrepet «ting» har blitt tolket teknologinøytralt for å åpne for digital bevisinnhenting over nett.[25] Etter Norge sluttet seg til Europarådets konvensjon om datakriminalitet (Budapestkonvensjonen) har en teknologinøytral tolkning vært sentral for å ivareta Norges

[25] NOU 2016: 24 Om ny straffeprosesslov Hentet fra: https://www.regjeringen.no/contentassets/6fe1d875248042b4a09b43b85aa46832/no/pdfs/nou201620160024000dddpdfs.pdf (07.02.2024) s. 336-337; Justis- og beredskapsdepartementet, Effektiv og tillitvekkende og rettssikker behandling av databevis, 2021. Hentet fra: https://www.regjeringen.no/contentassets/13417a44276c4b4086fdcbabb2108455/utredning-databevis-2021.pdf (07.02.2024) s. 10

internasjonale forpliktelser ved utlevering av data på forespørsel.[26] Dersom en leser strpl. §§ 192, 206 og 210 gir ikke ordlyden rammene for det stedlige virkeområdet for etterforskningsmetodene. Kommisjonen som forberedte straffeprosessloven leverte sin innstilling i 1969. Det var før den teknologiske utviklingen tilsa at det forelå behov for særregulering av databevis og forholdet er dermed ikke vurdert nærmere.[27] Forarbeidene forbundet med Budapestkonvensjonen vurderer om norsk lov er i tråd med forpliktelsene til å utlevere og bistå i etterforskning i andre land, ikke hvilke kanaler norske myndigheter må benytte for å innhente bevis lagret i utlandet.[28]

Mangelen på skille mellom digitale og analoge bevis er tvetydig. En forståelse er at reglene for bevisinnhentning på tvers av landegrenser gjelder likt for analoge og digitale bevis. Motargumentet er at når grenseoverskridende bevisinnhenting og tilknyttede utfordringer ikke har gjort seg særlig gjeldende før i nyere tid så bør ikke digitale bevis omfattes av et «utdatert» regelverk. Samtidig var problemstillinger tilknyttet reguleringen av digital ekstraterritoriell bevisinnhenting aktuelle allerede før Budapestkonvensjonen.[29] Mangelen på særregulering kan tyde på at lovgiver mener at digitale og analoge bevis bør behandles likt. Samfunnets bruk av digitale hjelpemidler, som sosiale medier og skylagring, har imidlertid økt vesentlig etter ratifiseringen av Budapestkonvensjonen. [30] Det kan derfor reises tvil om det før innføringen av Budapestkonvensjonen var mulig å forutse omfanget av utfordringene tilknyttet digital ekstraterritoriell bevisinnhenting ved nasjonalt begåtte forbrytelser. Denne utviklingen kan, uavhengig av forarbeidene, trekke i retning av at skillet mellom analoge og digitale bevis kan være sentralt for om bevisinnhenting krenker suverenitetsprinsippet.

Spørsmålet om hvilken adgang det er til å etterforske datanettverk i utlandet ble behandlet mer utførlig i Metodeutvalgets utredning fra 1997.[31] Utvalget poengterte at digitale bevis ikke er tilknyttet de tradisjonelle territorialgrensene. Videre mente utvalget at folkeretten ikke setter grenser dersom dataene er hentet gjennom norske tvangsmidler på norsk territorium da dette må regnes som ransaking i Norge. For å nå denne konklusjonen så utvalget til praksis

[26] Council of Europe Convention on Cybercrime (ETS No. 185), 23. November 2001 (entered into force 01. July 2004) (Budapestkonvensjonen); Justis- og beredskapsdepartementet (2021) s. 16
[27] NUT 1969:3 Innstilling om rettergangsmåten i straffesaker fra Straffeprosesslovkomiteen s. 16
[28] NOU 2003: 27 om lovtiltak mot datakriminalitet — Delutredning I om Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi s. 53-58
[29] Currie (2017) s. 77-78
[30] Meld. St. nr. 34 (2020-2021) Sammen mot barne-, ungdoms- og gjengkriminalitet s. 44-45
[31] NOU 1997: 15 punkt 4.2.1.3

for andre grenseoverskridende tvangsmidler som vitneplikt og telefonavlytting. I lys av denne parallellen ble det lagt til grunn at det avgjørende må være om dataene kunne nås fra en terminal i Norge.[32] Høyesterett synes å konstatere at det ikke foreligger noen grundig vurdering av den ekstraterritorielle virkningen av telefonavlytting, noe som svekker den rettskildemessige verdien av parallellen og etterarbeidene.[33]

Omfanget av akseptabel digital ekstraterritoriell bevisinnhenting ble ansett å være minst like vidt som ved tradisjonell ransakelse av analoge bevis i Norge. Etter Metodeutvalgets syn kan ikke politiet selvstendig skaffe seg en tilgang som ikke den ransakede allerede har, for eksempel ved hacking - men de kan benytte alle tilganger den mistenkte har, inkludert ulovlige anskaffede tilganger. [34] Grensedragningen synes intuitiv, da politiets innbrudd i servere i utlandet ville vært på lik linje med å ta seg inn i en eiendom som verken tilhørte ransakede eller som ransakede hadde tilgang til.

Utvalgets betraktninger må anses som et etterarbeid da det ikke førte til noen lovendring, og utvalget påpekte selv at rettstilstanden er usikker på grunn av manglende domstolsbehandling og juridisk teori om problemstillingen i Norge. Andre land som Tyskland har landet på at digital ekstraterritoriell bevisinnhenting er rettstridig.[35] Når utvalget kommer til motsatt konklusjon er det begrunnet i reelle hensyn som effektiv og praktisk gjennomførbar etterforskning. Utvalget åpnet for at ny rettsutvikling nasjonalt og i folkeretten kunne endre rettstilstanden. [36] Metodelæren stadfester at etterarbeider generelt har begrenset og varierende vekt. Til tross for usikkerheten har etterarbeidende her likevel noe rettskildemessig vekt, da problemstillingen er utførlig vurdert og egnet til å inngi tillit til vurderingene, og dermed være representativ for den norske rettstilstanden. Spesielt i lys av det sparsomme norske rettskildebildet på dette området.[37] Høyesterett synes å betrakte Metodeutvalgets resonnement som sentralt, ettersom førstvoterende aktivt benyttet vurderingsmomentene skissert i etterarbeidet i Tidal-kjennelsen til tross for arbeidets svakheter.[38]

Forholdet mellom innhenting av databevis og suverenitetsprinsippet ble også kommentert i forarbeidene til bokføringsloven i 2002. Bokføringsutvalget pekte her på at oppbevaring av

[32] NOU 1997: 15 punkt 4.2.1.3
[33] HR-2019-610-A avsnitt 46
[34] NOU 1997: 15 punkt 4.2.1.3
[35] NOU 1997: 15 punkt 4.2.1.3
[36] NOU 1997: 15 punkt 4.2.1.3
[37] Eckhoff, T., og Helgesen, J. E. (2001). *Rettskildelære*, 5. utg., Oslo: Universitetsforlaget s. 95-100
[38] HR-2019-610-A avsnitt 46 og avsnitt 67-70

regnskap i utlandet ville vanskeligjøre politiets kontroll av regnskapet ettersom norske myndigheter måtte be om tillatelse for å gjennomgå regnskapet.[39] Bokføringsutvalget synes å forutsette at kontroll av regnskap som er lagret på servere i utlandet er rettstridig uavhengig av om tilgangen kan oppnås fra norsk territorium. Betydningen bokføringsutvalgets konklusjoner har for rettstilstanden, må ses i lys av at det er et etterarbeid til straffeprosessloven, og utvalget synes ikke å gjøre en grundig vurdering av jurisdiksjonsspørsmålet. Høyesterett valgte derfor å ikke tillegge de nevneverdig vekt i Tidal saken.[40] Bokføringsutvalget tar heller ikke stilling til argumentene til Metodeutvalget.

I lys av ovenstående konkluderes det med at straffeprosessloven, dens forarbeider og etterarbeider som omtaler problematikken er uklare, motstridende eller tause. Rettstilstanden fremstår derfor som usikker, særlig fordi det kan ha skjedd større utviklinger i folkeretten og teknologi i ettertid. Uklarheten og mangelen på tidligere domstolsbehandling er trolig bakgrunnen for at Tidal-saken ble behandlet i Høyesterett.

3.2 Tidal-saken

3.2.1 Tingretten og lagmannsretten

Økokrim begjærte tredjemannsransakelse av Tidals lokaler og datasystemer for Oslo tingrett i desember 2018. Tingretten besluttet at vilkårene for ransakelse etter straffeprosessloven § 197, jf. § 192 andre ledd nr. 3, jf. § 170 a var oppfylt, og beslag ble igangsatt. I beslutningen ble det lagt til grunn at ved digitale bevis omfattet «begjæringen også de aktuelle databærere og elektronisk lagret informasjon som vedkommende har tilgang til», deriblant «online databærere i form av servere mm.».[41] Under ransakelsen tok politiet beslag i data som var tilgjengelig ved hjelp av dataterminaler som var lokalisert i selskapets Oslo kontor, men informasjonen var lagret på utenlandske servere.

Tidal anket beslutningen inn for lagmannsretten med begrunnelsen at formuleringen til tingretten gav en for vid adgang til ransakelse da den åpnet for innhenting av dokumenter som

[39] NOU 2002: 20 s. 105
[40] HR-2019-610-A avsnitt 47
[41] TOSLO-2018-182196

var lagret på servere i utlandet som etter Tidals mening var i strid med folkeretten.[42] Som begrunnelse for sitt standpunkt viste Tidal til forarbeidene til bokføringsloven, som nevnt i uttalelsene ovenfor. I tillegg viste Tidal til art. 18 og 32 i Budapestkonvensjonen som de mente viste at det ikke var adgang til å innhente databevis på tvers av landegrenser.[43]

Lagmannsretten tok stilling til partenes anførsler i kjennelsen ved å se til Budapestkonvensjonen, Metodeutvalget og Bokføringsutvalget. Retten sa seg enig i Økokrims anførsel om at strpl. § 4 ikke begrenset ransakelsesadgangen til politiet, i dette tilfellet på bakgrunn av metodeutvalgets betraktninger.[44] Til tross for Tidals anførsel om at metodeutvalgets resonnementer må anses som svake, ulogiske og foreldede, har ikke lagmannsretten gjort en selvstendig vurdering av folkeretten for å fastslå om Metodeutvalgets betraktninger fremdeles er holdbare i lys av mulig rettsutvikling. En slik vurdering er sentral når dokumentet kjennelsen bygger på er over tjue år gammelt og et etterarbeid til straffeloven. Kjennelsen ble anket av Tidal til Høyesterett med begrunnelsen at lagmannsretten hadde lagt til grunn feil lovforståelse.

3.2.2 Høyesterett

Tidal-saken ble behandlet i avdeling i Høyesterett og resultatet ble enstemmig at lagmannsrettens lovforståelse måtte anses som rett og at anken derfor forkastes. Høyesterett startet med å konstatere at vilkårene for ransakelse og beslag etter strpl. § 192 tredje ledd var oppfylt.[45] Deretter tolket retten ordlyden i strpl. §192 og konstaterte at dersom det foreligger en begrensing i adgangen til digital bevisinnhenting må det være fordi strpl. § 4 første ledd fordrer en innskrenkende tolkning.[46] Førstvoterende dommer Kallerud undersøkte deretter folkerettslige kilder for å vurdere om det foreligger behov for innskrenkende tolkning.[47]

I avsnitt 35-38 legges det til grunn at Budapestkonvensjonen ikke gir tolkningsbidrag ettersom konvensjonsbestemmelsene ikke direkte angår et tilfelle som i Tidal-saken og ikke forbyr ransakingen. Denne forståelsen synes å bygge på Økokrims anførsel for lagmannsretten om at Budapestkonvensjonen ikke gir uttrykk for rettstilstanden tilknyttet

[42] LB-2018-190770
[43] LB-2018-190770
[44] LB-2018-190770
[45] HR-2019-610-A avsnitt 24-31
[46] HR-2019-610-A avsnitt 33
[47] HR-2019-610-A avsnitt 35 flg.

ekstraterritoriell bevisinnhenting i folkeretten basert på en rapport om konvensjonens artikkel 32.[48] Høyesterett gir så uttrykk for at det er uklart i hvilken utstrekning det veletablerte suverenitetsprisnippet gjelder for ny digital teknologi som skylagring.[49] For å ta stilling til spørsmålet ser dommer Kallerud først til norsk praksis i avsnitt 44-47. Her brukes utredningen til Metodeutvalget til å underbygge at norsk praksis har lagt til grunn at det avgjørende for jurisdiksjon er hvor dataterminalen er lokalisert, ikke det lagrede innholdet. Førstvoterende peker imidlertid på at utredningen ikke førte til lovendringer og at jurisdiksjonsspørsmålet ikke synes å ha vært problematisert ytterligere.

Dommer Kallerud ser til andre europeiske lands praksis og konstaterer at praksisen er ulik etter å ha sett til dansk rett, svensk rett og en rapport fra Europarådet. Basert på disse undersøkelsene legger han til grunn at det innad i Europa ikke foreligger enighet om digital ekstraterritoriell bevisinnhenting, og at Norge ikke er alene om forståelsen om at dataterminalens lokasjon er mest sentral.[50] For et mer internasjonalt perspektiv ser retten til Tallinn-manualen, en rapport om reglene i cyberspace utviklet av en rekke internasjonale eksperter i regi av NATO.[51]

Regel 11 i Tallinn-manualen behandler ekstraterritoriell håndhevelsesjurisdiksjon og utfordringer knyttet til regulering av jurisdiksjon på nett. Høyesterett tolket regel 11 til støtte for den norske forståelsen om at det er dataterminalen og rettssubjektets lokasjon som er avgjørende for om materialet kan innhentes.[52] Førstvoterende konkluderte derfor i avsnitt 58 med at det ikke foreligger folkerettslig sedvane om rettsspørsmålet. Høyesterett bemerket likevel at mange stater godtok en praksis med innhenting av digitale bevis lagret i utlandet i lys av rapporten fra Europarådet.[53]

Den gjennomgåtte utredningen av rettskildene danner grunnlaget for Høyesteretts delkonklusjon i avsnitt 61 om at rettsspørsmålet ikke er regulert i folkeretten, og at «norske rettsanvendere på selvstendig grunnlag [må] ta stilling til om bruk av tvangsmidler krenker en annen stats suverenitet». Retten gir ikke føringer for hvordan norske rettsanvendere skal

[48] LB-2018-190770; Council of Europe (2001) Explanatory Report to the Convention on Cybercrime. Council of Europe. Hentet fra: https://rm.coe.int/16800cce5b (Lest: 05.03.2024) s. 53
[49] HR-2019-610-A avsnitt 40-42
[50] HR-2019-610-A avsnitt 53-54
[51] Schmitt, M. N., & NATO Cooperative Cyber Defence Centre of Excellence. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*, 2. utg. Cambridge University Press. (Tallinn-manualen)
[52] HR-2019-610-A avsnitt 56
[53] HR-2019-610-A avsnitt 59

foreta suverenitetsvurderingen, men konstaterer at det kan være nyttig å vurdere om handlingen griper inn i en annen stats håndhevelsesjurisdiksjon på en måte som er i strid med suverenitetsprinsippet.[54] Uttalelsen sier ikke noe om i hvilke situasjoner innhenting av digitale bevis vil krenke suverenitetsprinsippet, eller hvilke momenter som er relevante ved den skjønnsmessige vurderingen. Hvordan den enkelte rettsanvender skal foreta vurderingen er dermed uklart, noe som kan føre til ulik praksis og dårlig rettsenhet. Uklarhet kan også bidra til myndighetsmisbruk og internasjonal disputt ved at påtalemyndigheten og domstolene tillater en for vid adgang til ekstraterritoriell bevisinnhenting.

Høyesterett går så over til å vurdere om ransakelsen i Tidal-saken utgjorde en krenkelse av suverenitetsprinsippet.[55] Innledningsvis pekes det på at det i dette tilfellet er tale om et tvangsmiddel gjennomført på norsk territorium mot et norsk selskap med tilgang til datamaterialet.[56] Dette brukes til å grunngi at Norge ikke gjør en selvstendig inntrenging i bevismaterialet lagret i utlandet.[57] Utfra denne vurderingen fremkommer det at Tidals tilgang til dataene var en viktig forutsetning for å konkludere at suverenitetsprinsippet ikke var brutt. Om Tidal ikke hadde hatt datatilgang og politiet hadde måttet tilegne seg materialet i utlandet ved hacking så ville det sannsynligvis utgjort et brudd på suverenitetsprinsippet. Et moment i suverenitetsvurderingen vil dermed være hvordan påtalemyndigheten får tilgang til datamaterialet. Dette er i tråd med Metodeutvalgets lovforståelse.[58]

Videre peker Høyesterett på effekten ransakelsen har i utlandet, og konstaterer at ransakelsen ikke har effekt når materialet på serveren ikke blir slettet, sperret eller endret på annen måte.[59] Her synes Høyesterett å legge til grunn at dersom tvangsmiddelet endrer karakteren til informasjonen i utlandet ved at en sletter det, eller ved at man hindrer tilgangen til informasjonen for andre parter, kan suverenitetsvurderingen få et annet utfall. En kritikk av Høyesteretts resonnement her er at de ikke tar stilling til effekten av at det foretas etterforskning i et annet land i seg selv. Dersom norsk politi hadde reist til Danmark for å intervjue vitner hadde ikke det etterlatt seg spor i form av at vitnene ikke kunne gjenta den

[54] HR-2019-610-A avsnitt 61
[55] HR-2019-610-A avsnitt 65-71
[56] HR-2019-610-A avsnitt 66-67
[57] HR-2019-610-A avsnitt 67
[58] NOU 1997: 15 punkt 4.2.1.3
[59] HR-2019-610-A avsnitt 70-71

samme informasjonen til dansk politi, likevel er det ubestridt at en slik handling ville krenket dansk suverenitet.

En forklaring på hvorfor Høyesterett differensierer digital bevisinnhenting fra analog kan være fokuset de innledningsvis har på at digitale bevis ikke er territorielle. Førstvoterende bruker tid på å uttrykke hvor tilfeldig det er hvor bevis blir lagret, noe som synes å påvirke Høyesteretts konklusjon om hvor inngripende effekten av etterforskning er i landet der data er lagret. Dette er også gjenstand for internasjonal diskurs som belyser under punkt 4.

Dersom en leser mellom linjene ser en at Høyesteretts utgreing om tilfeldigheter og bevisenes grenseløse natur hviler på effektivitetshensyn. Hvis politiet må vite hvor et bevis befinner seg, eller spørre ti land om tillatelse til å innhente beviset gjennom en langtekkelig prosess, vil dette være et hinder for effektiv rettshåndhevelse i Norge.[60] Effektivitetshensyn blir aldri eksplisitt vektlagt i kjennelsen, men utfra argumentasjonen til Høyesterett synes det klart at dette har vært et sentralt hensyn som kan ha vært bestemmende for hvordan Høyesterett har tolket rettskildene. Et viktig spørsmål blir i hvilken grad effektivitetshensyn åpner for å innhente bevis i andre tilfeller enn det som forelå i Tidal saken.

Reelle hensyn, som effektivitetsbetraktninger, er en sentral og anerkjent rettskilde i norsk rettskultur, særlig der autorative kilder er uklare eller tvetydige som i foreliggende tilfelle. Det er imidlertid sentralt at den juridiske argumentasjonen i en kjennelse skal være grundig, balansert og etterprøvbar for å sikre rettslig integritet. At effektivitetshensyn fremstår som en indre overveielse,[61] som kun kommer til syne implisitt, kan gi inntrykk av at førstvoterende vekter rettskildene med forutinntatthet for å lande på at ekstraterritoriell bevisinnhenting er akseptabelt.

Manglende gjennomsiktighet åpner for å stille spørsmål rundt hvor grundig og balansert Høyesteretts vurdering av de autoritative kildene egentlig er når førstvoterendes indre overveielser ikke kommer klart frem. Det kan spesielt gjøre seg gjeldende ved pragmatiske vurderinger som i Tidal-saken. Samtidig kan det påpekes at effektivitetshensynet i dette tilfellet er et konsekvensorientert hensyn som brukes for å ivareta rettslige- og samfunnsmessige verdier i det norske rettssystemet.[62] Førstvoterende bygger dermed ikke på

[60] HR-2019-610-A avsnitt 41-42
[61] Tande, K. M. (2011). Individuelle valg og vurderinger i rettsanvendelsesprosessen. *Jussens venner*, *46*(1), 1–36. Hentet fra: https://doi.org/10.18261/ISSN1504-3126-2011-01-01 (Lest: 27.03.2024) s. 15-17
[62] Eckhoff (2001) s. 377-397

rene rimelighetsbetraktninger, men systembetraktninger for å sikre rettssikkerhet. Det gir argumentasjonen troverdighet, selv om argumentasjonen hadde vært bedre dersom Høyesterett hadde synliggjort at effektivitetshensyn var sentralt i kjennelsen.

Høyesterett konkluderer med at en kan innhente digitale bevis på tvers av landegrenser ved bruk av tvangsmidlene i straffeprosessloven, i visse tilfeller - der en kan få adgang gjennom tilgangen til den tvangsmiddelet er rettet mot, og bruken av tvangsmiddelet ikke vil endre eller fjerne data. Her er det sentralt å vurdere hvordan Høyesteretts konklusjon påvirker digital bevisinnhenting utenfor Tidal-saken ved å parallelltolke kjennelsens ratio decidendi opp mot mulige tilfeller av ekstraterritoriell bevisinnhenting. Det kan tenkes tre typetilfeller: a) politiet ransaker en e-postkonto som er koblet opp mot en sky fra mistenktes datamaskin i Norge, b) politiet ransaker e-postkontoen til en mistenkt som er bosatt i Norge fra politiets egne datasystemer og c) politiet ransaker e-postkontoen til en mistenkt som er bosatt i utlandet eller har ukjent oppholdssted fra politiets egne datasystemer.

Typetilfelle a) er sammenfallende med tilfellet i Tidal-saken. Her ville det, i lys av argumentasjonen i Tidal saken, være uproblematisk å logge inn på den mistenktes maskin, ransake og beslaglegge materialet i skyen så lenge politiet brukte mistenktes tilgang ved innloggingen. Scenario b) skiller seg i større grad fra tilfellet i Tidal-saken, men det er likevel klare likheter. Rettssubjektet er bosatt i Norge, og i hvilket land detaljene knyttet til e-postkontoen er lagret fremstår som tilfeldig ettersom den ransakede klart nok har en tilknytning til Norge. Det er vanskelig å forestille seg at det skulle være en forskjell om politiet brukte egne maskiner til å tilegne seg dette materialet, kontra å bruke mistenktes maskin, gitt at politiet også her bruker mistenktes tilgang. Det kan dermed argumenteres at scenario b) er så likt faktum i Tidal-saken at det må anses som akseptabelt.

Både i scenario a) og b) blir derimot tilgangen mer tvilsom dersom politiet hacker seg inn i e-postkontoen. Dette fremgår av Høyesteretts betraktninger rundt selvstendig inntrenging i utenlandske servere. At politiet må ha lovlig adkomst til enheten vil også være et kriterium i scenario c). Scenario c) skiller seg imidlertid ytterligere fra Tidal-saken sammenlignet med scenario a og b. En utenlandsk bosatt vil ha mindre tilknytning til Norge, spesielt når verken mistenkte, mistenktes datamaskin/mobil eller dataene befinner seg i Norge. Dette vil forsterkes ytterligere dersom mistenkte heller ikke er norsk statsborger. Scenario b) skiller seg fra scenario c) i den forstand at dataene i scenario b) er ment tilgjengeliggjort fra Norge og lagringsstedet fremstår tilfeldig. I scenario c) er det ingenting som tilsier at norsk politi har

håndhevelsesjurisdiksjon over dataene, og parallellen strekker argumentasjonen i Tidal-saken for langt til å være rettslig forsvarlig. En slik tolkning hadde medført en vid adgang til å innhente ekstraterritoriell data. Adgangen ville være markant utenfor tilfellet som ble godtatt i Tidal-saken og samsvarer dårlig med vurderingsmomentene Høyesterett trakk frem.

3.3 Etterfølgende juridisk diskurs

3.3.1 Innledende kritikk av Tidal-sakens omfang

I etterkant av Tidal-saken er det kommet både tilfang og kritikk til kjennelsen. Professor ved UiB Jon Petter Rui var den første som kritiserte kjennelsen. Han hevdet kjennelsen gav påtalemyndigheten i Norge en «noe nær ubegrenset adgang til å ransake og ta beslag» i digitalt bevismateriale som befinner seg utenfor norsk territorium.[63] Rui er kritisk til Høyesteretts forståelse av suverenitetsprinsippet, ettersom han mener at det avgjørende er om handlingen «har effekt» på et annet territorium, i lys av internasjonal rettspraksis. Etter hans forståelse vil enhver etterforskning av materiale lagret i utlandet utgjøre en krenkelse. [64] Oppsummert uttrykker artikkelen at selv om ekstraterritoriell bevisinnhenting er forskjellig fra analoge etterforskningsmetoder gjelder suverenitetsprinsippet ettersom suverenitetsprinsippet er ufravikelig internasjonal rett (jus cogens).[65]

Rui bygger synspunktet sitt på flere kilder. I artikkelen trekker han blant annet frem at Budapestkonvensjonens prosedyrer for ekstraterritoriell bevisinnhenting blir formålsløse dersom stater lovlig kan innhente bevis lagret ekstraterritorielt.[66] Han ser så til den amerikanske lovgivningen som regulerer utlevering og tilgang til data lagret på servere i USA, Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Rui bruker eksistensen av CLOUD Act som bevis på at innhenting av bevis lagret på amerikansk jord, i det minste, må anses som et brudd på amerikansk lovgivning.[67] Rui begrunner ikke hvorfor eller i hvilken utstrekning amerikansk lov har innvirkning på norsk rettstilstand og internasjonal rett, noe som begrenser argumentets vekt. Artikkelen bidrar heller ikke til hvordan en løser et tilfelle hvor dataens lokasjon er usikker (loss of location - LOC), dersom det ikke er adgang til å

[63] Rui (2019) s. 261
[64] Rui (2019) s. 261-262
[65] Rui (2019) s. 261-262
[66] Rui (2019) s. 261
[67] Rui (2019) s. 262

innhente bevis uten å samarbeide med staten informasjonen er lagret i. Konklusjonen til Rui er at rettstilstanden presentert i Tidal-kjennelsen ikke er forenlig med suverenitetsprinsippet.[68]

3.3.2 Skjolds kommentar til Høyesteretts kjennelse i Tidal-saken og Ruis kritikk

Som motsvar til Ruis kritikk av kjennelsen i Høyesterett kom førsteamanuensis ved UiO Jørgen S. Skjold til forsvar av Høyesteretts avgjørelse. Artikkelen omhandler hvorfor Skjold mener Høyesteretts analyse er treffende, og hvordan rettsanvendere skal foreta suverenitetsvurderingen Høyesterett forutsetter i Tidal.[69] Innledningsvis motsetter Skjold seg Ruis forståelse av jus cogens. Skjold mener at jus cogens, som suverenitetsprinsippet, må tolkes, akkurat som andre rettsregler. Dette mener Skjold medfører at suverenitetsprinsippet har begrenset rekkevidde i relasjon til digitale bevis.[70]

For å begrunne suverenitetsprinsippets begrensning bruker Skjold internasjonal rettspraksis, Lotus-saken og Trail Smelter-saken til å konstatere at enhver ekstraterritoriell tilknytning eller konsekvens ikke medfører suverenitetskrenkelse. Han innvender at bevisinnhenting ved moderne teknologi sjeldent vil medføre en relevant konsekvens ettersom dataene forblir uendret, som i Tidal-saken.[71] En innvending til dette perspektivet er at Trail Smelter ikke forutsetter fysisk tilstedeværelse for krenkelse, og at etterforskningshandlingen alene kan utgjøre en suverenitetskrenkelse. Mot dette presenterer Skjold et «de minimis non curat lex»-argument.[72] Begrepet er latinsk for at loven ikke regulerer trivialiteter.

Skjold argumenterer for at ekstraterritorielle etterforskningshandlinger er trivielle, ettersom statspraksis viser at mange stater tillater det. Han viser eksempelvis til at innhenting av informasjon som er åpent tilgjengelig på internett ikke anses som suverenitetskrenkelse.[73] Til denne logikken kan det innvendes at nettopp tilgangen til offentlig tilgjengelig data er regulert i art. 32 i Budapestkonvensjonen. Det er klart forskjell mellom åpent tilgjengelig data og

[68] Rui (2019) s. 262
[69] Skjold (2019) s. 617-619
[70] Skjold (2019) s. 621-622
[71] Skjold (2019) s. 622-623
[72] Skjold (2019) s. 623
[73] Skjold (2019) s. 623-625

privat, utilgjengelig data. Aksept for det ene, tilsier ikke at det andre faller under de minimis-terskelen.

Skjold er også kritisk til at Høyesterett konkluderer med at det ikke foreligger noen folkerettslig sedvane knyttet til digital ekstraterritoriell bevisinnhenting. Han gir uttrykk for at Høyesterett må mene at det foreligger aksept i form av sedvane, til tross for inkonsekvent praksis.[74] CLOUD Act brukes her som argument for at rettsforståelsen i Tidal-saken er riktig i motsetning til Ruis artikkel. Begrunnelsen er at lovgivningen tillater amerikanske myndigheter å kreve bevisutlevering av amerikanske selskaper, uavhengig av dataens lokasjon.[75] I likhet med Rui, begrunner ikke Skjold hvorfor amerikansk rett er relevant i denne sammenhengen. Skjold kommenterer heller ikke at CLOUD Act krever en bilateral avtale mellom landende for at amerikanske myndigheter skal være kompetente til å hente informasjon lagret på utenlandske servere.[76]

Avslutningsvis gir Skjold uttrykk for at det er vanlig å tolke internasjonale rettskilder for å sikre effektiv jurisdiksjon på alle områder. Artikkelen uttrykker også at bekymringer rundt inngrep i retten til privatliv ikke er relevant for jurisdiksjonsspørsmålet, ettersom stater og egne regelsett må beskytte disse.[77] Skjold konkluderer med at Tidal-saken som prejudikat ikke tillater en nær ubegrenset jurisdiksjon, men gir en begrenset adgang til ekstraterritoriell bevisinnhenting i lignende tilfeller som følge av de minimis-argumentet. Denne løsningen åpner også for bevisinnhenting i LOC-tilfellene, da Skjold mener dette virker etter mer-til-mindre prinsippet her.[78] Etter min forståelse av Skjold, gir ikke Tidal-saken føringer dersom LOC-tilfellene krever hacking, eller medfører ødeleggelse av enten data, eller dataterminalene, da dette vil være over de minimis-terskelen.

3.3.3 Nygårds analyse av Skjold og Høyesteretts resonnement og kildebruk

Det nyeste norske tilskuddet til debatten er en artikkel skrevet av politiadvokat Victoria S. Nygård som kritiserer Skjold og Høyesterett for å overse relevante rettskilder i deres analyser.[79] Skjolds og Nygårds innledende forståelse av suverenitetsprinsippet er

[74] Skjold (2019) s. 626-629
[75] Skjold (2019) s. 629-630
[76] Cloud Act § 2523
[77] Skjold (2019) s. 631-633
[78] Skjold (2019) s. 633-639
[79] Nygård (2021) s. 140

sammenfallende.[80] Nygård synes også å si seg delvis enig i de minimis-argumentet til Skjold. Som støtte for dette viser hun blant annet til regel 11 i Tallinn-manualen, som ble brukt av Høyesterett i avsnitt 56, som argument for at ekstraterritoriell bevisinnhenting er akseptert. Der Nygård synes å skille seg fra Høyesterett og Skjold, er i spørsmålet om hvilke tilfeller som faller under de minimis-terskelen. Her hevder Nygård at Tidal-saken overskrider terskelen for suverenitetskrenkelse etter folkeretten.[81]

Nygård poengterer at det faktum at Budapestkonvensjonen har prosessuelle regler om ekstraterritoriell bevisinnhenting, forutsetter at det er ulovlig. I likhet med Rui, bruker hun dette som argument for at Tidal-ransakelsen var ulovlig.[82] Verken Nygård eller Rui tar stilling til hvordan det skal vektes at Europarådets rådgivende rapport forutsetter at Budapestkonvensjonen art. 32 er uten betydning for rettstilstanden i folkeretten. Dette er et argument som er sentralt for lagmannsrettens beslutning om at Budapestkonvensjonen ikke gir tolkningsbidrag på området, og som Høyesterett slutter seg til.[83] Kritikken fremstår dermed som mindre treffende når den ikke forklarer hvorfor Høyesteretts argumentasjon på dette området ikke er dekkende.

Nygård mener at Budapestkonvensjonens reguleringer er utdatert, noe som gjenspeiles i at vi ser eksempler på at land lager egne lovhjemler for innhenting av digitalt bevismateriale utenfor eget territorium. CLOUD Act er et eksempel på det. CLOUD Act er imidlertid i en særstilling, ettersom den forutsetter en gjensidig avtale. De fleste slike lovhjemler er ensidige, og åpner kun for å hente informasjon ved alvorlig kriminalitet.[84] CLOUD Act minner derfor mer om en tradisjonell politisamarbeidsavtale. Artikkelen viser også til en United Nations Office on Drugs and Crime (UNDOC) undersøkelse fra 2013 om at aksept for, og bruk av, grenseoverskridende datatilgang i etterforskning varierer. Nygård tolker UNDOC-undersøkelsen dithen at de fleste stater mener grenseoverskridende datainnhenting er ulovlig, men praktiserer det fordi de mangler effektive alternativer.[85]

Når det kommer til å trekke grensen for hva som er tillatt, åpner Nygård for at noen former for ekstraterritoriell bevisinnhenting er akseptabelt. Det første tilfellet er der informasjonen er

[80] Nygård (2021) s. 143
[81] Nygård (2021) s. 143-146
[82] Nygård (2021) s. 147-148; Rui (2019) s. 261
[83] HR-2019-610-A avsnitt 35-38; LB-2018-190770
[84] Nygård (2021) s. 149-151
[85] Nygård (2021) s. 152-154

åpent tilgjengelig på nett, som det også åpnes for i Budapestkonvensjonen art. 32 bokstav a.[86] Eksempelvis må bevisinnhenting av informasjon åpent tilgjengelig på en Instagram-konto anses som akseptabelt. Det er derimot uakseptabelt å innhente bevis som kun er tilgjengelig for den som eier Instagram-kontoen, eksempelvis meldinger med andre brukere. Et vanskeligere grensetilfelle kan oppstå der en må bli akseptert som følger til en privat konto for å se innholdet.

Det neste tilfellet Nygård mener må være akseptabelt er der det foreligger LOC. Dette baserer hun på praksis, en rapport fra Europarådets Cybercrime-komite og internasjonal juridisk litteratur.[87] Artikkelen går imidlertid ikke nærmere inn på i hvilken utstrekning en kan innhente bevis i LOC-tilfellene. Det er dermed uklart om Nygård mener grensen må trekkes på samme måte som skissert i Tidal-saken, snevrere eller om en i LOC-tilfellene kan gå lenger ved for eksempel å hacke seg til informasjonen.

Konklusjonen til Nygård er dermed at en kun kan innhente offentlig tilgjengelig data, og at det kan innhentes data ved LOC. For å kunne konkludere med dette diskrediterer Nygård funnene fra Tallinn-manualen. Hun peker her på at funnene i Tallinn-manualen passer dårlig overens med de øvrige rettskildene hun har sett på. Den er i strid med Norges ratifisering av Budapestkonvensjonen, som etter Nygårds syn forutsetter at bevisinnhenting på tvers av landegrenser er ulovlig.[88] Konklusjonen kan kritiseres for at rettskildebildet Nygård har skissert ikke nødvendigvis er så entydig som det gis uttrykk for i artikkelen - spesielt med tanke på at Høyesterett mener at Budapestkonvensjonen ikke er retningsførende for internasjonale regler om ekstraterritoriell bevisinnhenting i tilfeller som Tidal-saken.[89]

Avslutningsvis legger Nygård til grunn at i lys av reelle hensyn, som hensynet til samfunns- og rettssikkerhet, fremsto Høyesteretts avgjørelse som den eneste riktige. Ettersom en annen konklusjon ville medført store utfordringer for politiets straffesaksbehandling, da det er rundt 85 prosent av straffesaker som har behov for elektronisk bevis, og at to tredjedeler av disse bevisene er lagret i utlandet.[90] Dette er et berettiget argument, som kan forklare hvorfor Høyesterett forkastet anken i Tidal-saken. Det kan tenkes at rettskildebildet og argumentasjonen Høyesterett benyttet er farget av behovet for effektivitet. Artiklene til Rui og

[86] Nygård (2021) s. 154-155
[87] Nygård (2021) s. 154-155
[88] Nygård (2021) s. 156-157
[89] HR-2019-610-A avsnitt 35-38
[90] Nygård (2021) s. 159-160

Nygård presenterer flere folkerettslige argumenter og kilder som Høyesterett ikke går inn på i kjennelsen, og som kan gi fotfeste til kritikken av kjennelsen. Det kan imidlertid være flere grunner til at Høyesterett ikke behandler alle argumentene, for eksempel at de anser at kildene er uten nevneverdig vekt. Ensidigheten i Høyesteretts argumentasjon kan likevel svekke prejudikatverdien.

3.4 Vurdering av rettstilstanden i Norge

Utfra den ovenstående analysen fremstår rettstilstanden i Norge som uklar, og det er behov for tydeligere regelverk knyttet til ekstraterritoriell bevisinnhenting. Straffeprosesslovens bestemmelser er tause om adgangen til å hente digitale bevis utenfor Norge. Forarbeidene til straffeprosessloven gir ikke tolkningsbidrag, og det er kun etterarbeid til andre lover som tar opp spørsmålet. Etterarbeidene fremstår som usikre, motstridene og har begrenset vekt, ettersom de mangler demokratisk legitimitet og relevans etter mer enn 20 år med teknologisk- og rettslig utvikling.

Endelig avklaring fra en autoritativ kilde kom gjennom Tidal-kjennelsen. Som følge av kjennelsen må ekstraterritoriell bevisinnhenting godtas i tilgrensende tilfeller. Kjennelsen gir likevel ikke uttømmende og klare føringer for hva som er akseptabel ekstraterritoriell bevisinnhenting. En kan likevel slutte at norske myndigheter ikke kan få tilgang til data lagret i utlandet ved selvstendig inntrenging (hacking). Videre kan ikke dataene sperres eller slettes. Her kan en trolig videre slutte at dataene heller ikke kan endres. I Tidal-saken synes Høyesterett å avgrense ekstraterritoriell bevisinnhenting til saker der politiet opptrer som en passiv leser. Tidal-kjennelsen tar ikke stilling til LOC-problematikken. En kan slutte fra mer-til-mindre prinsippet at en minst kan gå like langt som der en vet dataenes posisjon, men det er uklart om det kan være utvidet tilgang til bevisinnhenting i LOC-tilfellene.

Kritikken i ettertid av kjennelsen kan så tvil om hvorvidt rettskildebildet Høyesterett baserer avgjørelsen på er riktig, og dermed også om kjennelsens prejudikatverdi. Det gjelder spesielt kritikken til Nygård og Rui om at Høyesterett har forbigått anførslene til Tidal under saksgangen.[91] Samtidig er Tidal-kjennelsen den tydeligste autoritative rettskilden på dette rettsområdet når loven og etterarbeidene er tause eller motstridene. Det er sentralt at juridisk

[91] Rui (2019) s. 262; Nygård (2021) s. 141

teori har begrenset vekt som rettskilde,[92] og at kritikken av kjennelsen også overser rettskilder og unnlater å ta stilling til alle argumentene i Høyesteretts resonnement. Dette svekker betydningen av kritikken, særlig når den juridiske teorien ikke er samstemt.

Høyesterett har ikke behandlet problemstillingen i ettertid, men Tidal-saken har blitt brukt i to senere lagmannsrettssaker ved vurdering av tilgrensende spørsmål. I LB-2021-122818 tok lagmannsretten stilling til om politiet kunne kreve data utlevert av Facebook og TikTok i forbindelse med hatefulle ytringer på nett. Lagmannsretten benyttet vurderingstemaet i Tidal-kjennelsen til å vurdere om folkeretten setter grenser for å fremme utleveringspålegg overfor et selskap foretaksregistrert i en annen jurisdiksjon. Konklusjonen var at utleveringspålegg kunne fremmes, men ikke tvangsgjennomføres uten politisamarbeid. Lagmannsretten brukte Høyesteretts resonnement i Tidal-kjennelsen aktivt ved vurderingen av om det foreligger en suverenitetskrenkelse. Faktum sammenfaller ikke med Tidal, men bruken av vurderingstemaet Høyesterett oppstilte taler for at Tidal-kjennelsen er førende for rettstilstanden i Norge - uavhengig av kritikken.

Lagmannsretten brukte også Tidal-kjennelsen i LB-2020-32690. Spørsmålet var om lotteritilsynet krenket suvereniteten til Malta når de testspilte spill på en Malta basert spillplattform. Lagmannsretten aksepterte dette, ettersom informasjonen var offentlig tilgjengelig, og testspillingen dermed ikke kunne anses som et selvstendig inngrep. Saken skiller seg fra Tidal da både selskapet og serverne befant seg i utlandet, og informasjonen var åpent tilgjengelig på internett. Likevel brukes Tidal-kjennelsen aktivt som grunnlag for lagmannsrettens vurdering.

Selv om underrettspraksis har begrenset verdi, viser praksisen at Tidal-saken aksepteres som rettsgivende for rettstilstanden i Norge for ekstraterritoriell bevisinnhenting, uavhengig av kritikken. Da kan det konkluderes med at ekstraterritoriell bevisinnhenting er akseptabelt dersom dataene kan nås fra Norge ved alminnelige tvangsmidler, og at data ikke sperres, endres eller slettes og at politiet bruker mistenktes tilgang til dataene. I LOC-tilfellene må en i det minste kunne innhente informasjon etter samme vurderingstema som gjøres gjeldende for Tidal. Grensetilfellene, både med og uten LOC, er mer utfordrende - særlig dersom det ikke foreligger alternative etterforskningshandlinger, som rettsanmodninger. Her vil trolig

[92] Eckhoff (2001) s. 270-275

hensynet til effektiv rettshåndhevelse balanseres mot suverenitetsprinsippet. Et viktig moment her kan være hvilken tilknytning dataene har til Norge, som kommentert under punkt 3.2.2.

4 Suverenitetsprinsippet som begrensing for ekstraterritoriell bevisinnhenting i folkeretten

4.1 Metode og avgrensinger

Selv om strpl. § 4 ikke gir uttrykk for at internasjonal rett har direkte virkning i Norge, er det likevel relevant å kartlegge grensene for ekstraterritoriell bevisinnhenting. Det er nyttig for å vurdere om rettstilstanden i Norge er i strid med Norges internasjonale forpliktelser, og om adgangen til ekstraterritoriell bevisinnhenting etter gjeldende norsk rett, som skissert i punkt 3.4, må avkortes. Det sentrale spørsmålet er om bevisinnhenting på tvers av landegrenser er i strid med suverenitetsprinsippet. Utgangspunktet er at enhver stat er suveren på sitt territorium, og at handlinger som påvirker et annet territorium, selv om en ikke er fysisk til stede, kan utgjøre en krenkelse.[93]

Folkeretten begrenser staters suverenitet i visse tilfeller, for eksempel går ikke en stats suverenitet så langt at den kan krenke en annen stats suverenitet.[94] Folkeretten oppstiller også unntak fra territorialprinsippet for å sikre at enkelte rettsområder ikke blir lovløse, som flaggstatsprinsippet på det åpne hav.[95] Fra dette kan vi slutte at suverenitetsprinsippet må tolkes for å oppstille en regel knyttet til ekstraterritoriell bevisinnhenting.

Folkerett dannes i hovedsak enten ved avtale eller sedvane. Ved avtale er det en frivillig konsesjon fra staten å underlegge seg internasjonale regler. Sedvanedannelse krever en relativt omfattende og ensartet praksis i tro om at det er en rettsregel (opinio juris). Denne praksisen illustrerer også konsesjon av suverenitet.[96] Ettersom suverenitetsprinsippet er jus cogens kan ikke ny rett stride mot suverenitetsprinsippet, men dette er ikke i veien for å begrense prinsippets rekkevidde, eller at en frivillig kan gi fra seg suverenitet.[97] I oppgaven

[93] Lotus-saken; Trail Smelter
[94] Evans, M. D. (2018) *International law*, 5.utg. Oxford University Press. s. 289-291
[95] Council of Europe. (2010, August 31). *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?* (Discussion paper). Economic Crime Division, Directorate General of Human Rights and Legal Affairs. Hentet fra: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df (Lest: 04.03.2024) s. 8
[96] Evans (2018) s. 90-98
[97] Vienna Convention on the Law of Treaties, 23 May 1969, 1155 UNTS 331 article 53

vurderer jeg hvordan folkeretten kan sette grenser for norsk ekstraterritoriell bevisinnhenting, med bruk av kilder fra Europa og Nord Amerika, da disse anses som mest relevante for rettstilstanden i Norge.

Når og hvor etterforskningen foregår avgjør om digital bevisinnhenting er ekstraterritoriell. Spørsmålet har ikke et entydig svar, men åpner for uenigheter rundt lovligheten av ekstraterritoriell bevisinnhenting. Data er ofte tilgjengelig fra flere innganger. Mistenkte kan nå data lagret i skyen fra egen dataterminal, men også fra enhver annen internettilkoblet dataterminal i verden. At en handling kan skje flere steder samtidig, kompliserer jurisdiksjonsspørsmålet. Det er særlig tre vanlige forståelser av hvor etterforskningshandlingen foregår. [98]

En tolkning er at stedet dataen leses er avgjørende, altså kan en laste ned data til en pc og undersøke dataen innenfor territoriet til den ransakende staten. [99] Dette kan eksemplifiseres ved at en åpner Dropbox-kontoen til den mistenkte på en pc i Norge og derfor mener at ransakelsen foregår i Norge. Den andre teorien er at etterforskningshandlingen foregår to steder samtidig. Dersom en åpner Dropbox-kontoen, vil det være en etterforskningshandling både i landet der serverne står, og i landet der informasjonen åpnes.[100] Siste tolkningsalternativ er at etterforskningshandlingen foregår når dataene blir lastet ned, og derfor skjer i landet informasjonen er lagret.[101]

I tillegg til de tre ovenstående forståelsene kan jurisdiksjonsspørsmålet kompliseres ytterligere dersom en spør om etterforskningshandlingen i det hele tatt bør knyttes til territoriet. Når innholdet fra en Dropbox-konto kan befinne seg på servere over hele verden kan det være uklart hvor dataene befinner seg. Det vanskeligjør andre og tredje tolkningsalternativ. Videre kan det innvendes at dataeierens nasjonalitet bør ha betydning, ettersom stater representerer sine rettssubjekter. Spørsmålet blir så om nasjonaliteten til eieren av Dropbox-kontoen, eller hvor selskapet Dropbox er foretaksregistrert, er avgjørende. Vi kan videre tenke oss kombinasjoner hvor både dataenes lokasjon, nasjonaliteten til dataeieren og landet der

[98] Osula, A-M. «Transborder Access and Territorial Sovereignty». *The Computer Law and Security Report* 31, no. 6 (2015): 719-35. Hentet fra: https://doi.org/10.1016/j.clsr.2015.08.003 (Lest: 04.02.2024) s. 723-725
[99] Osula (2015) s. 723-724
[100] Osula (2015) s. 724
[101] Osula (2015) s. 724-725

selskapet er foretaksregistrert blir aktuelt. For eksempel der en gir utleveringspålegg til et selskap.

Selv enkle spørsmål innenfor jurisdiksjon kan bli kompliserte ved innhenting av digitale bevis. Det er ikke noe klart eller entydig svar på hvor etterforskningshandlingen foregår i folkeretten.[102] Uklarheten tilknyttet etterforskningshandlingens lokasjon er sentral for vurderingen av suverenitetsprinsippets rekkevidde, ettersom løsningsforslagene i folkeretten varierer basert på staters forståelse av hvor og hvordan suverenitetskrenkelse oppstår.

4.2 Suverenitetsprinsippet i traktatretten

4.2.1 Budapestkonvensjonen

Innledningsvis kan traktatretten gi tolkningsbidrag til rekkevidden av suverenitetsprinsippet ved ekstraterritoriell bevisinnhenting. Norge er tilsluttet Budapestkonvensjonen, som regulerer prosess ved kriminalitet på internett. Den er betydningsfull, ettersom det er en av de største konvensjonene på rettsområdet med 71 signaturer fra land over hele verden.[103] Det er særlig artikkel 32 som er relevant, ettersom den tillater ekstraterritoriell datainnhenting dersom dataen a) er «publicly available» eller b) en person med «lawful authority to disclose the data» har samtykket. Bokstav b) åpner ikke for at norske myndigheter kan innhente data etter domstolsamtykke.

Dersom bevisinnhenting faller utenfor disse to tilfellene, som det ofte gjør, benyttes gjerne avtaler om gjensidig politisamarbeid for å innhente bevismaterialet.[104] Rui og Nygård bruker dette som argument for at ekstraterritoriell bevisinnhenting er i strid med suverenitetsprinsippet, til tross for Europarådets forutsetning om at konvensjonen ikke påvirker rettstilstanden.[105] Selv om art. 32 ikke tillater ekstraterritoriell bevisinnhenting ved domstolsamtykke bør en være varsom med slik antitetisk tolkning av rettskildene.

---

[102] Osula (2015) s. 723
[103] Council of Europe. (2024) *Chart of signatures and ratifications of Treaty 185.* Council of Europe. Hentet fra: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (Lest: 05.04.2024) (1)
[104] T-CY (2014) *Transborder access to data and jurisdiction: Options for further action by the T-CY*. Council of Europe. Hentet fra: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726e (05.04.2024) (1) s. 17-18
[105] Rui (2019) s. 261; Nygård (2021) s. 147-148; Council of Europe (2001) s. 53

Budapestkonvensjonen i seg selv åpner dermed ikke for ekstraterritoriell bevisinnhenting i samme utstrekning som Tidal-saken. [106] Motsetningsvis er det ikke rettskildemessig holdbart å konkludere at ekstraterritoriell bevisinnhenting ved domstolsamtykke er akseptert i folkeretten basert på Europarådets rapport om Budapestkonvensjonens virkeområde, som lagmannsretten og Skjold viser til i sin drøftelse av Tidal-saken.

Europarådet utformet i 2022 en tilleggsprotokoll som skal sikre bedre samarbeid for digitale bevis.[107] Protokollen kom som følge av misnøye med å benytte rettsanmodninger, ettersom lang behandlingstid medfører forsinkelser for politiet, og fare for bevisenes integritet.[108] Formålet er å sikre effektiv utveksling av digitale bevis. Dette for å ivareta staters sikringsplikt mot kriminalitet i lys av den økte mengden digitalt bevismateriale.[109] Tilleggsprotokollen er per dags dato ikke ikraftsatt ettersom kun to land har ratifisert avtalen, til tross for at 41 land har signert den. Norge har verken ratifisert eller signert avtalen.[110]

Tilleggsprotokollen sikrer effektivitet gjennom de prosessuelle reglene i art. 7-10. Her gir art. 7 rett for «competent authorities» til direkte å beordre utenlandske tjenesteleverandører til å overlevere data relevant for etterforskning. Art. 8 gir samme mulighet, men forutsetter samarbeid med lokalt politi for tilgang til mer omfattende data. Videre krever art. 9 at tjenesteleverandører overfører data til «competent authorities» gjennom «the 24/7 Network referenced in Article 35 of the Convention» om det foreligger en «emergency». Art. 10 regulerer også nødsituasjoner, men gir korte tidsfrister for nasjonale myndigheters behandling av rettsanmodninger. Rettsanmodning er unødvendig dersom en går direkte til tjenesteleverandøren som forutsatt i art. 9.

I en forklarende rapport legger Europarådet til grunn at «competent authorities» må vurderes utfra statenes egne nasjonale lover. [111] Tilleggsprotokollen stiller flere vilkår til overlevering, som formkrav til forespørselen, krav om informasjon om dataen som søkes utlevert og

[106] LB-2018-190770; Skjold (2019) s. 630; Council of Europe (2001) s. 53
[107] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) (Tilleggsprotokoll nr. 2)
[108] Council of Europe (2022) *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*. Council of Europe. Hentet fra: https://rm.coe.int/1680a49c9d (05.03.2024) s. 2-3
[109] Tilleggsprotokoll nr. 2, preamble
[110] Council of Europe. (2024) *Chart of signatures and ratifications of Treaty 224.* Council of Europe. Hentet fra: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224 (Lest: 05.04.2024) (2)
[111] Council of Europe (2022) s 14

lovkrav. Hva som kreves varierer utfra hvilken bestemmelse en benytter, for eksempel krever art. 9 og 10 at det foreligger en «emergency». Hva som regnes som et nødstilfelle er ikke definert, og må vurderes konkret utfra om risikoen er «significant and imminent». Rapporten eksemplifiserer gisselsituasjoner, pågående seksuelt misbruk av barn og i noen tilfeller terrorhandlinger. [112] Hva som kan anses som en «emergency» er dermed relativt vidt, og mange tilfeller kan falle innunder dersom det er risiko for skade eller liv.

Tilleggsprotokollen utelukker ikke bruk av tradisjonelle midler som rettsanmodninger, men tilrettelegger for raskere og mer sømløst samarbeid mellom tjenesteleverandører og politi på tvers av landegrenser. Protokollen er ikke rettskraftig, men kan likevel brukes som argumentasjon for at det ikke foreligger tilfredsstillende internasjonal sedvane for innhenting av «traffic data» og «personal data». At en opplever et behov for å regulere forholdet og at 41 land har signert, deriblant viktige stormakter innenfor data som USA, trekker i retning av at ekstraterritoriell bevisinnhenting utgjør en krenkelse av suverenitetsprinsippet.[113]

Det er likevel viktig å ikke trekke for vide slutninger ettersom protokollen ikke nødvendigvis regulerer tilfellene der dataen er tilgjengelig fra landet som etterforsker ved alminnelig innlogging, som i Tidal-saken. En annen interessant observasjon er at konvensjonen knytter seg til tjenesteleverandørers land. Egenskapene til data gjør at selv om en tjenesteleverandør er foretaksregistrert i for eksempel Irland, vil ikke dataene nødvendigvis befinne seg i Irland, eller i det hele tatt innenfor Europa. Konvensjonen synes etter min vurdering ikke å ta stilling til denne problematikken.

4.2.2 CLOUD Act og E-evidence

Europarådet er ikke de eneste som har forsøkt å gjøre overlevering av digitale bevis mer sømløst. Både den europeiske union (EU) og USA har kommet opp med egne løsninger på problemet. Deres løsninger er relevante, ettersom EU og USA er etableringsland for mange store skylagringsleverandører. CLOUD Act, en amerikansk føderal lovgivning om grenseoverskridende data, ble opprettet i kjølvannet av «Microsoft Ireland»-saken. Spørsmålet i rettsaken var om amerikanske etterforskere kunne pålegge Microsoft å utlevere brukerinformasjon lagret i Irland i forbindelse med en narkotika etterforskning. Under

[112] Council of Europe (2022) s. 8
[113] Council of Europe (2024) (2)

saksgangen i det amerikanske rettssystemet ble CLOUD Act vedtatt, loven klargjorde den amerikanske rettstilstanden, og saken ble avvist av amerikansk Høyesterett ettersom rettsspørsmålet manglet relevans.[114] CLOUD Act § 2713 stadfester at amerikanske myndigheter kan kreve at amerikanske tjenesteleverandører utleverer data, uavhengig av dataens lokasjon. Utleveringsretten er begrenset til informasjon om amerikanske innbyggere, uansett lokasjonen. [115] Loven gir inntrykk av at amerikanerne mener det er tjenesteleverandøren som er avgjørende ved jurisdiksjonsspørsmålet.

CLOUD Act åpner for bilaterale avtaler om datatilgang gjennom § 2523. Avtalene sikrer gjensidig tilgang til informasjon om personer med særlig tilknytning til det ene avtalelandet fra tjenestetilbydere basert i det andre avtalelandet. Dette er spesielt lukrativt for andre land, ettersom USA er hjemlandet til mange store tjenestetilbydere. Det gir også USA tilgang til nisjelagringstjenester i andre land. Verken CLOUD Act eller bilaterale avtaler gir USA og avtalepartnere ubetinget utleveringsrett. Lovverket krever et alvorlig lovbrudd, tilfredsstillende personvern- og rettssikkerhetsgarantier og at personen som etterforskes har tilstrekkelig tilknytning til landet som ber om dataene.[116] Bilaterale avtaler åpner også for å forhandle særbestemmelser. Samlet skal dette sikre balansen mellom hensynet til privatlivet til den mistenkte og effektiv etterforskning - ved å etablere en direktelinje mellom myndighetene i et land og tjenestetilbyderne i et annet. I skrivende stund har kun Storbritannia og Australia inngått bilaterale avtaler med USA, men flere land og EU vurderer å forhandle frem avtaler.[117]

EU har likevel uttrykt at de, til tross for vurdering av inngåelse av bilaterale avtaler, vil ta rettslige skritt, dersom USA henter informasjon lagret i EU med hjemmel i CLOUD Act. De fremstår dermed skeptiske til den amerikanske jurisdiksjonsforståelsen.[118] EU stoppet også midlertidig samarbeidet med USA om en felles digital bevisutvekslingsavtale under arbeidet

[114] Gallagher, P. J. (2019) The CLOUD ACT: Mooting the Microsoft Ireland Case, but Not Forecasting Clear Skies Just Yet. Columbia Law Review. Hentet fra: https://journals.library.columbia.edu/index.php/CBLR/announcement/view/161 (Lest: 05.03.2024)
[115] CLOUD Act s. 2202-2212
[116] CLOUD Act s. § 2523
[117] Propp, K. (2023) Navigating Toward an EU-U.S. Agreement on Electronic Evidence. Lawfare. Hentet fra: https://www.lawfaremedia.org/article/navigating-toward-an-eu-u.s.-agreement-on-electronic-evidence (05.03.2024)
[118] European Data Protection Supervisor. (2019) ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence. Hentet fra: https://www.edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf (Lest: 05.04.2024) s. 8-9

med sin egen lovgivning (E-evidence) som skal sikre bedre flyt av digitale bevis innad i EU.[119] Pakkeløsningen, med både forordning og direktiv, ble publisert i 2023, og blir rettskraftig i 2026.[120]

E-evidence muliggjør å henvende seg direkte til tjenesteleverandører innenfor EU for å be om sikkerhetskopiering av data, eller utlevering av data direkte til det etterforskende landet. Dette gjelder uavhengig av hvor dataen er lagret. Ved sikkerhetskopiering bevares data i minst 60 dager mens myndighetene i det etterforskende landet vurderer behovet for utlevering.[121] Utleveringsbegjæring gir tjenesteleverandøren 10 dagers frist til å levere dataene. I nødstilfeller kan fristen forkortes til 8 timer.[122] Data som utleveres er ikke begrenset, og en kan kreve «content data», «traffic data» og «personal data». Hvilke data som forespørres bestemmer hvem som kan be om dataen, men en domstol kan be om alle typer data.[123]

Selv om E-evidence gir relevante myndigheter rett til data direkte fra tjenesteleverandører, må forespørrende myndighet, uten ugrunnet opphold, informere relevant myndighet i tjenesteleverandørens etableringsland og personen dataen gjelder. Det sikrer berørte parters informasjonstilgang. Utviklingen av E-evidence var upopulær og motstanderne argumenterte med at det er svake rettssikkerhetsgarantier.[124]

Norge har ingen bilateral avtale med USA gjennom CLOUD Act, og er ikke tilsluttet E-evidence. Begge formene for avtaler er relativt små og regionale avtaler som ikke i seg selv utgjør en internasjonal presedens for digital bevishåndtering. Likevel er det interessant at store dataaktører, som EU og USA, ser behov for å danne eget lovverk om bevisoverlevering. Det kan gi uttrykk for at rettsoppfatningen er at selvstendig innhenting av grenseoverskridende digitale bevis ikke godtas. Bekymringer rundt privatliv og rettssikkerhet ved fri flyt av digitale bevis er søkt ivaretatt i avtalene, for eksempel gjennom informasjonsplikten i E-evidence. Ut fra ovenstående diskusjon kan en trolig slutte at

[119] Propp (2023)
[120] Europaparlamentets og Rådets forordning (EU) 2023/1543; Europaparlamentets og Rådets direktiv (EU) 2023/1544
[121] European Commission (2018) Frequently Asked Questions: New EU rules to obtain electronic evidence. Hentet fra: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345 (Lest.05.03.2024)
[122] European Commission (2018)
[123] European Commission (2018)
[124] Propp (2023)

selvstendig bevisinnhenting av grenseoverskridende data ikke kan anses akseptabelt i de fleste tilfeller.

Både CLOUD Act og E-evidence knytter seg til tjenesteleverandørene, og ikke territoriet, der dataene er lagret. Denne presisjonen er trolig av praktiske grunner, ettersom dataen kan være lagret hvor som helst og flyttes raskt. Det kan gjøre det nærmest umulig å vite hvilket land en skal henvende seg til. Dette var også et sentralt poeng i Høyesteretts argumentasjon for å tillate grenseoverskridende datainnhenting i Tidal-saken.[125]

Ved å stille utleveringskravet til tjenesteleverandøren omgås problematikken rundt lokalisering av data, inkludert LOC-tilfellene. Lokasjonen må ikke identifiseres, kun tjenesteleverandøren. Løsningen i CLOUD Act og E-evidence fremstår som problematisk dersom en bygger på et territorialt suverenitetsprinsipp, ettersom de fleste tjenesteleverandører har mange dataparker og lagrer data over hele kloden. Reguleringene forflytter kostnader og risiko tilknyttet tredjelandskonflikter til tjenesteleverandøren, uten å bidra til mer klarhet. Dersom tjenesteleverandører har servere utenfor medlemsland i E-evidence eller CLOUD act, vil det ved utlevering fremdeles kunne oppstå en suverenitetskrenkelse i tredjelandet. For å unngå denne problematikken må alle land som lagrer data være med i avtalen og godta muligheten for utlevering av data lagret på deres territorium.

4.3 Suverenitetsprinsippet i sedvanerett

4.3.1 Kartlegging av statenes rettsoppfatning

Ettersom Norge ikke er part til en konvensjon som regulerer ekstraterritoriell bevisinnhenting, er det aktuelt å vurdere om det foreligger internasjonal sedvanerett som kan være bestemmende for norsk rett. Sentralt for om det foreligger sedvanerett er statenes rettsoppfatning når det kommer til digital bevisinnhenting på tvers av landegrenser. Her er det aktuelt å se til rapporter, konvensjoner, uttalelser og lignende for å kartlegge rettsoppfatningen.[126] Ettersom konvensjoner er sett på i det ovenstående vil ikke dette gjentas. Det er særlig to rapporter, Tallinn-manualen og United Nations Office on Drugs and Crime

[125] HR-2019-610-A avsnitt 35-38
[126] Evans (2018) s. 93

(UNDOC) sin rapport fra 2013, som gir en grundig gjennomgang av rettsoppfatningen internasjonalt.[127]

UNDOC-rapporten undersøker både praksis og rettsoppfatning blant stater, og er derfor aktuell å se til for å avgjøre om det foreligger sedvane.[128] Minst 2/3 av verdens land svarte at det ikke er adgang til ekstraterritoriell bevisinnhenting.[129] Dette kan bety at det foreligger en presumpsjon om territoriell suverenitet ved digital bevisinnhenting. En mulig feilkilde er at undersøkelsen ikke definerte ekstraterritoriell bevisinnhenting entydig.[130] Noen stater har vist til rettsanmodning som unntak der bevisinnhenting vil være lovlig likevel. Dette illustrerer hvorfor mangelen på definisjon av ekstraterritoriell bevisinnhenting i rapporten er problematisk, da politisamarbeid er den tradisjonelle måten for å unngå suverenitetskrenkelse ved analoge bevis.

Andre land som responderte på UNDOC-rapporten gav utrykk for at en må kunne hente informasjon dersom situasjonen er «urgent».[131] Det gis i rapporten ikke videre informasjon om hva som menes med «urgent», og hvor langt etterforskere kan gå i disse situasjonene.[132] Videre gir enkelte uttrykk for at man kan gå frem uten samtykke der det foreligger LOC.[133] En mulig begrunnelse er at rettsanmodning er en ubrukelig løsning uten dataens lokasjon. Avslutningsvis gir UNDOC-rapporten uttrykk for at digital bevisinnhenting utgjør et komplekst rettsområde. Det er særlig to motstående hensyn som gjør seg gjeldende i statenes svar i undersøkelsen: Hensynet til effektiv rettshåndhevelse og hensynet til territorial- og suverenitetsprinsippet.[134]

Tallinn-manualen samler meningene til et stort utvalg med eksperter i internasjonal rett, i regi av NATO. Utgangspunktet er dermed at rapporten reflekterer enighet i juridisk teori fra forskjellige land. Noen stater har også kommet med uformelle innspill under sammenfatningen.[135] Rapporten er oppbygd som en rekke regler gjeldende i cyberspace med

---

[127] Schmitt (2017); United Nations Office on Drugs and Crime (UNDOC). (2013) *Comprehensive Study on Cybercrime. Vienna.* Hentet fra: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-CRP05/Comprehensive_study_on_cybercrime.pdf (Lest: 05.03.2024) (2013)
[128] UNDOC (2013) s. xxiii-xxvi
[129] UNDOC (2013) s. 220
[130] UNDOC (2013) s. 220
[131] UNDOC (2013) s. 216-220
[132] UNDOC (2013) s. 220
[133] UNDOC (2013) s. 216-220
[134] UNDOC (2013) s. 222-223
[135] Schmitt (2017) s. 3-8

utfyllende kommentarer til hver regel. Regel 11 er aktuell for grenseoverskridende prosess- og etterforskningsregler. Den gir i utgangspunktet uttrykk for at territorial- og suverenitetsprinsippet gjelder, også ved etterforskning i cyberspace, med mindre det foreligger et eksplisitt unntak i internasjonal rett, eller samtykke til å utøve jurisdiksjon på den andre statens territorium.[136] Dette utgangspunktet synes å være svært likt rettsoppfatningen til statene i UNDOC-rapporten.

I kommentarene til regel 11 åpnes det likevel for at det finnes områder innenfor etterforskningsprosess som ikke omfattes av det territorielle suverenitetsprinsippet i regel 11. Dette står i kontrast til UNDOC-rapporten, og er mer i tråd med Høyesteretts argumentasjon i Tidal-saken. Spesialistene skriver i kommentarene at det avgjørende for om digital bevisinnhenting utgjør en suverenitetskrenkelse, er om informasjonen var tilsiktet tilgjengelig fra den etterforskende staten. Dette gjelder uavhengig av om informasjonen er offentlig tilgjengelig eller krever innlogging. Ekspertenes kommentarer åpner dermed for at en i like stor grad kan innhente informasjon fra en brukerkonto som ved å søke på internett, så lenge informasjonen som innhentes er tilsiktet tilgjengelig fra det etterforskende landets territorium.[137]

Utvalget forutsetter at en ikke kan pålegge en tjenesteleverandør i et annet land å utlevere informasjon direkte. Her må en ty til de alminnelige reglene for rettsanmodning. En kan heller ikke foreta en selvstendig inntrenging i et datasystem utenfor statens territorium, for eksempel ved å hacke seg inn i en datamaskin som befinner seg i en annen stat.[138] Utvalget oppstiller dermed klare grenser for unntakene fra suverenitetsprinsippet. Enhver datainnhenting vil ikke kunne godtas. Rettsoppfatningen det gis uttrykk for i Tallinn-manualen, er nærmest tilsvarende den rettstilstanden Høyesterett skisserer i Tidal-saken. Dette kan forklares med at Høyesterett har vektlagt rapporten under arbeidet med Tidal-saken. Tallinn-manualen er imidlertid taus om LOC-tilfellene. Der unntakene i regel 11 gjør seg gjeldende fremstår ikke dette som problematisk, da en kan slutte fra mer-til-mindre på samme måte som i den norske rettstilstanden beskrevet under punkt 3.4. Problemet oppstår når en befinner seg i de tilfellene som vanligvis vil kreve en rettsanmodning til staten informasjonen er lagret i.

[136] Schmitt (2017) s. 66-67
[137] Schmitt (2017) s. 69-70
[138] Schmitt (2017) s. 69-70

4.3.2 Vurdering av statenes rettsoppfatning

I lys av UNDOC-rapporten, Tallinn-manualen og konvensjonsretten som er gjennomgått under punkt 4.2 kan det sluttes at rettsoppfatningen blant statene er at det territorielle suverenitetsprinsippet gjelder også når det kommer til digital ekstraterritoriell bevisinnhenting. Utgangspunktet er dermed at det ikke er adgang til å gjennomføre bevisinnhenting som utgjør etterforskningshandlinger på et annet territorium. Det er imidlertid gjennomgående forskjeller mellom konvensjonene og statenes uttrykte meninger på viktige punkter, som hvor effekten av en eventuell bevisinnhenting foregår og dermed også hvem som kan samtykke.

I Tallinn-manualen og UNDOC-rapporten fremstår det som avgjørende hvor informasjonen rent fysisk er lagret, mens i CLOUD Act og tilleggsprotokollen til Budapestkonvensjonen fremstår det som avgjørende hvor tjenesteleverandøren som lagrer dataene er foretaksregistrert. E-evidence skiller seg ut ved at den gir uttrykk for begge forståelsene, ettersom den åpner for at en utleveringsordre kan imøtegås der det kommer i strid med interessene til et tredjeland. Forskjellen kan til dels forklares med at det er tjenesteleverandørens plikt å operere på en måte som hindrer tredjelandskonflikter. Med dagens kommunikasjon og datalagring er dette en urealistisk forventing til tjenesteleverandører, ettersom det foreligger regionale føringer, men ikke verdensomspennende enighet. Et eksempel på dette er for eksempel at en datapark i Skien kun vil kunne benyttes til å lagre norske kunders data, ettersom Norge ikke har overføringsavtale med noen andre land.

Videre er det ikke klare føringer for hvor grensen for rettsbrudd går. I UNDOC-rapporten ser en at land definerer ekstraterritoriell bevisinnhenting ulikt. Tallinn-manualen tillater for eksempel bevisinnhenting som det ikke gis uttrykk for at det er adgang til å innhente i Budapestkonvensjonen, CLOUD Act eller E-evidence. At grensen for hva som kan anses som lovlig bevisinnhenting er uklar er spesielt interessant når faktum er at det fremfor internasjonale domstoler aldri har blitt fremsatt en tvist om brudd på suverenitet ved digital bevisinnhenting. Suverenitet er typisk et rettsområde hvor statene er årvåkne for å beskytte sine interesser og hvor grensene hyppig blir testet i internasjonale domstoler.[139] Det er derfor

[139] Currie (2017) s. 71

underlig at det ikke er blitt gjort når det kommer til digital bevisinnhenting. Det kan kanskje bero på at skylagring utenfor landegrensene fortsatt er relativt nytt.

4.3.3 Etterlevelse av rettsoppfatningen

Praksis er den andre delen av sedvane. UNDOC-rapporten la til grunn at 20-50 % av verdens land benyttet digital ekstraterritoriell bevisinnhenting ved etterforskning. Europa toppet statistikken, hvor rundt 50 % av landene innhentet bevis utenfor landegrenser.[140] Det er utvilsomt at bruken av skylagringstjenester og sosiale medier har økt etter at rapporten ble utgitt i 2013, og at flere bevis enn tidligere er digitale.[141] Dette kan tyde på at ekstraterritoriell bevisinnhenting er mer utbredt i dag, på grunn av behovet for å sikre effektiv rettshåndheving. Det påpekes også i Tallinn-manualen. På den andre siden, definerer ikke UNDOC-rapporten ekstraterritoriell bevisinnhenting. Tallene representerer dermed ikke nødvendigvis kun selvstendig innhenting av digitale bevis uten aksept i andre territorier. Dette kan medføre at rapporten gir utrykk for at et falskt høyt antall stater benytter seg av ekstraterritoriell bevisinnhenting.[142]

4.4 Vurdering av rettstilstanden internasjonalt

Utfra rettskildene gjennomgått under punkt 4.2 og 4.3 kan det sluttes at det territorielle suverenitetsprinsippet til en viss grad gjør seg gjeldende, også på bakgrunn av folkerettslig sedvane. Det foreligger en gjennomgående holdning til at det er forbudt å innhente bevis direkte fra en annen stat. Statene handler deretter ved å opprette konvensjoner, og i varierende grad å unngå å hente bevis direkte. Det er derimot uklart hvor langt suverenitetsprinsippet kan strekkes.

Det foreligger ikke en klar nok opinio juris, eller etterlevelse, til å oppstille et generelt forbud mot alle former for ekstraterritoriell bevisinnhenting av digitale bevis på bakgrunn av folkerettslig sedvane. At sedvaneretten ikke gir klare svar for grensene, er ikke overraskende når en ikke synes å kunne komme til enighet rundt fundamentale konsepter som hvor en handling har effekt og hvem som kan samtykke til innhentingen av bevisene. Rettstilstanden

[140] UNDOC (2013) s. 219
[141] Satistisk sentralbyrå. (2024) *Bruk av nettskytjenester (prosent), etter tjenestetype, forvaltningsnivå, antall innbyggere, statistikkvariabler og år.* Hentet fra: https://www.ssb.no/statbank/table/12032/tableViewLayout1/ (05.03.2024)
[142] UNDOC (2013) s. 219

fremstår dermed som uklar utover at det ikke er adgang til å gjennomføre selvstendig inntrenging ved for eksempel hacking, eller å beordre utlevering direkte fra en tjenesteleverandør. Dersom data er åpent tilgjengelig på nett kan det innhentes fritt uten suverenitetsbegrensninger.

Det er uklart om en kan innhente informasjon som ikke er åpent tilgjengelig på nett, men som kan innhentes fra den etterforskende stats territorium. Virkeområdet for suverenitetsprinsippet er også utydelig der traktatretten forutsetter at rettsanvender må benytte rettsanmodning, ettersom avtalene forutsetter at rettsanmodningene skal til landet hvor tjenestetilbyderen er registrert. Utfra en tradisjonell forståelse av suverenitetsprinsippet, hadde det vært naturlig at en rettsanmodning måtte fremsettes til landene der dataene var lagret. En slik forståelse åpner imidlertid for nye utfordringer, som at det kan ta lang tid, eller være utfordrende å vite hvor den konkrete dataen er lagret på ethvert tidspunkt.

Spørsmålet om hvor langt en kan gå i LOC-tilfeller har ikke noe entydig svar i de gjennomgåtte kildene. Dersom tjenesteleverandøren eier dataene, og landet der tjenesteleverandøren er lokalisert kan samtykke, blir rettsspørsmålet noe lettere. Det kan likevel oppstå problemer der en har flere filialer som operer i ulike jurisdiksjoner. Dersom tjenesteleverandørlandet blir avgjørende, åpner det videre for at enkelte stater kan praktisere ingen utlevering og sekretessebelagte ordninger som kan være attraktivt for kriminelle miljøer. Dette kan medføre reguleringer som minner om «flag of convenience» i shipping, hvor en får et uregulert marked. Særlig kan dette gjøre seg gjeldende om det ikke foreligger internasjonale avtaler med standarder for utlevering.

Noe av bakgrunnen for at det er vanskelig å si at territorial- og suverenitetsprinsippet forbyr ekstraterritoriell jurisdiksjon for digital bevisinnhenting, er at prinsippene ble utviklet for analoge bevis. Anvendelse på digitale bevis er ineffektivt, og lager enorme utfordringer tilknyttet effektiv rettshåndhevelse.[143] Uklarheten rundt rettstilstanden fremstår som et resultat av at rettstilstanden henger etter moderniseringen av samfunnet, og at rettsutviklingen enda ikke fullt ut innbefatter digitaliseringen av samfunnet.

Resultatet er at det blir uklart hvor langt suverenitetsprinsippet kan strekkes når det kommer til digitale bevis. Dette kommer dels til uttrykk gjennom de ulike reguleringene i traktatretten,

[143] Council of Europe (2022) s. 2-3

og de sprikende rettsoppfatningene til statene. Traktatretten og rettsoppfatningen gir likevel uttrykk for at en bør utvise forsiktighet med selvstendig bevisinnhenting, som i Tidal-saken, da kun Tallinn-manualen åpner eksplisitt for dette.

Bruken av reelle hensyn i fastsettelsen av rettsregler, som hensynet til effektiv rettshåndhevelse, er en særnorsk tradisjon. Selv om slike hensyn kan virke motiverende for utviklingen av internasjonale regelverk, som for eksempel ekstradiksjonsavtaler og avtaler om gjensidig politisamarbeid, har de begrenset vekt ved vurderingen av om det foreligger internasjonal rett.[144] Utgangspunktet er at en ikke kan gjøre ekstraterritoriell bevisinnhenting. At noen stater gjør det av hensyn til effektiv rettshåndhevelse, er ikke tilstrekkelig til å oppstille en rett til slik ekstraterritoriell rettshåndhevelse. Dette må heller anses som et symptom på at rettsutvikling er nødvendig.

[144] Statute of the International Court of Justice. (24. september 1945). 59 Stat. 1031, TIAS 9939. (ICJ-statuettene)

5 Norsk og internasjonal rett sammenholdt og mulig rettsutvikling

5.1 Retten til ekstraterritoriell bevisinnhenting i Norge bør innskrenkes i lys av folkeretten

Sammenligner vi funnene under punkt 3.4 og 4.4 ser vi at norsk rett og folkeretten i stor grad bygger på de samme rettskildene. Store deler av rettsforståelsen er også lik. Både norsk rett og folkerett har som hovedregel at en ikke kan tillate ekstraterritoriell bevisinnhenting, ettersom dette vil utgjøre en suverenitetskrenkelse. Norsk rett skiller seg fra folkerett gjennom vurderingstemaet Høyesterett fremsatte i Tidal-kjennelsen: «norske rettsanvendere [må] på selvstendig grunnlag ta stilling til om bruk av tvangsmidler krenker en annen stats suverenitet» for å vurdere om ekstraterritoriell bevisinnhenting kan aksepteres i noen tilfeller. En finner ikke et motstykke i folkeretten som tillater ekstraterritoriell bevisinnhenting i visse tilfeller - selv om det er kilder som argumenterer for å åpne for det, som pekt på i punkt 4.3. En mulig grunn til forskjellen, er at det i norsk rett er definert hvor håndhevelseshandlingen finner sted ved ekstraterritoriell bevisinnhenting. Som norsk rettsanvender stiller Høyesterett et krav til selvstendighet gjennom vurderingstemaet, noe som kan by på utfordringer knyttet til rettsenhet, rettssikkerhet og internasjonalt samarbeid, til tross for at en kan støtte seg på vurderingsmomentene oppstilt av Høyesterett i Tidal-saken.

Høyesterett konkluderer med at det avgjørende for jurisdiksjonsspørsmålet, er hvor dataterminalen som laster ned de digitale bevisene befinner seg, ikke bevisenes lokasjon. Etter forståelsen lagt til grunn i Tidal-saken, får etterforskning som ransakelse eller beslag kun effekt i en annen stat dersom data endres, politiet gjør en selvstendig inntrenging eller lignende. I nye tilfeller må rettsanvendere selv vurdere om tilfellet ligger nært nok opp mot Tidal-saken til å forsvarlig konkludere at ikke suverenitetsprinsippet krenkes. I folkeretten er det ikke like klart og entydig hvor håndhevelseshandlingen får effekt. Dette kan være en forklaring på hvorfor det er vanskeligere å oppstille unntak fra suverenitetsprinsippet i folkeretten, da en ikke er enig om hvordan et slikt unntak bør utformes.

En annen viktig forskjell er at reelle hensyn ikke er en rettskilde ifølge ICJ-statuettene, som gjelder som sedvanerett.[145] Hensynet til effektiv rettshåndhevelse var sentralt i Høyesteretts avgjørelse i Tidal-saken. Det skiller seg fra rettskildebildet i folkeretten. I folkeretten fremstår hensynet til effektiv rettshåndhevelse som et rettspolitisk ideal. Der det ikke foreligger effektiv rettshåndhevelse kan det tolkes som et symptom for at det er behov for rettsutvikling. Det synes å være tilfelle for ekstraterritoriell bevisinnhenting.

På grunn av behovet for rettsutvikling ser man at flere stater, inkludert Norge, tøyer grensene for hva som er akseptabelt i lys av suverenitetsprinsippet, men praksisen er ikke tilstrekkelig til å utgjøre sedvanerett. Grensene for hvor langt suverenitetsprinsippet strekker seg fremstår derfor uklart i folkeretten. Vi kan likevel konkludere at Norge tillater ekstraterritoriell bevisinnhenting utover hva som er akseptabelt i folkeretten basert på konklusjonen i punkt 4.4. For å opprettholde sine folkerettslige forpliktelser og forebygge konflikt kunne Norge dermed isolert sett innskrenket retten til ekstraterritoriell bevisinnhenting etter strpl. § 4.

Problemet med at Norge innskrenker retten til selvstendig ekstraterritoriell bevisinnhenting etter strl. § 4 er at det ikke foreligger en klar internasjonal konsensus om hvordan en skal innhente bevis. Dersom vi legger til grunn at tradisjonelle rettsanmodninger ikke er tilstrekkelig effektive, så vil avkortning av retten til ekstraterritoriell bevisinnhenting kunne bli svært utfordrende for effektiv rettshåndhevelse. Det er dermed utfordrende å rettferdiggjøre en avkortning av norsk rett til ekstraterritoriell bevisinnhenting etter strpl. § 4 i lys av hensyn til Norge som rettstat. Dersom Norge ikke avkorter retten til ekstraterritoriell bevisinnhenting, bør vi likevel utvise reservasjon i lys av folkeretten. Ved vurdering av adgangen til å innhente bevis i tilfeller som avviker fra Tidal-saken, bør en utvise forsiktighet og benytte en konservativ forståelse av Tidal-sakens utgangspunkter. Når det kommer til LOC-tilfellene fremstår rettstilstanden i Norge og folkeretten som uklar, og det er derfor vanskelig å gi et klart svar på om rettstilstandene samsvarer.

5.2 Drøftelse av mulig internasjonal regulering

Ut fra dagens rettstilstand er det et klart behov for rettsutvikling for å sikre en entydig og samsvarende praksis nasjonalt og internasjonalt. Rettsutviklingen internasjonalt kan gå ulike veier. En retning er å tillate bevisinnhenting for alle i samsvar med dagens norske rettstilstand

[145] ICJ-statuettene artikkel 38

etter Tidal-saken. Dette ville løst mange utfordringer i forbindelse med effektivitet fordi en i samme grad som ved analog ransakelse kan benytte mistenktes egen tilgang for å ransake og beslaglegge bevismateriale på nett. En utfordring med fri ekstraterritoriell bevisinnhenting er at bevisinnhentingsadgangen bygger på et lands interne lover for å bestemme hvor langt politiet kan gå. I Norge har denne ordningen fungert godt til nå, ettersom vi har høy tiltro til politiet og generelt gode rettssikkerhetsgarantier.

Dersom vi ser for oss fri ekstraterritoriell bevisinnhenting på en global skala, vil det inkludere totalitære land med dårlige rettssikkerhetsgarantier. Her vil det være opp til de respektive landene å bestemme hva som utgjør kriminalitet og hvor langt en kan gå i etterforskningen - så lenge etterforskningen ikke påvirker landet der dataen er lagret. Da kan en se for seg rettferdiggjøring av overvåkning som kan krenke retten til privatliv for alle staten mener har tilstrekkelig tilknytning til landet, og som er mistenkt for en forbrytelse som etterforskes. Internasjonal aksept for ekstraterritoriell bevisinnhenting av en slik rekkevidde kan være konfliktskapende og fremstår også som problematisk, særlig sett i lys av staters tradisjonelle uvillighet til å gi fra seg suverenitet.[146]

En kan også se for seg et strengt territorielt suverenitetsprinsipp som setter klare føringer for at folkeretten ikke aksepterer ekstraterritoriell bevisinnhenting. Dette vil hindre eventuell misbruk av data lagret i en annen jurisdiksjon. Samtidig vil totalforbud mot ekstraterritoriell bevisinnhenting være et stort hinder for effektiv rettshåndheving innad i en stat. Utfra den digitale utviklingen er det sannsynlig at vi går mot en fremtid hvor en enda større del av bevismaterialet vil være digitalt, og trolig på servere utenfor Norges landegrenser. For å kunne etterforske disse sakene og fange opp lovbrudd som narkotikasalg, overgrep og utpressing, kreves det at en innhenter bevis som er lagret i utlandet.

I dag må en sende rettsanmodning med brevpost til den aktuelle myndigheten i landet en ønsker skal utlevere dataen og vente på at de kontakter tjenesteleverandøren.[147] Det samme vil trolig gjelde ved et strengt territorielt suverenitetsprinsipp. I beste fall fører det til forsinkelser i etterforskningen, ettersom tidsestimatet for å innhente slike opplysninger etter reglene i

[146] Currie (2017) s. 71
[147] Justis- og politidepartementet, Rundskriv G-19/2001 om Internasjonalt rettslig samarbeid: Gjensidig hjelp i straffesaker og utlevering av lovbrytere (1. august 2001), Hentet fra: https://www.regjeringen.no/globalassets/upload/kilde/jd/rus/2001/0020/ddd/pdfv/139144-g192001.pdf (25.03.2024) s. 12

Budapestkonvensjonen er 6-24 måneder.[148] Dette tidsperspektivet kan bety at bevis går tapt som følge av datas flyktige natur. Selv om beviset kan innhentes, vil det kunne føre til lavere tiltro til rettssystemet i lys av prinsippet om at «justice delayed is justice denied». For i det hele tatt å kunne be om datautlevering må det også foreligge samarbeidsavtaler med landene der data er lagret. For å kunne fortsette å ha et strengt territorielt suverenitetsprinsipp forutsetter realitetene dermed rettsutvikling i form av bedre internasjonalt samarbeid om utlevering av data lagret på servere i utlandet.

Det internasjonale samarbeidet har allerede startet med Budapestkonvensjonen, og har fortsatt i USA og Europa med henholdsvis CLOUD Act og E-evidence. Norge har foreløpig ikke tatt særlig del i denne utviklingen. Dette mener jeg er et feilsteg. Det er uomtvistelig at ekstraterritoriell bevisinnhenting er viktig, og kommer til å bli enda viktigere i fremtiden. Samtidig er det lite trolig at nasjonalstatene vil få etablert en internasjonal sedvane om rett til ekstraterritoriell bevisinnhenting innen rimelig tid. Vi har videre antatt at verken Norges ordning eller et strengt territorielt suverenitetsprinsipp vil være funksjonelt på et internasjonalt plan. Da må problemet løses gjennom internasjonale avtaler for å balansere hensynene til effektiv etterforskning og rettssikkerhet. Arbeidet med de nevnte avtalene er en begynnelse, men avtalene er langt fra optimale, da avtalenes beskaffenhet avhenger av regionale og bilaterale forhold, og de mangler internasjonal konsensus.

5.3 De lege ferenda

5.3.1 Multilaterale avtaler

For å drive rettsutviklingen videre er det sentralt å komme til enighet om hvem som kan samtykke til innhenting av bevis i utlandet, og i hvilke tilfeller det er nødvendig. Dersom vi legger til grunn at utgangspunktet er at ekstraterritoriell bevisinnhenting har effekt i land dataen er lagret i, blir det komplisert å innhente bevisene. CLOUD Act og E-evidence synes å være på rett spor med å gi klare føringer og effektive måter for å innhente bevis ved å knytte aksept til tjenesteleverandøren, ikke territorium. Om dette skal fungere på et internasjonalt plan må dataene kun være lagret i landene som er med i avtalen, og derfor må et tilstrekkelig

[148] Transborder Group of the Cybercrime Convention Committee (T-CY) (2014) *T-CY assessment report: The mutal legal assistance provisions of the Budapest Convention on Cybercrime.* Council of Europe. Hentet fra: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c (Lest: 25.03.2024) (2) s. 123.

antall relevante land delta. Det er også viktig å sikre at avtalen er åpen og god nok til at ulike stater velger å tiltre avtalen i stedet for å ta seg til rette ved ekstraterritoriell bevisinnhenting.

Fordelen med knytte dataene til tjenesteleverandør i stedet for territorium er at en ikke trenger å lokalisere dataene. Tjenesteleverandørene har evne til å gi ut data når politiet ber om det, og kan ansette ressurser som gjør at dette kan gjøres raskere enn med dagens ordninger. Ved å hoppe over postgangen og byråkratiet tilknyttet rettsanmodninger sparer en verdifull tid som illustrert i CLOUD Act og E-evidence.

En negativ side ved en slik ordning er at det pålegger tjenesteleverandører en byrde i form av ekstra kostnader for å kunne sikre effektiv utlevering innenfor rammene av en eventuell internasjonal avtale. Samtidig er heller ikke dagens noe uklare ordning optimal for tjenesteleverandørene. De kan havne i en situasjon der de pålegges å utlevere data til politiet etter et lands lover, men ved å utlevere dataene bryter de loven i landet der dataene er lagret, eller der brukeren er basert. Dette er problemstillingen som refereres til som tredjelandproblemer i E-evidence forordningen.[149] En avtale som forplikter tjenesteleverandørene kan medføre kostnader og byrder for dem, men de får til gjengjeld fordelen av å kunne forholde seg til en klar rettstilstand og klare retningslinjer.

Selv om det er klart at en ikke fritt frem kan ha adgang til data og fremdeles ivareta rettssikkerheten, betyr ikke det at adgang til data bør knyttes til territorium. Basert på dataens egenskaper er det irrelevant hvor den er lagret. I en internasjonal avtale gir det mening å knytte utlevering til staten der tjenesteleverandøren er etablert. Etableringsstaten har det beste grunnlaget for å lage entydig regelverk for tjenesteleverandøren og for å kontrollere etterfølgelse. Når data effektivt kan utleveres av tjenestetilbyderen uten brukers bidrag, gir det praktisk mening å knytte data til tjenesteleverandøren. Gjennom internasjonale avtaler kan en knytte vilkår til når og hvordan tjenesteleverandøren skal utlevere data. I en avtale kan det legges inn insentiver for land med tjenesteleverandører til å ivareta rettssikkerhetsgarantier og kontroller, men det vil trolig også være viktig for tjenesteleverandører for å ivareta et godt omdømme.

[149] Propp (2023)

5.3.2 Norsk deltagelse i multilateralt samarbeid

En ideell avtale vil omfatte alle verdens land, og ha en god balanse mellom effektivitet, personvern og rettssikkerhet. Foreløpig foreligger det ikke en ideell løsning. Likevel ser vi at utviklingen av løsninger som E-evidence og CLOUD Act har kommet langt i forsøket på å balansere disse hensynene og skape en innovativ løsning. Norge kan trolig best minimere fremtidige internasjonale konflikter, og sikre egne innbyggeres personvern og rettssikkerhet, ved å bli med i en av disse avtalene. E-evidence er mest nærliggende, gitt Norges EØS-samarbeid. Avtalen er langt fra ideell med tanke på rettssikkerhetsgarantier, personvern og effektiv etterforskning, likevel gir E-evidence klare føringer og muligheten til å være med på videreutvikling av prosessuelle regler som kan håndtere den teknologiske utviklingen.

En annen stor fordel med avtaler er at de kan endres. Ved å melde seg inn i E-evidence, eller ved å lage en bilateral avtale under CLOUD Act, kan Norge være med å påvirke internasjonal standard for personvern og rettssikkerhetsgarantier, som er det hyppigst kritiserte i regelverkene. Det er gode sjanser for at USA og EU vil lage en samarbeidsavtale. Da vil mesteparten av den vestlige halvdelen av kloden, og hjemmet til en brorpart av tjenesteleverandørene, ha et felles system for bevisutlevering. Det er også sannsynlig at en slik blokk vil tiltrekke seg andre land, slik at avtalen kan bli enda mer omfattende og internasjonal. En slik løsning og utvikling synes å være veien videre både for den norske og internasjonale rettstilstanden.

Løsningen er ikke problemfri, og kommer trolig heller ikke til å bli det i nærmeste fremtid. Dette er en følge av at jussen henger etter den teknologiske utviklingen, og at vi er midt i et viktig teknologisk skifte hvor en må finne opp nye metoder for å håndtere problemstillingene som oppstår. For meg fremstår likevel de eksisterende løsningene som bedre enn alternativene uten regulering. Den beste måten å forbedre reguleringen på er å være en aktiv samarbeidspartner som kan bidra til positiv endring. Ettersom Norge, gjennom Tidal-saken, har gitt utrykk at vi behøver effektiv ekstraterritoriell bevisinnhenting, bør vi være et av landene som er på fronten av ny regulering for å sikre rettsikkerhet, rettsenhet og internasjonalt samarbeid.

Litteraturliste

Norske lover, utenlandske lover og konvensjoner

Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 1213 (2018)

Council of Europe Convention on Cybercrime (ETS No. 185), 23. November 2001 (entered into force 01. July 2004)

Europaparlamentets og Rådets direktiv nr. 2023/1544 av 12. juli 2023 om Laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, OJ L 191, 28.7.2023, s. 181–190

Europaparlamentets og Rådets forordning nr. 2023/1543 av 12. juli 2023 om European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L 191, 28.7.2023, s. 118–180

Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven/strpl.)

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) (Tilleggsprotokoll nr. 2)

Statute of the International Court of Justice. (24. september 1945). 59 Stat. 1031, TIAS 9939

Rettsavgjørelser

HR-2019-610-A

TOSLO-2018-182196

LB-2018-190770

LB-2020-32690

LB-2021-122818

Forarbeider og andre offentlige publikasjoner

Justis- og beredskapsdepartementet, Effektiv og tillitvekkende og rettssikker behandling av databevis, 2021. Hentet fra: https://www.regjeringen.no/contentassets/13417a44276c4b4086fdcbabb2108455/utredning-databevis-2021.pdf (Lest: 07.02.2024)

Justis- og politidepartementet, Rundskriv G-19/2001 om Internasjonalt rettslig samarbeid: Gjensidig hjelp i straffesaker og utlevering av lovbrytere (1. august 2001), Hentet fra: https://www.regjeringen.no/globalassets/upload/kilde/jd/rus/2001/0020/ddd/pdfv/139144-g192001.pdf (Lest: 25.03.2024)

Meld. St. nr. 34 (2020-2021) Sammen mot barne-, ungdoms- og gjengkriminalitet.

NOU 1997: 15 Om etterforskingsmetoder for bekjempelse av kriminalitet — Delinnstilling II

NOU 2003: 27 om lovtiltak mot datakriminalitet — Delutredning I om Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi

NOU 2016: 24 Om ny straffeprosesslov. Hentet fra: https://www.regjeringen.no/contentassets/6fe1d875248042b4a09b43b85aa46832/no/pdfs/nou201620160024000dddpdfs.pdf (Lest: 07.02.2024)

NUT 1969:3 Innstilling om rettergangsmåten i straffesaker fra Straffeprosesslovkomiteen (Komiteen til revisjon av straffeprosessloven). Avgitt i juni 1969.

Prop. 68 L (2015-2016) om Endringer i straffeprosessloven mv. (skjulte tvangsmidler)

Utenlandske og internasjonale forarbeider, etterarbeider og rettsavgjørelser

Council of Europe (2001) *Explanatory Report to the Convention on Cybercrime*. Council of Europe. Hentet fra: https://rm.coe.int/16800cce5b (Lest: 05.03.2024)

Council of Europe (2022) *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence.* Council of Europe. Hentet fra: https://rm.coe.int/1680a49c9d (Lest: 05.03.2024)

Council of Europe. (2024) *Chart of signatures and ratifications of Treaty 185.* Council of Europe. Hentet fra: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (Lest: 05.04.2024) (1)

Council of Europe. (2024) *Chart of signatures and ratifications of Treaty 224.* Council of Europe. Hentet fra: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224 (Lest: 05.04.2024) (2)

European Commission (2018) *Frequently Asked Questions: New EU rules to obtain electronic evidence.* Hentet fra: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345 (Lest: 05.03.2024)

European Data Protection Supervisor. (2019) *ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence.* Hentet fra: https://www.edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf (Lest: 05.04.2024)

Microsoft Corporation v United States of America, 829 F3d 197 (2d Circ 2016), rehearing en banc denied, No 14-2985, 2017 WL 362765 (2d Cir, 24 January 2017).

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

Trail Smelter (United States of America v. Canada) (1938/41) 3 RIAA, 1905. s. 1965

Transborder Group of the Cybercrime Convention Committee (T-CY) (2014) *Transborder access to data and jurisdiction: Options for further action by the T-CY*. Council of Europe. Hentet fra: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726e (Lest: 05.04.2024) (1)

Transborder Group of the Cybercrime Convention Committee (T-CY) (2014) T-*CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime.* Council of Europe. Hentet fra:

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c (Lest: 25.03.2024) (2)

Transborder Group of the Cybercrime Convention Committee Cloud Evidence Group (Cloud group) (2016) *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY*. Council of Europe. Hentet fra: https://rm.coe.int/16806a495e (Lest: 05.04.2024)

Fagbøker og artikler

Council of Europe. (2010, August 31). *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?* (Discussion paper). Economic Crime Division, Directorate General of Human Rights and Legal Affairs. Hentet fra: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df (Lest: 04.03.2024)

Currie, R. J. (2017). Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"? *Canadian Yearbook of International Law*, 54, 63–97. Hentet fra: https://doi.org/10.1017/cyl.2017.7 (Lest: 05.03.2024)

Eckhoff, T., og Helgesen, J. E. (2001). *Rettskildelære*, 5. utg., Oslo: Universitetsforlaget

Economic Crime Division. (2010) *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?*, Council of Europe. Hentet fra: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df (Lest: 06.03.2024)

Ekaas, I. *Dataavlesning som etterforskningsmetode: En rettslig analyse av straffeprosessloven § 216 o*, Universitetet i Bergen, 01. juni 2017, Hentet fra: https://bora.uib.no/bora-xmlui/bitstream/handle/1956/16227/Jus399_V17_208.pdf?sequence=1&isAllowed=y (Lest: 13.02.2024).

Evans, M. D. (2018) *International law*, 5 utg. Oxford University Press.

Gallagher, P. J. (2019) The CLOUD ACT: Mooting the Microsoft Ireland Case, but Not Forecasting Clear Skies Just Yet. *Columbia Law Review*. Hentet fra: https://journals.library.columbia.edu/index.php/CBLR/announcement/view/161 (Lest: 05.03.2024)

Nygård, V. S. (2021). Politiets adgang til ransaking og beslag i data på utenlandske servere. *Tidsskrift for strafferett*, *21*(2), 140–160. https://doi.org/10.18261/issn.0809-9537-2021-02-03 (Lest: 20.02.2024)

Osula, A-M. «Transborder Access and Territorial Sovereignty». *The Computer Law and Security Report* 31, no. 6 (2015): 719-35. Hentet fra: https://doi.org/10.1016/j.clsr.2015.08.003 (Lest: 04.02.2024)

Rui, J. P. (2019). Høyesterett i «skyen». *Lov og rett*, *58*(5), 261–262. https://doi.org/10.18261/issn.1504-3061-2019-05-01 (Lest: 19.02.2024)

Schmitt, M. N., & NATO Cooperative Cyber Defence Centre of Excellence. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*, 2. utg. Cambridge University Press.

Skjold, J. S. (2019). Suverenitet, jurisdiksjon og beslag i informasjon på server i utlandet: En kommentar til Høyesteretts kjennelse i Tidal-saken og Ruis kritikk. *Lov og rett*, *58*(10), 617–639. https://doi.org/10.18261/issn.1504-3061-2019-10-03 (Lest: 20.02.2024)

Tande, K. M. (2011). Individuelle valg og vurderinger i rettsanvendelsesprosessen. *Jussens venner*, *46*(1), 1–36. Hentet fra: https://doi.org/10.18261/ISSN1504-3126-2011-01-01 (Lest: 27.03.2024)

Propp, K. (2023) Navigating Toward an EU-U.S. Agreement on Electronic Evidence. Lawfare. Hentet fra: https://www.lawfaremedia.org/article/navigating-toward-an-eu-u.s.-agreement-on-electronic-evidence (05.03.2024)

Rapporter, nettsider og statistikk

Pulse Technology. «Cloud Storage: Where is my data actually stored?», 26. juni 2023 Hentet fra: https://www.pulsetechnology.com/blog/cloud-storage-where-is-my-data-actually-stored (Lest: 06.03.2024)

Statistisk sentralbyrå. (2024) *Bruk av nettskytjenester (prosent), etter tjenestetype, forvaltningsnivå, antall innbyggere, statistikkvariabler og år*. Hentet fra: https://www.ssb.no/statbank/table/12032/tableViewLayout1/ (05.03.2024)

United Nations Office on Drugs and Crime (UNDOC). (2013) *Comprehensive Study on Cybercrime.* Vienna. Hentet fra: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-CRP05/Comprehensive_study_on_cybercrime.pdf (Lest: 05.03.2024)

Økokrim. (2023) *Bedrageri - et samfunnsproblem*. Hentet fra: https://img8.custompublish.com/getfile.php/5180722.2528.qaamznluipnjsl/Bedrageri+-+et+samfunnsproblem.pdf?return=www.okokrim.no (Lest: 06.03.2024)

Leksikon

Bush, P. A. «Internetts historie» i Store Norske Leksikon, 17. oktober 2023. Hentet fra: https://snl.no/Internetts_historie (Lest: 06.03.2024)

Enli, G. «Sosiale medier» i Store Norske Leksikon, 06.02.2023. Hentet fra: https://snl.no/sosiale_medier (Lest: 13.02.2024)

Nätt T. H. «Data» i Store Norske Leksikon, 22.10.2022. Hentet fra: https://snl.no/data (Lest: 13.02.2024)

Nätt, T. H. «Hacking» i Store Norske Leksikon, 07.02.2024. Hentet fra: https://snl.no/hacking (Lest: 27.03.2024)

Nätt T. H. «Skylagring» i Store Norske Leksikon, 8. desember 2023. Hentet fra: https://snl.no/skylagring (Lest: 06.03.2024)

Øverby, H. «Internett» i Store Norske Leksikon, 1. oktober 2021. Hentet fra: https://snl.no/internett (Lest: 06.03.2024)