Internettkriminalitet og jurisdiksjon

– en sammenlikning mellom norsk straffelovs jurisdiksjon, andre lands straffelovers og internasjonale konvensjoners jurisdiksjon.

Kandidatnummer: 88

Antall ord: 14726

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

31.05.2018

«[D]en økende bruken av data som kommunikasjonsmiddel i samfunnet – og den økende kriminalitet i den forbindelse – medfører imidlertid at det vil være hensiktsmessig med lovregler som er spesielt utformet med tanke på datarelaterte overtredelser.»

- Førstvoterende dommer Karina M. Bruzelius, Rt. 2004 s. 1619

Innholdsfortegnelse:

1. Internettkriminalitet og jurisdiksjon

1.1 Tema, aktualitet og problemstilling

Bruken av datamaskiner, smarttelefoner og Internett har de siste 15-20 årene eksplodert, og disse teknologiske hjelpemidlene er i dag en stor og viktig del av våre liv. I 1995 var det estimert at antallet nettbrukere var ca. 30 millioner på verdensbasis.[1] Bruken av internett har eskalert med 170 % fra år 2000 til 2005[2], og det ble i 2015 estimert av International Telecommunication Union at 3.2 milliarder mennesker hadde tilgang til Internett.[3]

I takt med denne voldsomme utviklingen av teknologi har stater, internasjonale og nasjonale organisasjoner og institusjoner, offentlig virksomhet, næringsvirksomhet og enkeltindivider inkorporert datamaskiner og Internett som en naturlig del av deres driftsvirksomhet. Ved å gjøre bruken av datateknologi en naturlig del av virksomheten og dens dagligdag har de nevnte eksemplene i økende grad blitt mer og mer avhengig av en velfungerende og sikker bruk av Internett. Denne avhengigheten har gjort oss mer sårbare for å bli utsatt for forskjellige typer datakriminalitet.

Da Internett var en realitet i midten av 1990-tallet konkluderte flere akademikere med at cyberspace måtte bli behandlet som et distinktivt og uavhengig sted som skilte seg fra «den virkelige verden (…) og deres lover basert på geografiske grenser.»[4] To av akademikerne, Johnson og Post, foreslo i 1996[5] at for å unngå en lovløs tilstand på Internett burde Internett bli underlagt et felles, globalt lovverk som skulle gjelde for alle nasjoner. Johnson og Post hevdet at et slikt felles rammeverk ville minimere problemer og spørsmål knyttet til Internett og jurisdiksjon, og at enighet rundt avgjøring av jurisdiksjon ville gjøre regulering av Internett og Internettrelatert kriminalitet mye enklere.

Internett reiser særlige problemstillinger rundt jurisdiksjon og håndheving av jurisdiksjon da Internett og kriminelle handlinger begått over Internett gjerne ikke følger landegrenser. Lovgivning når det gjelder Internettkriminalitet og datakriminalitet har blitt utformet i de enkelte land i stedet for å bli underlagt en global lovgivning, og i noen tilfeller der hvor

[1] https://no.wikipedia.org/wiki/Internett
[2] Mørketallsundersøkelsen 2006
[3] https://en.wikipedia.org/wiki/Global_Internet_usage
[4] Johnson and Post: *Law and borders – The rise of Law in Cyberspace*. Stanford Law Review (1996) s.1378-1386
[5] Johnson and Post: *Law and borders – The rise of Law in Cyberspace*. Stanford Law Review (1996) s.1376

handlingen faller utenfor et lands jurisdiksjon har dette ført til at klart straffverdige handlinger ikke kan straffes fordi det er utenfor landets jurisdiksjon.

Bestemmelsene i Straffeloven 2005 §§4, 5, 6 og 7 regulerer straffelovens stedlige virkeområde, og slår fast hvilke handlinger som kan straffes i Norge. Straffelovens kapittel 1 er indirekte avgjørende for norske domstolers kompetanse i straffesaker med tilknytning til utlandet.[6] Rammes en hendelse av et straffebud i norsk strafferett eller i særlovgivningen er dette kun et utgangspunkt. Det fremgår av straffelovens kapittel 1 at det etter nærmere bestemte vilkår i dette kapitlet at det er fullt mulig at norsk straffelovgivning kan anvendes på handlinger begått utenfor landets grenser så langt norsk straffemyndighet ikke utøves utover sine grenser.

Det at Internett, herunder kriminelle handlinger begått over Internett, ikke følger fysiske grenser mellom land reiser først og fremst spørsmål om strafferettslig jurisdiksjon. Kan norsk straffelov for eksempel anvendes i tilfeller der hvor utøveren av den kriminelle handlingen befinner seg i utlandet, eller i tilfeller der hvor skaden av den kriminelle handlingen inntreffer i utlandet?

Tema for denne avhandling er å se på hvordan jurisdiksjonsbestemmelsene i norsk strafferett kommer til anvendelse i saker ved datakriminalitet der hvor handlingen har blitt begått over eller ved hjelp av Internett. En vesentlig del av oppgaven vil ta for seg en sammenlikning mellom internasjonale konvensjoner og andre nasjoners jurisdiksjonsbestemmelser for å vise til hvordan disse løser spørsmålene rundt Internettkriminalitet og jurisdiksjon.

1.2 Metodisk tilnærming og struktur

Denne delen av innledningen til avhandlingen skal kort ta for seg hvordan strukturen for avhandlingen ser ut videre, og hvilken juridisk metode som skal brukes for å besvare problemstillingen.

Denne avhandlingen skal forsøke å komme frem til hva som er gjeldende rett når det kommer til Internettkriminalitet og jurisdiksjon. Avhandlingen tar sikte på å bruke norske rettsregler, men siden Internettkriminalitet også er et utpreget internasjonalt spørsmål, vil de norske rettsreglene i Straffelovens kapittel 1 måtte anvendes sammen med andre relevante rettskilder

[6] Norsk Lovkommentar note (48)

for å se hvordan jurisdiksjonsspørsmålet kan løses. Videre vil det ses til andre land og internasjonale avtaler for å se hvordan disse har taklet jurisdiksjonsspørsmålet ved tilfeller av Internettkriminalitet.

De norske jurisdiksjonsbestemmelsene er mer generelt utformet og sier ikke direkte noe om hvordan de skal anvendes i mer spesifikke tilfeller, som for eksempel ved Internettkriminalitet. Jurisdiksjonsbestemmelsene i Straffelovens kapittel 1 må anvendes sammen med andre relevante rettskilder, da hovedsakelig forarbeid til Straffeloven 2005 og rettspraksis på rettsområdet.

Etter norsk rettskildeoppfatning[7] har Høyesterettspraksis mer rettskildemessig vekt enn rettspraksis fra underrettsdomstoler. På rettsområdet Internettkriminalitet foreligger det få dommer her i Norge, og det vil i avhandlingen vises til en dom fra Salten Herredsrett for å illustrere hva en norsk tingrett har lagt til grunn for et visst aspekt av Internettkriminalitet. Denne dommen har ikke særlig stor rettskildemessig vekt da den kun er en tingrettsdom, men kan allikevel ha noen nyttige vurderingsmomenter som er verdt å ta opp. Den aktuelle tingrettsdommen viser hvordan norske domstoler tolker de generelle jurisdiksjonsbestemmelsene ved å støtte seg til Straffelovens forarbeider når det gjelder tilfeller av Internettkriminalitet.

Straffelovens stedlige virkeområde har en side mot domstolenes kompetanse, og en side mot legalitetsprinsippet.[8] [9] Selv om legalitetsprinsippet ikke har sitt kjerneområde i Straffelovens jurisdiksjonsbestemmelser vil prinsippet kunne ha virkning på selve utøvelsen og håndhevingen av jurisdiksjon. Dette vil drøftes mer utdypende.

Norge har ratifisert Datakrimkonvensjonen, en internasjonal konvensjon underskrevet av flere andre land. Tolkning av konvensjonen vil skje i tråd med Wien-konvensjonen om traktatretten av 23.mai 1969 artikkel 31, som legger til grunn at en traktat må fortolkes i god tro i tråd med den ordinære betydning, som bør tillegges traktatens ordlyd sett i sin sammenheng og i lys av traktatens gjenstand og formål. Norge har ikke underskrevet eller ratifisert de folkerettslige instrumentene i Wien-konvensjonen, men anses allikevel som bundet av de fleste bestemmelsene da det meste av konvensjonen anses som folkerettslig sedvanerett i Norge.[10]

[7] https://jusleksikon.no/wiki/Rettskildel%C3%A6re
[8] Rt. 2010 s. 1271, avsnitt 9

[9] Jo Stigen, «Lokalisering av straffbare handlinger», side 144

[10] Ruud, Morten (1998). *Innføring i folkerett*. [Oslo]: Tano Aschehoug. s. 23–24.

Hoveddelen for avhandlingen er strukturert slik at norsk rett skal behandles for seg selv under punkt 2 og tilhørende underpunkter, da hovedfokuset for oppgaven skal være å finne frem til hva som er gjeldende rett for norsk straffelov når det kommer til datakriminalitet og jurisdiksjon. Deretter vil folkerettslige avtaler (Datakrimkonvensjonen) tas opp under punkt 3.1, da Norge har ratifisert Datakrimkonvensjonen.

Videre vil avhandlingen gå inn på andre lands bestemmelse om deres respektive retts virkeområde, dette for å se hvordan disse valgte landene har forsøkt å løse jurisdiksjonsspørsmålet ved tilfeller ved datakriminalitet. Landene som vil bli behandlet i separate punkter i punkt 3 er USA, Tyskland og Storbritannia. Gjennom punkt 3 vil det foretas en løpende sammenlikning av hvert land sett opp mot hvordan Norge har løst disse problemstillingene rundt jurisdiksjon. I punkt 4 med tilhørende underpunkter vil jurisdiksjonstilnærmingene tilhørende norsk, britisk, tysk og amerikansk straffelov oppsummeres. Avslutningsvis vil veien videre for Internettkriminalitet og jurisdiksjon tas opp.

1.3 Begrepsavklaring

Jurisdiksjon betyr kort forklart rettshåndhevelse, og handler om staters og lokale myndigheters kompetanse eller grunnlag for å utøve tvang på sine statsborgere og i sitt territorium.[11] Jurisdiksjon kan også i videste forstand omhandle kompetanse eller utøvelsesmakt over en stat i forhold til andre staters rett til å regulere.

Internett er «et verdensomspennende nettverk av datamaskiner som kommuniserer med hverandre i henhold til en standard kommunikasjonsprotokoll (TCP/IP).»[12] Denne kommunikasjonsprotokollen gjør det mulig for datamaskiner å kommunisere på tvers av forskjellige fysiske nett som fiber, kabel, radiolink satellitt og trådløst nett.[13] Fra et teknisk synspunkt er Internett et samkjøringsnett av datamaskiner kalt vertsmaskiner, som utveksler informasjon på digital form via et overføringsnett. Overføringsnettet består av ulike slag overføringskanaler knyttet sammen via spesialiserte datamaskiner kalt rutere. Vertsmaskiner

[11] https://jusleksikon.no/wiki/Jurisdiksjon

[12] https://no.wikipedia.org/wiki/Internett
[13] https://no.wikipedia.org/wiki/Internett

med ulike formål kan utveksle informasjon av alle typer som kan kodes digitalt. Vertsmaskinene kan lagre, bearbeide og presentere informasjon.

Datakriminalitet kan omfatte all form for kriminalitet der hvor data eller nettverk benyttes som mål, middel eller arena for å skaffe seg uberettiget tilgang, uberettiget vinning (økonomisk og ikke-økonomisk), eller å utføre skade.[14] Straffelovrådet behandlet i NOU 1985: 31[15] datakriminalitet, der hvor utnyttelse av datateknologi har vært vesentlig for overtredelsen. Straffelovrådet viste til at dette også omfattet tilfeller der hvor tradisjonelle forbrytelser ble begått ved hjelp av datateknologi. Straffelovrådet, i likhet med den internasjonale tolkningen av datakriminalitet, delte begrepet datakriminalitet inn i to hovedgrupper som fortsatt brukes i dag. Den første hovedgruppen er forbrytelser der hvor datamaskinen ble brukt som hjelpemiddel ved den straffbare handlingen. Den andre hovedgruppen er forbrytelser der hvor datamaskinen eller datasystemet var objekt for handlingen – eksempelvis angrep mot servere eller bestemte nettsider.[16]

Internettkriminalitet er en underkategori av datakriminalitet der hvor den straffbare handlingen skjer på Internett, eller lovbryteren benytter Internett som et verktøy for å begå den straffbare handlingen. Internettkriminalitet er for eksempel ulovlig opplastning eller nedlastning av opphavsbeskyttet materiale, nedlastning eller opplastning av ulovlig materiale som overgrepsmateriale og barnepornografi, hacking, forskjellige typer svindel, dataskadeverk etc.

Skylagring er en form for datalagring der digitale data lagres i sammenslutninger hvor det ofte blir lagret på flere servere og på flere steder. Skylagringsleverandørene er ansvarlig for å holde dataene tilgjengelig til alle tider, mens deres fysiske serverplassering skal beskytte det en har lagret fra å havne i uvedkommende sine hender. Personer og organisasjoner kan kjøpe eller lease lagringskapasitet, mot avgift, fra leverandørene for å lagre butikk, organisasjons og applikasjonsdata eller informasjon.[17] Eksempel på tilbydere av skylagring er blant annet Dropbox, Google Mail og Microsoft One Drive.

1.4 Avgrensing

[14] John D. Howard; An Analysis of Security Incidents on the Internet 1989-1995, kapittel 6.4
[15] NOU 1985: 31 Datakriminalitet side 6
[16] Stein Schjølberg: Lov og Rett 1983 side 468
[17] https://no.wikipedia.org/wiki/Skylagring

Som nevnt under punkt 1.3 er Internettkriminalitet en form for datakriminalitet, som har blitt mer vanlig de siste årene fordi tilgangen til oppkobling til Internett har blitt mye enklere gjennom smarttelefoner og trådløse nettverk, nesten alt av datamaskiner er koblet til Internett nå i dag. Det vil i denne avhandlingen fokuseres på Internettkriminalitet og spørsmålene rundt jurisdiksjon ved tilfeller av Internettkriminalitet.

2. Internettkriminalitet og jurisdiksjon - Norge

2.1 Hovedregel jurisdiksjon – Straffeloven §4 og §5

Hvor en kriminell handling er foretatt er avgjørende for om den faller innenfor eller utenfor norsk territorium, og dermed vår territorielle jurisdiksjon.[18] Hvilket fremmed land handlingen er begått kan også ha betydning.[19]

Det fremgår av Straffeloven §4 første ledd at «straffelovgivningen» gjelder for handlinger foretatt i «Norge.» Med «Norge» kommer det klart frem av Straffeloven §4 at det menes norsk territorium, som inkluderer Svalbard, Jan Mayen og de norske bilandene.[20] Videre regner Straffeloven §4 annet ledd bokstav a-c opp visse innretninger, områder og fartøy som norsk straffelovgivning er gjeldende for. Internett er ikke nevnt i bestemmelsen og for løsningen av spørsmålet om datakriminalitet omfattes av straffelovgivningen må man gå rett til en vurdering av tilknytningspunktene til Norge. Tilknytningspunktene er oppregnet i Straffeloven §4 annet ledd bokstav a-c. §4 gir uttrykk for territorialprinsippet i folkeretten, der utgangspunktet er at hver stat har fullt rådvelde på eget territorium både med tanke på lovgivning og håndhevelse, og bruken av denne kompetansen er i utgangspunktet et indre anliggende som andre stater plikter til å respektere. Unntak fra prinsippet følger blant annet av alle staters plikt til å respektere internasjonale menneskerettigheter. Dersom en stat skal utøve tvangsmyndighet på en annen stats territorium krever det særskilt hjemmel for å ikke komme i strid med folkeretten.[21]

[18] Straffeloven 2005 §4
[19] Straffeloven 2005 §5
[20] Straffeloven 2005 §4
[21] https://snl.no/territorialprinsippet_-_folkerett

«Straffelovgivning» i Straffeloven §4 omfatter straffelovens bestemmelser og straffesanksjonerte normer i spesiallovgivningen. For spesiallovgivningen er åndsverkslovens bestemmelser praktiske for Internettkriminalitet.[22]

En handling som oppfyller vilkårene for straff etter et norsk straffebud men som er begått og har sin virkning utenfor Norge, omfattes som hovedregel ikke av norsk straffelovgivning. Hvis for eksempel et datainnbrudd begått via Internett av en person i New York, mot en server i Los Angeles, faller det utenfor hovedregelen i §4, jf. §7. Hvis det er ønskelig å straffe handlingen etter norsk rett må annet rettsgrunnlag påvises, og slike rettsgrunnlag finnes i Straffeloven §§5 og 6.

Norsk straffelov har lovfestet to folkerettslige prinsipper om jurisdiksjon i Straffeloven §5, nemlig det aktive personalprinsipp og beskyttelsesprinsippet. Det aktive personalprinsippet fremgår av Straffeloven §5 første ledd bokstav a-c som sier at norsk straffelovgivning gjelder for handlinger foretatt av en «norsk statsborger», av en «person med bosted i Norge» eller handling foretatt «på vegne av et foretak registrert i Norge.»

For at straffeloven skal kunne anvendes for handlinger begått av nordmenn i utlandet, må kravet om dobbel straffbarhet i Straffeloven §5 første ledd nr.1 være oppfylt. Etter §5 første ledd nr. 1 gjelder norsk straffelovgivning for handlinger som er straffbare «også etter loven i landet der de er foretatt.» Vilkåret om dobbel straffbarhet kan være oppfylt for handlinger relatert til Internettkriminalitet da mange land har tilpasset straffelovgivningen i lys av utfordringene som har fulgt med Internett og den tekniske utviklingen. Internasjonale konvensjoner som Europarådets datakrimkonvensjon (ETS 185), konvensjonen mot seksuell utnyttelse av barn mv. (ETS 201) og EUs regelproduksjon har bidratt til at mange land har valgt å harmonisere innholdet i sin nasjonale straffelovgivning på dette området.[23] Det må påpekes at dobbel straffbarhet kun kan gjøres gjeldende overfor norske borgere, personer med bosted i Norge, eller overfor en person som utførte handlingen på vegne av et foretak registrert i Norge, jf. Straffeloven §5 bokstav a-c.

Straffeloven §5 tredje ledd regulerer norsk straffelovgivnings anvendelse på handlinger som er begått i utlandet av personer som ikke er norske borgere eller bosatt i Norge eller annet nordisk land. Tredje ledd stiller opp tre kumulative vilkår som må være oppfylt for at norsk straffelovgivning skal kunne anvendes i slike tilfeller. Det første kravet er at lovbryteren

[22] Åndsverkloven 12.mai 1961 nr. 2
[23] Direktiv 2013/40/EU, om angrep mot elektroniske informasjonssystemer

oppholder seg i Norge når straffeforfølgningen innledes her. Det andre kravet er at handlingen det innledes straffeforfølgning for må ha en strafferamme på fengsel i mer enn 1 år. Det tredje kravet er at et av de alternativene som er nevnt i første ledd nr. 1, 2, 4 eller 6 foreligger. Hovedregelen er her også et krav om dobbel straffbarhet, jf. §5 første ledd nr.1, men det er ikke noe krav om at handlingen i handlingslandet må ha en strafferamme på mer enn 1 års fengsel.[24]

Bakgrunnen for det videre omfanget som den nye §5 har fått er at det i de siste årene har blitt et stadig tettere internasjonalt samarbeid mellom andre nasjoner når det gjelder å stoppe Internettkriminalitet. Det tettere internasjonale samarbeidet har gjort det slik at det kan være aktuelt for norske myndigheter å begjære en person utlevert fra et annet land, men dette forutsetter at forholdet eller handlingen er straffbart etter norsk straffelovgivning. Den nye, nå gjeldende §5, bidrar til å sikre norsk jurisdiksjon i slike tilfeller.[25]

I enkelte tilfeller finnes det grunnlag for utvidet jurisdiksjon, jf. Straffeloven §5 første ledd nr. 9-11 og §6. For §§ 136, 183, 185 og 311 finnes flere grunnlag for utvidet jurisdiksjon. Disse utvidede grunnlagene kommer til anvendelse også når man mangler kunnskap om hvor gjerningspersonen var på det avgjørende tidspunktet.[26]

Et av kanskje de mest aktuelle straffebudene nå for tiden, midt oppe i Dark Room-saken, er Straffeloven §311. Straffeloven §311 kriminaliserer fremstillingen av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn, og kan straffes med bot eller fengsel i inntil 3 år dersom et av vilkårene i første ledd bokstav a-e er oppfylt. Bakgrunnen for en utvidet tilnærming til jurisdiksjon for §311 er for å understreke alvoret i seksuelle overgrep mot barn og styrke barns beskyttelse mot overgrep.[27] Jeg kommer tilbake til §311 og den utvidede jurisdiksjonen senere i avhandlingen, under punkt 2.4 og 3.1.

2.2 Lovbryteren er i Norge på gjerningstidspunktet – virkning inntrer i utlandet

En straffbar handling begått av en person som enten er norsk statsborger eller oppholder seg i Norge anses som foretatt i Norge og kan derfor straffes etter norsk straffelovgivning, jf. Straffeloven §4 og §5 første ledd a-c. Når virkningen av handlingen også inntrer i Norge

[24] Ot.prp. nr.90 (2003-2004) punkt 30.1
[25] Ot.prp. nr. 22 punkt 16.1
[26] Inger Marie Sunde, *Datakriminalitet: En fremstilling av strafferettslige regler om datakriminalitet*, side 51

[27] Ot.prp. nr. 22 s.14

anses dette som så selvsagt at det normalt ikke presiseres.[28] Spørsmålet om handlingen er «foretatt i Norge» er mer aktuelt når gjerningspersonen på gjerningstidspunktet er i Norge, mens virkningen inntrer i utlandet. Denne situasjonen reguleres ikke av §7, da §7 bare tillegger virkningen betydning som tilknytningspunkt til Norge når gjerningspersonen er i utlandet. I et slikt tilfelle må man gå direkte på en tolkning av §4 og §5.

Selv om det i utgangspunktet bør være enkelt å slå fast hvorvidt en handling har skjedd i Norge eller ikke, har rettspraksis vist til at dette ikke alltid så enkelt når det gjelder Internettkriminalitet.

Høyesterett gjorde i Rt. 2004 s. 1619 («Bakdørskjennelsen») en tolkning av daværende Straffeloven §12 (nå §4) ved tilfelle av datakriminalitet der hvor virkningen inntraff i utlandet. Spørsmålet som ble reist i saken var om straffbare handlinger utført fra Norge via Internett med virkning i utlandet var begått utenfor Norge.

«Bakdørskjennelsen» gjaldt to personer som uberettiget hadde skaffet seg tilgang til henholdsvis 235 og 202 datamaskiner som befant seg i utlandet, bortsett fra en. De ble begge domfelt for overtredelse av Straffeloven §145, 2. ledd i tingretten og i lagmannsretten fordi den straffbare handlingen kunne anses forøvet i riket, jf. Straffeloven §12, nr. 1. Forsvarerne hevdet at det straffbare etter §145 annet ledd er «å bryte en beskyttelse», og at dette først skjer der hvor datamaskinen man trenger seg inn i er lokalisert, derfor måtte den straffbare handlingen anses som foretatt i utlandet der datamaskinene var lokalisert.

Høyesterett slo fast at «… de datamaskinene de tiltalte brukte og de fysiske handlingene, kommandoene, som iverksatte søk mot og inntrengning i de andre datamaskinene, var i riket. Uten den handlingen og utstyret i riket, faller resten av handlingsrekken bort.»[29] Høyesterett uttalte at «det utslagsgivende må være at alle nødvendige handlinger for å bryte beskyttelsen fant sted i Norge.» Videre ble det uttalt at «... uten den handlingen og utstyret i riket, faller også resten av handlingsrekken bort.»

«Bakdørskjennelsen» legger frem et krav om dersom handlingen skal anses for å være foretatt i Norge må handlingen være nødvendig. Med dette vises det til at handlingsrekken faller bort i den aktuelle saken dersom utstyret og kommandoer tas bort. Alle handlinger som er grunnleggende for at forbrytelsen blir begått vil måtte anses å være tilstrekkelig. De enkelte handlingene fra landet må kunne anses å være avgjørende for forbrytelsen for at handlingen

[28] Inger Marie Sunde, *Datakriminalitet: En fremstilling av strafferettslige regler om datakriminalitet*, side 50
[29] Rt. 2004 s. 1619, avsnitt 17

skal anses som begått i landet. På bakgrunn av forståelsen i «Bakdørskjennelsen» er det altså tilstrekkelig at gjerningspersonen er i Norge da virkningen av handlingen inntreffer.

Av «Bakdørskjennelsen» kan det utledes en rettsregel om at stedet der alle de fysiske handlingene er utført vil avgjøre hvorvidt norsk Straffelov kan anvendes eller ikke. Dette reiser da et nytt spørsmål: Hva så med handlinger som anses for å bare delvis være begått i Norge?

Problemstillingen har kun blitt drøftet i en tingrettsdomsavsigelse, RG 2001 s.219. Tingretten gikk bort fra å drøfte hvorvidt handlingen i sin helhet ble begått i Norge eller om den ble begått delvis i Norge og i utlandet. Det blir i dommen konkludert med at handlingen har skjedd i Norge fordi handlingen hadde «tilsiktet virkning» her, jf Straffeloven 1902 §12,2 (nå Straffeloven §7).

RG 2001 s.219 har ikke like stor rettskildemessig vekt som «Bakdørskjennelsen», men er likevel et uttrykk for at ved vurderingen av hvor handlingen har skjedd, må det enten stilles krav til handlingen – altså hvor stor del av handlingen som har utspilt seg i Norge, eller det åpnes for at handlingen kan anses som begått delvis i Norge og delvis i utlandet.

2.3 Lovbryteren er i utlandet på gjerningstidspunktet – virkningen inntrer i Norge

Både Straffeloven §5 og §7 åpner opp for at en lovbryter som oppholder seg i utlandet kan i visse tilfeller straffeforfølges for handlinger som har virkning i Norge.

Som nevnt tidligere vises det i §5 første ledd til at det i visse tilfeller kan utøves utvidet jurisdiksjon enn det som fremgår av §§4, 6 og 7. I §5 femte ledd presenteres det som i folkeretten kalles offerprinsippet: jurisdiksjon kan avgjøres på bakgrunn av offerets nasjonalitet. På bakgrunn av §5 kan norske myndigheter utøve en utvidet jurisdiksjon og anvende norsk Straffelov overfor en utenlandsk lovbryter som oppholder seg i utlandet dersom handlingen «har en lengstestraff på fengsel i 6 år eller mer» og er «rettet mot noen som er norsk statsborger eller er bosatt i Norge.»

§5 femte ledd gir uttrykk for at det bør utvises en viss tilbakeholdenhet med å straffeforfølge handlinger begått i utlandet her i Norge, og at kravet til dobbel straffbarhet som nevnt i §5 første ledd nr. 1 fortsatt må gjelde. Unntaket i §5 femte ledd åpner opp for en bred skjønnsmessig vurdering om hvilke handlinger som kan anses som å være rettet mot norske statsborgere eller personer bosatte i Norge. Ved den skjønnsmessige vurderingen vil det være av betydning hvor alvorlig handlingen er, hvilken tilknytning lovbryteren har til Norge og i

hvilken grad handlingen berører norske interesser, særlig om den fornærmede eller den som er rammet av handlingen er norsk. Dette gjelder ikke for tilfeller av folkemord og forbrytelser mot menneskeheten.[30]

§5 femte ledd gjør seg særlig gjeldende i tilfeller av barnepornografisk materiale, som er kriminalisert i blant annet Straffeloven §311 og i Datakrimkonvensjonen artikkel 9. Fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn anses som en veldig alvorlig handling, og vil i de aller fleste relevante tilfeller falle inn under den utvidede jurisdiksjonen i §5 femte ledd. Bakgrunnen for en utvidet jurisdiksjon for §311 er for å understreke alvoret i seksuelle overgrep mot barn og styrke barns beskyttelse mot overgrep.[31]

Straffeloven §7 åpner opp for at handlinger foretatt i utlandet kan anses for å ha gjerningssted også i Norge. Det fremgår av Straffeloven §7 at når straffbarheten av en handling «avhenger eller påvirkes» av en «inntrådt» eller «tilsiktet» virkning, anses handlingen foretatt også der virkningen er «inntrådt» eller «tilsiktet fremkalt.»

Straffeloven §7 stiller opp to hovedvilkår som må være oppfylt for at norske myndigheter kan utøve straffejurisdiksjon ovenfor gjerningsperson i utlandet som har begått en handling som har virkning i Norge. Det ene vilkåret er at handlingen har virkninger som er avgjørende for eller påvirker straffbarheten. Det andre hovedvilkåret er at virkningen enten har inntrådt på territoriet, eller at det var innenfor lovbryterens forsett at virkningen skulle inntre på norsk territorium (tilsiktet).

Det første vilkåret i §7 krever at straffbarheten må være avhengig av eller påvirkes av virkningen – handlingen må være nødvendig, jf. Rt. 2004 s.1619. I nødvendighetskravet ligger det at handlingen(e) fra landet må kunne anses å være avgjørende for forbrytelsen for at handlingen skal anses som begått i landet.

Andre vilkår sier det i seg selv – virkningen av handlingen, altså effekten eller skaden av handlingen må enten ha inntrådt på territoriet, eller at det var lovbryterens mening at virkningen skulle inntre på norsk territorium eller ramme det norske rettsgodet.

Kravet om tilsiktet virkning i §7 reiser et interessant spørsmål i tilfeller der nettverksrelaterte handlinger rammer tilfeldig. I tilfeller ved generelle dataangrep må man ta stilling til om det

[30] Ot.prp. nr. 90 (2003-2004) punkt 30.1
[31] Ot.prp. nr. 22 s.14

tilfeldige dataangrepet mot et sårbart system er «tilsiktet» å inntre i Norge, jf. §7. Spørsmålet blir derfor om tilfeldige handlinger kan omfattes av «tilsiktet» i §7.

Formålet med §7 er å sikre muligheten til å kunne straffeforfølge når det krenkede rettsgodet er i Norge. Hensynet gjør seg gjeldende også for tilfeldige krenkelser, og det er i teorien lagt til grunn at «likestilt med tilsiktet er at virkningen faktisk har inntrådt.»[32] Dette betyr med andre ord at det ikke gjelder noe krav om «stedsforsett» når et norsk datasystem faktisk ble rammet, og løsningen på spørsmålet ved tilfeldige angrep bør være den samme som ved straffbart forsøk. Dette betyr at virkningen er «tilsiktet» fremkalt i Norge, jf. §7 når datasystemet som utsettes for et straffbart forsøk er i Norge, selv om lovbryteren ikke hadde noen tanke for datamaskinens lokalisering.

Elektronisk skadeverk som rammer et datasystem på norsk territorium omfattes uten tvil av Straffeloven, jf. §7, jf. §4. Dette fordi den strafferettslig relevante skaden inntrådte i Norge. Dersom skadeverket mislykkes er det tale om forsøk, og dermed at virkningen er tilsiktet fremkalt i Norge, jf. §7.

Et illustrerende eksempel på at en handling er «tilsiktet» inntrådt i Norge er Rt. 2003 s. 1770, som omhandlet grovt bedrageri utført fra Sverige, Finland og Bahamas. Det fremgår av Rt. 2003 s. 1770 at «markedsføringen av virksomheten tok sikte på markedet i Norge. Heller ikke er det tvilsomt at virkningen faktisk også inntrådte i Norge for de aller fleste.»[33] Denne uttalelsen fra Høyesterett må forstås som at virkningen ansås både som inntrådt og tiltenkt inntrådt i Norge i denne saken – det falt klart innenfor lovbryterens forsett at de som skulle bedras primært befant seg i Norge. Det at et betydelig tap oppstod i Norge måtte også kunne vektlegges i denne saken, og at dette var tilstrekkelig til å anse at bedragerihandlingen også hadde handlingssted i Norge. Dommen stiller videre opp rettsregelen om at det må stilles krav til en form for tilknytning gjennom virkning eller målrettet aktivitet mot Norge for at det skal kunne hevdes jurisdiksjon over Internett, noe som støttes opp i NOU 2007:2, der målrettet aktivitet beskrives ved at «nettsider er spesielt tilrettelagt for bruk i Norge og hvor de negative konsekvensene i hovedsak eller utelukkende manifesterer seg her.»[34]

[32] Ot.prp. nr. 22 (2008-2009) punkt 2.7.4
[33] Rt. 2003 s. 1770, avsnitt 32
[34] NOU 2007: 2, side 143-144

Et annet spørsmål som reiser ved handlinger som anses som Internettkriminalitet er om forberedende handlinger er tilstrekkelig grunnlag for å anse handlingen som «tilsiktet» å inntre i Norge.

Ved hacking, som er en form for Internettkriminalitet, kan det hende at lovbryteren må gå til anskaffelse av hjelpemidler for å gjennomføre handlingen. Denne anskaffelsen anses som en forberedende handling til å begå lovbruddet. Som regel vil ikke forberedende handlinger i seg selv regnes for å ha relevant virkning i Norge. Straffebud som slår ned på forberedende handlinger som selvstendig straffbar handling regnes ikke for å ha en relevant virkning i Norge selv om gjennomføringen som straffebudet er ment å motvirke, skal skje i Norge.[35] Forberedende handlinger var et av temaene Høyesterett tok opp i Rt. 2010 s. 1217. Høyesterett anså i saken anskaffelse og tilvirkning av skimmingutstyr i utlandet som fullbyrdet overtredelse av strl. 1902 §186 (nå §370). Grunnen til at Høyesterett kom frem til denne avgjørelsen var fordi skimmingen var planlagt å bli utført i Norge.[36] I forberedende handlinger må det altså kunne bevises utstyret som er anskaffet skal brukes til å begå en kriminell handling i Norge eller mot et norsk rettsgode.

Et illustrerende tilfelle på at det straffbare forholdet ansås for fullbyrdet i utlandet er Rt. 2003 s. 179, som gjaldt organisert menneskesmugling. Det var oppgitt uriktige opplysninger til [37]norsk utenriksstasjon for å få visum til Norge, og dette var falsk forklaring, jf. Straffeloven 1902 §166 (nå Straffeloven 2005 §221). Handlingens straffbarhet var inntrådt ved avgivelsen av opplysningene i utlandet, men selv om formålet var å oppnå innreise til Norge var ikke straffbarheten avhengig av eller påvirket av dette, jf. Straffeloven 2005 §7. Forholdet ble ansett som fullbyrdet i utlandet og falt derfor utenom virkeområdet for den norske straffeloven.

2.4 Vedvarende forbrytelser

Internettkriminalitet vil ofte være en eller annen form for vedvarende forbrytelser, gjennom for eksempel besittelse av ulovlig materiale. Straffbar besittelse er en kategori av vedvarende forbrytelser, der hvor overtredelsen løper fra besittelsen inntrer til den opphører. Eksempel på besittelsesforbud som omfatter digitalt materiale er Straffeloven §201 som omhandler

[35] Inger Marie Sunde, *Datakriminalitet: En fremstilling av strafferettslige regler om datakriminalitet*, side 55
[36] Kopiering av magnetstripen etter Straffeloven 1902 ansett som uberettiget adgang til data, jf. §145 annet ledd. Kopieringen rammes nå av Straffeloven 2005 §204.
[37] Matningsdal 2016. Punkt 4. note 1 til §7

tilgangsdata/hackerprogrammer og Straffeloven §311 som omhandler overgrepsbilder av barn.

Det reiser seg flere spørsmål rundt besittelse av forbudt materiale, det første om besittelsen kan rammes av norsk lov når det forbudte materialet oppbevares på en brukerkonto på Internett i en såkalt skytjeneste. Forutsatt at lovbryteren har tilgang til Internett, er materialet under han eller hennes kontroll uavhengig av hvor han eller hun oppholder seg. Materialet kan derfor i utgangspunktet besittes fra Norge. Spørsmålet ved denne tolkningen er om besittelsen anses for å ha virkning i Norge, jf. §7, eller om det er lovbryterens geografiske oppholdssted som er avgjørende. Er det tilstrekkelig å anse handlingen som foretatt i Norge, at lovbryteren har oppholdt seg i Norge i løpet av besittelsesperioden, eller kreves det noe mer – for eksempel at lovbryteren var i Norge da besittelsen oppstod eller at materialet ble benyttet mens lovbryteren var i Norge?

Bruken av utenlandsk skylagring har blitt tatt opp i RG 2001 s. 218 (Salten herredsrett) der det ble slått fast at det ikke er holdepunkter for at bruk av utenlandsk skytjeneste skulle være tilstrekkelig for å bringe forholdet utenfor rekkevidden av norsk straffelovgivning, fordi det ville åpne for enkel omgåelse av loven. På bakgrunn av omgåelseshensynet vist til i rettspraksis og juridisk teori[38] er ikke skytjenestens nasjonalitet relevant. Problemstillingen oppstår utelukkende på grunnlag av den globale tilgangsmuligheten. Besittelse av overgrepsbilder av barn, jf. Straffeloven §311, omfattes av Straffeloven §5 første ledd nr. 9 og medfører at besittelsen av denne typen materiale er straffbar for nordmenn som oppholder seg i utlandet og for utlendinger som kommer til Norge mens besittelsen varer.

Ved forbrytelser (brudd på straffeparagrafer som nevnt i Straffeloven §5 første ledd nr.9-11) kan norske myndigheter straffeforfølge lovbryteren såfremt han/hun var i Norge da publiseringen/tilgjengeliggjøringen eller nedlastningen ble foretatt. Det stilles ikke et krav om at den utsatte gruppen eller rettsgodet som handlingen gjelder, er i Norge. Eksempel på dette er faktum i Dark Room-saken som har vært omtalt i norsk media, der hvor 51 menn ble tatt med overgrepsmateriale av både norske og utenlandske barn. Hvor ofrene oppholdt seg var ikke av betydning i saken, det viktigste var hvor materialet var lastet opp og ned.

Besittelse anses som en tilstand, og gjerningspersonen er i denne tilstanden uansett hvor han befinner seg. Dette fordi gjerningspersonen disponerer tilgangsdataene til det virtuelle oppbevaringsstedet. Uten tilgangsdataene mister gjerningspersonen kontrollmuligheten, og

[38] Inger Marie Sunde, *Datakriminalitet: En fremstilling av strafferettslige regler om datakriminalitet*, side 57

derfor også besittelsen. Juridisk teori[39] påpeker at gjerningspersonens fysiske lokalisering bør være avgjørende da besittelsen ikke kan anses å ha «virkning» i Norge etter §7 uten at lovbryteren er i Norge. En gjerningsperson som har oppholdt seg i Norge, i en kortere eller lengre periode mens besittelsen varte, har hatt besittelsen i Norge.

Dagens rettstilstand medfører at gjerningspersonen selv kan sette seg ut av besittelsen ved å gi opp disposisjonsretten eller slette materialet før personen kom til Norge. Dersom sletting eller frasigelse av disposisjonsretten ikke er gjort er besittelsesforbudet overtrådt og handlingen foretatt i Norge, jf. §4. Besittelsen kan følgelig straffes etter norsk lov.

2.5 Legalitetsprinsippet i relatet til Internettkriminalitet og jurisdiksjon

Straffelovens stedlige virkeområde har en side mot domstolenes kompetanse, og en side mot legalitetsprinsippet.[40] [41] Selv om legalitetsprinsippet ikke har sitt kjerneområde i straffelovens jurisdiksjonsbestemmelser vil prinsippet kunne ha virkning på selve utøvelsen og håndhevingen av jurisdiksjon. På strafferettens område fremgår legalitetsprinsippet av Grunnloven §96, som slår fast at «Ingen kan dømmes uten etter lov eller straffes uten etter dom.» Det følger av bestemmelsen at domstolene har enekompetanse til å idømme straff og at straffedom bare kan avsies med hjemmel i lov.[42] Slik regelen i § 96 er tolket er det ikke tilstrekkelig at hjemmelen er forankret i formell lov. Lovhjemmelen må også være tilstrekkelig klar, eller tydelig.

Ved utformingen av de nye straffebestemmelsene ble det lagt til grunn prinsippet om teknologi- og innholdsnøytralitet for å ta høyde for den fremtidige utviklingen så langt det var mulig. For å ta hensyn til videre utvikling må enkelte straffebud utformes mer generelle enn andre, men legalitetsprinsippet setter grenser for hvor generelt straffebud kan utformes. Dersom generaliserings- eller abstraksjonsnivået blir for høyt, fratas straffebudene også noe av de pedagogiske og opplysende funksjoner.[43]

Hovedformålet med legalitetsprinsippet er å verne mot overgrep og å gjøre det mulig for borgerne å forutberegne sin rettsstilling. Dersom lovbestemmelser er uklare kan uklarheten føre til at det materielle rettssikkerhetsbegrepet står i fare for å bli overtrådt.[44]

---

[39] Inger Marie Sunde, *Datakriminalitet: En fremstilling av strafferettslige regler om datakriminalitet*, side 58
[40] Rt. 2010 s. 1271, avsnitt 9

[41] Jo Stigen, «Lokalisering av straffbare handlinger», side 144

[42] Norsk Lovkommentar, note (229)
[43] NOU 2007:2 s.43
[44] NOU 2009:15, punkt 7.5

Metodekontrollutvalget uttalte i NOU 2009:15 at «Utvalget er nok likevel av den oppfatning at forutberegnelighet har en verdi i seg selv, idet borgerne gis anledning til å vite hvordan det faktisk forholder seg, selv om man skulle være uenig i de verdier inngrepshjemlene bygget på.»[45]

Etter min vurdering vil det å operere med en utvidet jurisdiksjon enn det som fremgår av straffeloven, dens forarbeider og rettspraksis sies å kunne komme i konflikt med legalitetsprinsippet, da en utvidet jurisdiksjon gjør det vanskeligere å kunne forutberegne sin rettsstilling. Når det gjelder eiere av servere, skylagringstjenester og nettsider vil det også være sterkt urimelig å kreve at de må sette seg inn i alle lands straffelovgivning og jurisdiksjonsbestemmelser for å sørge for at innholdet på deres server eller nettside er i samsvar med loven. Hensynet til forutberegnelighet taler videre for at jurisdiksjonsbestemmelsene i den norske straffeloven i tvilstilfeller ikke bør tolkes utvidende, iallfall i tilfeller der hjemmelen anses som uklar.

Ved uklar lovhjemmel kommer også klarhetsregelen i legalitetsprinsippet inn i vurderingen. Klarhetskravet stiller nemlig opp en generell skranke mot at en straffedom ikke skal kunne avsies på grunnlag av «alminnelige rettsgrunnsetninger.»[46] I dette legges det at det aktuelle straffebudet ikke kan tolkes videre enn hva som fremgår av loven, og rettspraksis viser til at det ikke er «...avgjørende hva lovgiver måtte ha ment, når en eventuell lovgiverintensjon ikke har kommet tydelig til uttrykk i loven.»[47] Legalitetsprinsippet stiller ikke et vilkår om absolutt klarhet i straffebudet, men en handlingsnorm må fremgå klart nok av straffebudet og hvem det gjelder for, jf. Rt. 2001 s.1303.

Et annet hensyn som kan spille inn på hvor vid tilnærming til jurisdiksjon kan tillates er hensynet til rettssikkerhet, da spesielt hensynet til forutberegnelighet. Dette hensynet gjør seg gjeldende når spørsmålet er om handlinger som skjer ut over landegrenser skal straffeforfølges av norske myndigheter. Hensynet gjør seg spesielt gjeldende når det er snakk om utenlandske statsborgere eller norske statsborgere som bor fast i utlandet. Det kan ikke legges til grunn at utenlandske statsborgere skal ha innsyn i norsk rett, hensynet til forutberegnelighet er således essensielt i en vurdering av norsk jurisdiksjon i tilfeller der en

[45] NOU 2009:15, punkt 7.5
[46] Arne Fliflet – Grunnloven Kommentarutgave s. 391
[47] Rt.1977 s. 1207

handling helt eller delvis begås av en gjerningsmann som ikke befinner seg på norsk territorium.

Slik som jurisdiksjonsbestemmelsene er utformet nå, står norske domstoler mer fritt til å finne gode løsninger i enkeltsaker med de mer generelle jurisdiksjonsbestemmelsene, og forarbeidene når det gjelder Straffelovens jurisdiksjonsbestemmelser er utdypende på mange forskjellige typetilfeller av Internettkriminalitet og hvordan jurisdiksjon kan løses i slike tilfeller. Disse forarbeidene vil utgjøre en god støtte for domstolenes løsninger, men i tilfeller som ikke har vært tatt opp i forarbeidene og tidligere rettspraksis vil domstolene måtte finne støtte for sine løsninger i utenlandsk rettspraksis, teori og lovgivning. En slik løsning vil bidra til en usikkerhet rundt det å kunne forutberegne sin rettsstilling. Den beste løsningen er nok å legge til grunn det samme som Høyesterett har gjort i de få dommene som gjelder Internettkriminalitet – fokusere på hva Straffelovens forarbeider har sagt og bygge avgjørelsene på de norske forarbeidene i første omgang.

2.6 Folkerettslige begrensinger straffeloven §2

Retten til å straffeforfølge handlinger foretatt på norsk territorium er en selvsagt del av den norske suvereniteten. På bakgrunn av folkeretten kan en stat etter følgende prinsipper også straffeforfølge utenlandshandlinger: det aktive personalprinsipp (egne borgeres handlinger i utlandet), det passive personalprinsipp (egne borgere er ofre for handlinger i utlandet), beskyttelsesprinsippet (handlinger i utlandet som truer statens vitale interesser) og universalprinsippet (et lite knippe særlige alvorlige forbrytelser begått av utlending i utlandet uten at statens særinteresser er berørt).[48] Universalprinsippet er en vid tilnærming til jurisdiksjon, og anvendes av de fleste nasjoner kun i svært bestemte tilfeller, da for eksempel ved folkemord, krigsforbrytelser, etnisk rensing og forbrytelser mot menneskeheten.

Den norske Straffeloven bygger jurisdiksjon som hovedregel ut i fra territorialprinsippet, jf. Straffeloven §4. Videre bygges norsk straffelovs jurisdiksjon på det aktive personalprinsipp og beskyttelsesprinsippet, jf. Straffeloven §5. Straffeloven §7 viser til at det passive personalprinsipp (offerets nasjonalitet eller oppholdssted) også er indirekte lovfestet. Universalprinsippet kan utledes av Straffeloven §5 første ledd nr.2 og 3.

Det fremgår derimot av Straffeloven §2 at «Straffelovgivningen gjelder med de begrensninger som følger av overenskomster med fremmede stater eller av folkeretten for øvrig.»

[48] Innst. O. nr. 72 (2004-2005) punkt 12.4.1

Straffelovens lokaliseringsbestemmelse og bestemmelsens betydning for norsk territoriell jurisdiksjon må på bakgrunn av straffeloven §2 tolkes i lys av mulige folkerettslige begrensninger.[49]

De generelle reglene om jurisdiksjon som er omtalt ovenfor kan i enkelte tilfeller tenkes å komme i konflikt med konkrete bestemmelser i traktater som Norge er bundet av. I slike tilfeller følger det av Straffeloven §2 at folkerettslige forpliktelser går foran jurisdiksjonsbestemmelsene. I tillegg inneholder EØS-loven generelle regler om forrang for lov og forskrift som er gitt for å gjennomføre forpliktelser etter EØS-avtalen.[50] Den folkerettslige begrensningen i §2 sørger derimot for at en bestemmelse i den norske Straffeloven ikke skal få et videre stedlig virkeområde enn det folkeretten tillater.[51]

Norge har ratifisert flere internasjonale konvensjoner, noen som gjelder for datakriminalitet og noen som gjelder opphavsbeskyttet materiale på Internett. Den mest aktuelle konvensjonen for denne avhandlingen er Datakrimkonvensjonen, som Norge har ratifisert. For å avklare den norske rettstilstanden når det gjelder Internettkriminalitet vil det derfor være hensiktsmessig å se om Datakrimkonvensjonen kan supplere jurisdiksjonsbestemmelsene i Straffeloven.

3. Datakriminalitet og jurisdiksjon – Datakrimkonvensjonen, Storbritannia, Tyskland og USA

3.1 Datakrimkonvensjonen (Budapest Convention on Cybercrime)

3.1.1 Generelt om Datakrimkonvensjonen

Datakrimkonvensjonen ble vedtatt 8. november 2001, og undertegnet av Norge 23. november 2001, jf. kgl. res. 16. november 2001.[52] Per dags dato (april 2018) har 56 stater undertegnet konvensjonen, mens 57 stater har ratifisert konvensjonen.[53] Datakrimkonvensjonen har som mål å legge opp til en harmonisering av nasjonal rett på strafferettens og straffeprosessens område. Videre er konvensjonens formål å effektivisere mekanismene for internasjonalt samarbeid for bekjempelse av datakriminalitet, og for utnyttelse av elektroniske bevis innen enhver form for kriminalitet. Konvensjonen er en folkerettslig forpliktelse som kan gjøres gjeldende i tilfeller av Internettkriminalitet. På bakgrunn av dette må det derfor vurderes om

[49] Jo Stigen; Lokalisering av straffbare handlinger, punkt. 1.3. (TFS 2011-2)
[50] NOU 2007: 2 s.144
[51] Ot.prp. (2003-2004) punkt 13.5.2.1
[52] Europarådets Convention on Cybercrime av 21. november 2001 8185 ETS
[53] https://en.wikipedia.org/wiki/Convention_on_Cybercrime

konvensjonen kan påvirke vurderingen under lokaliseringen av en straffbar handling etter straffelovens geografiske jurisdiksjonsbestemmelser.

3.1.2 Datakrimkonvensjonen artikkel 22

Det fremgår av Datakrimkonvensjonen art. 22 nr. 1 bokstav a-d at hver part skal vedta slike lovgivningsmessige og andre tiltak som måtte være nødvendige for å etablere jurisdiksjon over et lovbrudd som er etablert i samsvar med artikkel 2 til 11 i denne konvensjon når lovbrudd er begått (a) i en parts «…territory…», (b) «…on board a ship flying the flag of that Party…», (c) «…on board an aircraft registered under the laws of that Party…» og (d) «…by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.»

Datakrimkonvensjonen art. 22 nr. 1 bokstav a-d forplikter Statene til å gjennomføre territorialprinsippet.[54] Territorialprinsippet går ut på at en stat har fullt rådvelde på eget territorium både med tanke på lovgivning og håndhevelse, og bruken av denne kompetansen er i utgangspunktet et indre anliggende som andre stater plikter til å respektere. Unntak fra prinsippet følger blant annet av alle staters plikt til å respektere internasjonale menneskerettigheter. Dersom en stat skal utøve tvangsmyndighet på en annen stats territorium krever det særskilt hjemmel for å ikke komme i strid med folkeretten.[55]

Ordlyden til art. 22 nr. 1 forstås som at artikkelen har som mål å forplikte medlemslandene til effektiv utforming av lov slik at de nasjonale lovene er dekkende for de straffbare handlingene som er videre definert i art. 2 til 11.

Den norske Straffeloven (2005) §§4-7 er utformet likt Datakrimkonvensjonens art. 22 nr. 1 bokstav a-d, noe som Datakrimutvalget i utformingen av lovforslag til den nye, nå gjeldende Straffeloven, kort slo fast ved å vise til at forpliktelsen etter konvensjonens artikkel 22 er oppfylt på bakgrunn av Straffeloven §12 (nå Straffeloven §4).[56] Dette viser til at Norge som en ratifiseringsstat forsøker å harmonisere sitt lovverk opp mot bindende internasjonale konvensjoner, for å være i samsvar med internasjonal gjeldende rett. Det fremgår videre av artikkel 22 nr. 4 at bestemmelsene i artikkel 22 ikke er til hinder for at statene etablerer en mer vidtrekkende jurisdiksjon enn det som følger av konvensjonen.[57]

[54] NOU 2007:2 punkt 8.2
[55] https://snl.no/territorialprinsippet_-_folkerett
[56] NOU 2007:2 punkt 5.1.3 (side 58)
[57] NOU 2007:2, punkt 8.2

Datakrimkonvensjonen sier ikke noe om locus delicti (lokalisering av den kriminelle handlingen) når det gjelder Internettkriminalitet, ikke noe om datakriminalitet generelt heller. Konvensjonen har lagt ballen på medlemslandenes side, og det er opp til ethvert land å avgjøre locus delicti basert på deres nasjonale lov(er) og rettspraksis.[58]

I kontrast til andre internasjonale konvensjoner som regulerer alvorlige forbrytelser som folkemord og forbrytelser mot menneskeheten inneholder ikke Datakrimkonvensjonen artikkel 22 noen forpliktelse om å undersøke eller tiltale. Bestemmelsene i Datakrimkonvensjonen er bare ment å være et minstekrav, og stater kan derfor vedta strengere bestemmelser, eller gjøre unntak for mindre alvorlige handlinger.[59]

Et rettsområde som Datakrimkonvensjonen regulerer, og som er veldig aktuelt både her i Norge og internasjonalt nå for tiden, er lover relatert til barnepornografi og besittelse/produksjon osv. av denne typen ulovlig materiale.

Det fremgår av Datakrimkonvensjonen artikkel 9 nr. 1 bokstav e, at «Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct (…) possessing child pornography in a computer system or on a computer-data storage medium." Medlemsstater forpliktes av konvensjonen for det første å kriminalisere all form for barnepornografi og seksuelle fremstillinger av barn, og for det andre til å straffeforfølge oppbevaring av barnepornografi på et datasystem eller et datalagringsmedium.

Hvorvidt Norge som medlem av Datakrimkonvensjonen oppfyller kravet til å kriminalisere handlinger beskrevet i Datakrimkonvensjonen artikkel 2-11 har vært tatt opp i både NOU 2003: 27 og NOU 2007: 2. I NOU 2003: 27 viste lovutvalget til at Straffeloven 1902 §204 (1) bokstav d (nå §311) rammer den som «produserer, innfører, besitter, overlater til en annen eller mot vederlag gjør seg kjent med barnepornografi.» Besittelse omfatter oppbevaring på skylagringstjenester, servere, harddisker og lignende lagringsenheter. Besittelseskravet oppstiller ikke noe krav om at gjerningspersonen må ha materialet fysisk hos seg. I forarbeidene til endringslov 1. august 2003 nr. 86 legger departementet til grunn at begrepet «skildringer» også omfatter fiktive eller animerte bilder, jf. Ot.prp. nr. 45 (2002-2003) s. 55.

Etter min mening viser forarbeidene til at straffeloven §311 langt på vei oppfyller forpliktelsene i artikkel 9, men som artikkel 9 nr. 1 bokstav d viser til er statene pliktige til å

[58] Bert-Jaap Koops, Susan W. Brenner, *Cybercrime and Jurisdiction,* side 10-11
[59] Stein Schjølberg, *Cybercrime: Straffbare handlinger mot den alminnelige orden og fred i cyberspace*, s. 17-18

straffesanksjonere anskaffelse av barnepornografi. Etter norsk rett er ikke selve anskaffelseshandlingen straffbar, da forarbeidene til Straffeloven viser til at det ikke er straffbar besittelse dersom man bare leser eller ser på det barnepornografiske materialet på egen skjerm uten at materialet er lastet ned.[60] Norsk forståelse når det gjelder denne typen materiale at en straffbar handling først oppstår når det ulovlige materialet publiseres eller lastes ned. Norsk forståelse er ikke i direkte samsvar med konvensjonen på dette punktet, men Norge har valgt å bruke reservasjonsretten sin når det gjelder besittelse av ulovlig materiale, noe som ble foreslått av Datakrimutvalget.[61]

Norsk rett er ellers i samsvar med konvensjonsforpliktelsene gitt i artikkel 9 nr. 2 som forplikter statene til å kriminalisere befatning med pornografisk materiale der som person fremstår som barn. Etter lovendring 1. august 2003 regnes en person som fremstår som under 18 år som barn i relasjon barnepornografibestemmelsen. Det er en global oppfatning at all slags former for barnepornografi, også datarelatert barnepornografi, bør være kriminalisert, noe som den norske Straffelovutvalget også har lagt til grunn i Straffelovens forarbeider.[62]

Etter min vurdering fremstår de norske jurisdiksjonsbestemmelsene som harmonisert og i samsvar med minstekravene gitt i Datakrimkonvensjonen. Gjennom en harmonisering fremsatt av Datakrimkonvensjonen vil risikoen reduseres for etablering av jurisdiksjoner med manglende tilsvarende standard, og konvensjonen fører til en styrking av det internasjonale samarbeidet og en lik internasjonal standard av straffebestemmelsene. Jeg tilfører for ordens skyld at bestemmelsene i Datakrimkonvensjonen er, som nevnt tidligere, bare ment å være et minstekrav, og stater kan derfor vedta strengere bestemmelser, eller gjøre unntak for mindre alvorlige handlinger.[63] Hva som forstås som «mindre alvorlige handlinger» er derimot opptil ethvert land selv å bestemme, og en slik utforming som dette fører etter min mening dessverre til at det ikke blir en tilsvarende lik standard blant medlemslandene da «mindre alvorlige handlinger» er en subjektiv vurdering.

Et felles internasjonalt regelverk som sikrer både en kriminalisering av datakriminalitet, og muligheten for å faktisk gjennomføre straffeforfølgning, er helt avgjørende dersom man skal greie å bekjempe trusselen som datakriminalitet representerer overfor det moderne samfunn.[64]

---

[60] Ot. prp. nr. 28 (1999-2000) s. 99
[61] NOU 2003: 27, punkt 2.9.3
[62] NOU 2003: 27, side 25-26

[63] Stein Schjølberg, *Cybercrime: Straffbare handlinger mot den alminnelige orden og fred i cyberspace*, s. 17-18
[64] NOU 2002:7 punkt 8.8

Derfor er det positivt at flere land har ratifisert Datakrimkonvensjonen og har oppfylt minstekravet som bestemmelsene i konvensjonen stiller opp.

3.2 Datakriminalitet og jurisdiksjon – Storbritannia

3.2.1 Materiell jurisdiksjon

Når datakriminalitet defineres vises det i britisk juridisk teori[65] til Datakrimkonvensjonens definisjon og inndeling av handlingen i tre kategorier. Internettkriminalitet bærer, som nevnt også under punkt 2, et preg av å være transnasjonal – de straffbare handlingene følger ikke nødvendigvis landegrenser.

Utgangspunktet for internasjonal strafferett er at en forbrytelse begått innenfor en stats territorium kan prøves der, selv om straffelovens territoriale bestemmelser ikke sammenfaller med territorial suverenitet.[66] Den tradisjonelle britiske oppfatningen av territoriell jurisdiksjon er relativt snever i sin tolkning da oppfatningen viste til at territoriell jurisdiksjon ble bestemt hvor *actus reus* (den skyldige handlingen) ble gjennomført. Den tradisjonelle oppfatningen tok ikke høyde for at lovbryter kunne oppholde seg i utlandet og at virkningen kunne skje i Storbritannia. Engelsk Court of Appeal[67] behandlet i 2004 det generelle prinsippet om straffelovsjurisdiksjon i henhold til engelsk common law. Domstolen kom frem til at jurisdiksjon bestemmes ut i fra om «the last act took place in England or a substantial part of the crime was committed here.» Den nye oppfatningen av territorialprinsippet og jurisdiksjon er betydelig videre enn den gamle, snevre oppfatningen.

Den nye oppfatningen fremlagt den engelske domstolen om at det er tilstrekkelig at delvis av handlingen var begått i Storbritannia samsvarer med forståelsen lagt til grunn av en tingrett her i Norge, jf. drøfting av RG. 2001 s.218 under punkt 2.4.

Akkurat som Norge møter rettshåndhevere og lovgivere i Storbritannia flere problem ved Internettkriminalitet – kan for eksempel den kriminelle handlingen anses for å ha blitt begått på britisk territorium? Og kan britiske lover anvendes?

Jurisdiksjon og lokalisering av den kriminelle handlingen har blitt behandlet av det britiske House of Lords i blant annet R v. Governor of Brixton Prison and another, ex parte Levin 1996 (også kalt Citibank fraud, USA.) I denne aktuelle saken hevdet den anklagedes (Levin)

[65] Dr. Ian Walden, *Cybercrime and jurisdiction in the United Kingdom*
[66] A. Cassese, *International Criminal Law* side 277, (Oxford, Oxford University Press 2003)
[67] Smith (Wallace Duncan) (No. 4) [2004] QB 1418, på s.57

forsvarer at den kriminelle handlingen ble begått i St. Petersburg på det tidspunktet Levin trykket bestemte knapper på tastaturet og satte i gang falske transaksjoner fra Citibank, og at russisk lov måtte bli gjeldende. Aktoratet hevdet på sin side at handlingen ble begått i USA og kunne straffes etter USAs straffelov fordi endringene av dataene (effekten/skaden av handlingen) inntraff i USA. Det ble i denne saken dømt i aktoratets favør på bakgrunn av at «the real-time nature of the communication link between Levin and the Citibank computer in USA meant that Levin's keystrokes were actually occurring on the Citibank computer.»[68] Denne forståelsen er derimot stikk i strid med hva juridisk teori i Storbritannia mener at jurisdiksjon skal avgjøres.

I avgjørelsen i denne saken ble det i vurderingen om lokaliseringen av handlingen lagt vekt på hvor effekten/skaden av den kriminelle handlingen fant sted, ikke hvor handlingen ble utført. Norske forarbeider har åpnet opp for at en lignende forståelse kan legges til grunn her i Norge, men at handlingen må ha virkning eller tilsiktet virkning i Norge eller mot et norsk rettsgode.

3.2.2 Lovbestemte regler

For å sikre og styrke legalitetsprinsippet i tilfeller ved jurisdiksjonsspørsmål knyttet til datakriminalitet og Internettkriminalitet har strafferettslige common-law prinsipper om jurisdiksjon blitt lovfestet konkret eller henvist til gjennom eksplisitte jurisdiksjonsbestemmelser i annen lovgivning. Bakgrunnen for denne endringen av oppfatning er saken R v. Gold, Schifreen (1988 2 All ER 186).

I saken R v. Gold, Schifreen ble det uttalt at lovgrunnlaget på sakens tidspunkt ikke var tilfredsstillende når det gjaldt regulering av datakriminalitet, og at det var svært tydelig at det var nødvendig å utarbeide et nytt lovverk for å kunne henge med på den teknologiske utviklingen. Det ble videre vist til at måten ordlyden i Forgery and Counterfeiting Act 1981 ble brukt i en videre forstand enn det som var tiltenkt terminologien i loven. Som en følge av R v. Gold, Schifreen ble The Computer Misuse Act utarbeidet og trådte i kraft i 1990.

Etter Computer Misuse Act 1990 kan overtredelse bli begått av enhver person[69], og britisk statsborgerskap har ikke noen særlig påvirkning når det gjelder overtrederens skyld.[70] Jurisdiksjon i transnasjonale aktiviteter er utøvd gjennom konseptet om en «significant link»

[68] R v. Governor of Brixton Prison and another, ex parte Levin (1996) 4 All ER 350, s.363 a
[69] Computer Misuse Act 1990 section 9
[70] Bert-Jaap Koops, Susan W. Brenner, *Cybercrime and Jurisdiction*, side 297

som må være til stede i «the home country.» Med «the home country» menes det at handlingen må ha blitt utført eller ha inntruffet i England og Wales, Skottland og Nord-Irland.

Med «significant link» menes det at handlingen må være straffbar etter britisk lov. Et andre alternativ er at enten den skyldige eller offeret befinner seg på britisk territorium, eller at handlingen eller skaden av handlingen hadde innvirkning på britisk territorium – handlingen må ha en tilknytning til britisk territorium.

Criminal Justice Act 1993, som regulerer bedrageri og forfalskning, har også inkorporert noen regler som spesifikt regulerer jurisdiksjon ved datakriminalitet og Internettkriminalitet. Lovens del 1 viser til at jurisdiksjon bestemmes på bakgrunn av en «relevant event.» En handling anses som relevant dersom en falsk eller svindelmelding er sendt eller mottatt i England og Wales.[71] Criminal Justice Act 1993 legger i likhet til Computer Misuse Act 1990 til grunn at den kriminelle handlingen må ha tilknytning til britisk territorium.

I punkt 2.1.4 ble det drøftet om spørsmålet om besittelse av ulovlig materiale på en utenlandsk skytjeneste eller nettside kunne omfattes av norsk straffelovs jurisdiksjon eller ikke. Lignende problemstilling har rettshåndhevere i Storbritannia måtte diskutere i Waddon (2000 All ER (D) 502. Spørsmålet i den aktuelle saken var hvordan jurisdiksjon skulle avgjøres i tilfeller der hvor ulovlig materiale (i denne saken barnepornografi) var publisert på en utenlandsk nettside.

Britisk Høyesterett viser i Waddon (2000 All ER (D) 502) til at det er to forskjellige handlinger eller publikasjoner som finner sted, og som er avgjørende for å avgjøre jurisdiksjon.[72] Den første handlingen skjer når data (ulovlig materiale) er lastet opp og lagt ut på en nettside. Den andre handlingen skjer når det ulovlige materialet er lastet ned.

Britisk Høyesterett legger til grunn en lik forståelse som norsk rett gjør – hvor serveren til nettstedet, og hvor nettstedet har sin opprinnelse er ikke av særlig betydelse når jurisdiksjon skal avgjøres. Det avgjørende er hvor gjerningspersonen var da han eller hun publiserte det ulovlige materialet, eller hvor han var da han lastet ned materialet.

Britisk Høyesterett bygget videre på tolkningen gitt i Waddon-saken i Perrin (2002 All ER (D) 359), og la også til grunn at section 1(3)(a) i Obscene Publication Act 1959 «offers it for sale» er en passiv form for publikasjon. Den siktede i saken, en fransk borger, hevdet at

[71] Bert-Jaap Koops, Susan W. Brenner, *Cybercrime and Jurisdiction*, side 298
[72] Waddon (2000 All ER (D) 502) avsnitt 12

nettsider opprettet og driftet i utlandet ikke kunne omfattes av britisk straffelov. Anførselen ble avvist, og det ble avgjort skyld på grunnlag av at publikasjonen gjennom nedlastning skjedde i England.

3.2.3 Jurisdiksjon utenfor britisk territorium

Som nevnt tidligere i avhandlingen er hovedregelen for en nasjons straffelovs jurisdiksjon territorialprinsippet, men i enkelte tilfeller av internasjonal kriminalitet kan jurisdiksjon hevdes på bakgrunn av 4 folkerettslige anerkjente prinsipper.[73] Disse prinsippene er det aktive personalprinsipp, det passive personalprinsipp, beskyttelsesprinsippet og universalprinsippet.

Tidligere common-law oppfatning av jurisdiksjonsspørsmålet var at dersom handlingen var begått utenfor England og Wales falt handlingen utenfor landets jurisdiksjon, selv om den anklagede er et britisk subjekt (britisk statsborger). Denne oppfatningen har blitt kalt utdatert[74], og har blitt endret ved innføring av lovbestemmelser når det gjelder enkelte overtredelser. I et forsøk på å harmonisere lovgivning med Datakrimkonvensjonen har Sexual Offences Act 2003 blitt innført, for å kriminalisere alle former for barnepornografi, også tegninger som skildrer mindreårige i pornografiske poseringer (Datakrimkonvensjonen artikkel 9 forbyr all fremstilling av pornografisk materiale som inkluderer mindreårige.) Sexual Offences Act 2003 innskrenker derimot rekkevidden av loven, og viser til at anklager kan kun stilles mot person(er) som er britiske statsborgere eller oppholder seg i Storbritannia.

Disse folkerettslige prinsippene er unntak fra hovedregelen om at jurisdiksjon baseres på territorialprinsippet, og disse unntakene gjør seg bare gjeldende i bestemte tilfeller. I Storbritannia i 2004 ble det diskutert av regjeringen om det aktive personalprinsippet skulle innføres som et lovfestet prinsipp i britisk straffelovgivning.[75], slik det er i Norge i Straffeloven §5. En slik lovfesting reiser flere motargumenter – for det første vil det oppstå praktiske problemer rundt det å måtte innhente bevis i utlandet og muligens hente inn vitner fra utlandet. For det andre er potensialet å havne i konflikt og strid med lokale lover stor, noe som kan forhindre at bevis kan innhentes, eller at de beskyldte blir utlevert. For det tredje kan det stilles spørsmål om det er offentlig interesse i saksforfølgelsen av saker der det ikke er noen innvirkning på Storbritannia. Et siste argument mot en slik lovfesting av folkerettslig prinsipp er om det med hensyn til forutberegnelighet er hensiktsmessig å gjøre britiske

[73] Bert-Jaap Koops, Susan W. Brenner, *Cybercrime and Jurisdiction*, side 299
[74] Bert-Jaap Koops, Susan W. Brenner, *Cybercrime and Jurisdiction*, side 294-296
[75] Fraud Law Reform: Government response to the consultation (November 2004), avsnitt 57

statsborgere i utlandet underlagt nasjonal lovgivning og lokal lovgivning samtidig – en slik oppfatning vil gjøre det mye vanskeligere og uoversiktlig å kunne forutse sin rettsstilling.

Til tross for disse synspunktene, vil britisk regjering måtte revurdere sin posisjon med hensyn til datakriminalitet, da de også har ratifiser Datakrimkonvensjonen. Konvensjonen innebærer jurisdiksjonsbestemmelser som inkluderer ekstraterritorial jurisdiksjon på grunnlag av det aktive personalprinsippet. Som sådan vil den britiske regjeringen være forpliktet til å vedta hensiktsmessige bestemmelser for å gjenspeile disse forpliktelsene i folkeretten. Crown Prosecution Service vil imidlertid være pålagt å vurdere offentlighetens interesse når de bestemmer seg for å fortsette på grunnlag av jurisdiksjon gjennom det aktive personalprinsippet, noe som kan være usannsynlig gitt argumentene mot.

3.3 Datakriminalitet og jurisdiksjon – Tyskland

3.3.1 Situasjonen i Tyskland

Som mange andre land har Tyskland ratifisert Datakrimkonvensjonen. Tyskland, og tyske lovgivere, har valgt til stor grad å harmonisere sin egen straffelovgivning (Strafgesetzbuch, heretter StGB) med bestemmelsene i Datakrimkonvensjonen for å reflektere den internasjonale utviklingen rundt regulering når det gjelder Internettkriminalitet.

Tysk straffelovgivning følger de fleste bestemmelsene gitt i Datakrimkonvensjonen med hensyn til materiell straffelov, og trenger derfor kun noen få endringer for å være oppdatert og i tråd med Datakrimkonvensjonen. Et av de få områdene som tysk straffelov ikke har innført bestemte lover, er produksjon, distribusjon og besittelse av hackingutstyr. Disse handlingene er ikke straffbare etter tysk lov, og det er foreslått at for å være helt i overensstemmelse med Datakrimkonvensjonen bør disse handlingene gjøres straffbare.[76]

3.3.2 Tilnærming Internettkriminalitet og jurisdiksjon

3.3.2.1 Hovedregelen for avgjøring av jurisdiksjon

Spørsmålet om tysk straffelov kan anvendes overfor tilfeller av Internettkriminalitet kan ikke besvares generelt i henhold til tysk rettssystem da Internettkriminalitet kan omfatte mange ulike lovbrudd, og den tyske loven om jurisdiksjon inneholder spesielle bestemmelser for konkrete lovbrudd. I tillegg er det et bredt spekter av fenomener med forskjellige

[76] Bert-Jaap Koops, Susan W. Brenner, *Cybercrime and Jurisdiction*, side 184

utgangspunkt for å bestemme plasseringen av den kriminelle handlingen. Tysk straffelovgivning skiller seg altså veldig fra den norske straffeloven, som er mer generelt utformet og som inneholder mer spesifikk informasjon i lovforarbeidene og uttalelser i høyesterettspraksis.[77]

I likhet med både norsk og britisk straffelov styres anvendeligheten av tysk straffelov av territorialprinsippet som i tysk straffelov er regulert i 3 StGB. I tillegg styres anvendeligheten av tysk straffelov av teorien om «ubiquity» som er regulert i § 9 StGb.

Det fremgår av 3 StGB at tysk straffelov gjelder for overtredelser som er «committed domestically.» 9 (1) StGB viser videre til at en «act is committed at every location at which the offender acted or, in the case of omission, should have acted, or at which the result inherent to the offence occurred or was expected to occur acccording to the intention of the offender.»

Forutsetningen for strafferettslig jurisdiksjon i Tyskland er altså i utgangspunktet enten at den handlingen som er et lovbrudd har skjedd på tysk territorium eller resultatet av den straffbare handlingen har skjedd på tysk territorium. Denne tosidige tilnærmingen til å kombinere handlingenes plassering og lokaliseringen av resultatet kalles teorien om «ubiquity».

Det foreligger tilfeller der hvor handlingen klart faller inn under tysk territoriallovgivning. Klare tilfeller er for eksempel når lovbryteren opererer/begår handlingen i Tyskland, eller at resultatet/skaden av handlingen inntraff – den hadde virkning i Tyskland, jf. seksjon 9 (1) StGB.

Ordlyden til den tyske straffeloven seksjon 9(1) StGB er lik ordlyden til den norske Straffeloven §4 og §7 – likheten ligger i det at begge bestemmelser først viser til territorialprinsippet, for å så regulere overtrederens intensjoner, «... expected to occur according to the intention of the offender» (s. 9(1) StGB) og jf. Straffeloven §7 handlingen anses foretatt også der virkningen er «inntrådt» eller «tilsiktet» fremkalt.

På de mer generelle jurisdiksjonsbestemmelsene er de tyske straffelovsbestemmelsene lik de norske straffelovsbestemmelsene, men tysk straffelov skiller seg ut ved at det for enkelte spesialbestemmelser som gjelder enkelte former for datakriminalitet (hacking, forfalskning etc.) har egne jurisdiksjonsbestemmelser knyttet til disse spesialbestemmelsene.

[77] NOU 2003: 27, NOU 2007:2

Tyskland har, i tråd med Datakrimkonvensjonen og andre internasjonale konvensjoner, i seksjon 4-7 StGB blant annet forbudt slavehandel, distribusjon av narkotika, spredning av barnepornografi og forfalskning av betalingskort. Tysk straffelov kan anvendes på overtredelser nevnt i seksjon 5-7 StGB uansett hvor den kriminelle handlingen er begått, så fremt de kriminelle handlingene har tilstrekkelig tilknytning til Tyskland.[78] Norsk straffelov har inntatt en lignende utvidet jurisdiksjon for §§ 136, 183, 185 og 311, jf. straffeloven §5 første ledd br. 9-11 og §6. Norge har en litt videre tolkning av jurisdiksjon enn Tyskland da de norske grunnlagene kommer til anvendelse også når man mangler kunnskap om hvor gjerningspersonen var på det avgjørende tidspunktet.[79]

Oppbevaring av ulovlig materiale på utenlandsk server har i likhet med norsk straffelov blitt diskutert i henhold til tysk straffelov. I en tysk lovkommentar legges det til grunn at det er først på serveren gjerningspersonen målrettet og kontrollert lagrer informasjonen,[80] og det er først fra serveren informasjonen kan lastes ned av andre og dermed få sin skadevirkning.[81] På bakgrunn av dette kan man straffes ved opplasting eller nedlastning fra denne serveren såfremt gjerningspersonen oppholdt seg på tysk territorium på opplastnings/nedlastningstidspunktet. I likhet med tysk lovkommentar har Salten herredsrett i underrettsdom valgt en lignende tilnærming til Internettkriminalitet og bruk av utenlandske servere. Underrettsdommen, RG 2001 s. 218, åpnet for at handlingen i den aktuelle saken kunne anses som «begått delvis i Norge og delvis i utlandet, hvor serveren sto.» Retten tok ikke stilling til om serverens plassering genererte noe gjerningssted, men Datakrimutvalget forutsetter i Delutredning II[82] at dette er mulig.

I tillegg til territorialprinsippet, bygger tysk straffelov på de tre ekstraterritorielle prinsippene om «active personality», «universality principle» og «protective principle.» I likhet med britisk straffelovgivning bruker tysk straffelovgivning disse prinsippene til å supplere territorialprinsippet i enkelte bestemte saker, for å kunne utøve jurisdiksjon utenfor sine territorielle grenser. Tysk straffelovgivnings jurisdiksjon skiller seg litt ut fra norsk og britisk jurisdiksjon ved at den tyske straffeloven har lovfestet offerprinsippet og tillater utvidet jurisdiksjon på bakgrunn av dette. Etter 7 StGB kan tyske myndigheter utøve utvidet

[78] Bert-Jaap Koops, Susan W. Brenner, *Cybercrime and Jurisdiction*, side 188
[79] Inger Marie Sunde, *Datakriminalitet: En fremstilling av strafferettslige regler om datakriminalitet*, side 51

[80] Eser 2006, *supra* note 48, s. 121, som viser til Cornils, «Der begehungsort von Äusserungsdelikten im Internet», *Juristenzeitung* 1999, s. 396.
[81] Eser 2006, *supra* note 48, s. 123-124
[82] NOU 2007:2, Lovtiltak mot datakriminalitet, punkt 8.4.4.

jurisdiksjon når gjerningspersonen eller offeret er tysk borger og handlingen er straffbar etter loven om jurisdiksjon hvor den påståtte handlingen er begått.

3.3.3 «Abstract endangerment offenses»

For tysk strafferett er det mest uklare området når det gjelder Internettkriminalitet under såkalte «abstract endangerment offenses». Eksempler på «abstract endangerment offenses» er spredningsforbrytelser og taleforbrytelser, som for eksempel å tilgjengeliggjøre pornografi, forherligelse av vold, eller hatefulle rasistiske eller nasjonalsosialistiske ytringer.

En lovovertredelse er kategorisert som «abstract endangerment offenses» hvis den gjør en oppførsel straffbar fordi den er iboende farlig, mens det ikke er relevant for fullførelsen av lovbruddet at gjerningsmannen faktisk har skadet eller truet bestemte personer eller gjenstander. Når en bestemt fare for eiendom eller personer er et element i lovbrudd, er en slik forbrytelse kalt «specific endangerment offenses».

Anvendelsen av territorialprinsippet etter seksjon 3 og 9 StGB på tilfeller av spredning av ulovlig materiale eller hatefulle ytringer fremsatt i et fremmed land er veldig kontroversielt, mye fordi tysk rett går langt utenfor sin territoriale jurisdiksjon for å straffe spredningen eller ytringen. Det tyske rettssamfunn har vært, og fremdeles er, splittet[83] om hvordan en etter tysk straffelovgivning skal avgjøre jurisdiksjon i tilfeller ved Internettkriminalitet. Det har blitt argumentert for å ta utgangspunkt i både en snever tilnærming, utvidet tilnærming og et kompromiss mellom de to tilnærmingene.

3.3.3.1 Snever tilnærming «abstract endangerment offenses»

Den snevre tilnærmingen i tysk strafferett tar utgangspunkt i at «abstract endangerment offenses» ikke har en «location of criminal result» i rettslig forstand etter seksjon 9(1) tredje alternativ StGB. I stedet hevdes det at «abstract endangerment offenses» bare har en «location of criminal act», jf. seksjon 9 (1) første alternativ StGB.

Den snevre tilnærmingen kan forstås slik at dersom en gjerningsperson publiserer for eksempel pornografisk eller nasjonalsosialistisk materiale på en utenlandsk nettside eller nettserver faller utenfor tysk straffelovs jurisdiksjon. Også en som linker til en tysk nyhetsside og lignende kilder som ligger på en utenlandsk nettside eller nettserver kan falle utenfor tysk jurisdiksjon. Denne forståelsen av seksjon 9(1) StGB er veldig snever, kanskje for snever, da

[83] Bert-Jaap Koops, Susan W. Brenner, *Cybercrime and Jurisdiction*, side 189

det er mange tilfeller/handlinger som faller utenfor tysk jurisdiksjon om tilnærmingen legges til grunn.

3.3.3.2 Vid tilnærming «abstract endangerment offenses»

Den vide tilnærmingen i tysk straffelov tar utgangspunkt i at en «location of the criminal result» er gitt alle plasser der hvor den abstrakte faren kan oppstå. Ut i fra den vide tilnærmingen kan en person straffes etter tysk lov selv om han eller hun oppholder seg i utlandet. Dette kan for eksempel gjelde dersom personen har sendt pornografisk eller nasjonalsosialistisk materiale, eller sendt fornærmende kommentarer/uttalelser til Tyskland. Om denne informasjonen kunne ses på en tysk server/nettside eller ikke spiller ikke så stor rolle etter den vide tilnærmingen når det gjelder «abstract endangerment offenses». På grunn av Internetts globale preg tar den vide tilnærmingen høyde for at det er mulig at det ulovlige materialet kan bli sett på i Tyskland av tyske borgere eller personer som oppholder seg i Tyskland, og dette er derfor tilstrekkelig for å hevde jurisdiksjon i tilfeller ved «abstract endangerment offenses».

En av mange konsekvenser en slik vid forståelse kan få, dersom den skulle få en større oppfølging av flere innad i rettssamfunnet i Tyskland, er at praktisk talt alt materiale på Internett kan bli subjekt for tysk straffelovgivning.[84] [85]

En annen konsekvens av denne vide tilnærmingen er at den vide omfavnelsen tysk straffelovgivning får kan, og mest sannsynligvis vil, kunne komme i konflikt med et annet lands territorielle rettigheter og landets straffelovgivning. Som medlem av Datakrimkonvensjonen er man til en viss grad oppfordret til å samarbeide med andre medlemsland gjennom utleveringsavtaler, informasjonssamarbeid osv. for å bekjempe Internettkriminalitet på en effektiv måte, men det er ikke noe krav om at medlemmene må samarbeide. Det er opptil ethvert land å bestemme hvorvidt de tillater et fremmed å utøve jurisdiksjon overfor deres egne borgere.

3.3.3.3 Forslag til kompromiss mellom snever og vid tilnærming

[84] B. Heinrich, *The Location of the Criminal Result in Abstract Endangerment Offenses* (1999) side 76

[85] N. P Flechsig & D. Gabel, *Criminal Liability on the Net for Providing Hyperlinks* (1988) side 352

For å unngå de vidtrekkende, negative konsekvensene som følger av å sammenligne plasseringen av det kriminelle resultatet med plasseringen av «abstract endangerment» har noen forfattere valgt å inkludere ekstra subjektive eller objektive kriterier.[86]

Til den vide tilnærmingen har det vært argumentert for at det bør høre med et tilleggskrav om at den anklagede enten visste eller burde ha visst at det ulovlige materialet han la ut kunne bli sett i Tyskland. Et annet krav er at han hadde målrettet valgt Tyskland og tyske borgere som mottakere av materialet.

Andre har krevd en territorialforbindelse som objektivt kriterium.[87] Med territorialforbindelse menes det at gjerningspersonen eller den kriminelle handlingen begått over Internett må ha en forbindelse til Tyskland, for eksempel at gjerningspersonen befinner seg i Tyskland mens handlingen er begått i Tyskland eller at virkningen/skaden av den straffbare handlingen inntreffer i Tyskland.

Noen forfattere[88] viser til at materialets språk utgjør en tilstrekkelig territorialforbindelse. En lignende forståelse har tidligere Justisminister Dørum uttalt i 2002 da han ble spurt om straffelovens rekkevidde relatert til sider på Internett, der hvor han viste til underrettsdommen RG 2001 s.219 og forståelsen lagt til grunn der: «Det vil være naturlig å prioritere de nettstedene som fremstår som særlig rettet mot et norsk publikum, for eksempel fordi nettstedet bruker norsk språk eller viser særlig interesse for norske forhold.»[89] Det ble i RG 2001 s. 219 kort vist til at hjemmesiden materialet var lagt up på ikke fremsto som rettet spesielt mot et norsk publikum, men at dette kunne brukes som et vurderingsmoment.[90]

Etter min mening kan ikke momentet om materialets språk, dersom språket er engelsk, ikke ilegges alt for stor vekt da engelsk er et universalt språk som store deler av verden forstår. Saken ville ha vært noe annet hvis det ulovlige materialet var skrevet på for eksempel norsk, da ville det fremstått som rettet mot et norsk publikum.

Tyskland har derimot gått vekk fra det foreslåtte supplerende vurderingsmomentet om materialets språk i en sak, den såkalte Toben-saken som omhandlet Holocaustfornektelse. Publiseringen av ytringene på Internett var såpass skadelig etter Forbundsdomstolens mening

[86] M. Kienle, *Internationales Strafrecht und Straftaten im Internet,* (Constance, Hartung-Gorre 1998) side 159
[87] Bert-Jaap Koops, Susan W. Brenner, *Cybercrime and Jurisdiction*, side 191
[88] E. Hilgendorf, *Thoughts on the Interpretation of the Ubiquity Principle of Criminal Law in the Age og The Internet* (1997), side 1876
[89] Odd Einar Dørum, svar på spørsmål fra Mette Gundersen (A) til justisministeren, dokument nr. 15: 107 (2001–2002). Dørum viste til Salten herredsretts i RG-2001-219.
[90] RG 2001 s. 219, på side 225

at ytringen måtte anses for å ramme Tyskland og tyske borgere, og at Fredrick Toben derfor kunne straffes etter tysk straffelov.

Toben-saken illustrerer hvor langt Tyskland kan gå i å utøve sin jurisdiksjon (Dom 12. desember 2000 – 1 StR 184/00, BGHSt 46, 212). I Toben-saken hadde en australsk borger, Fredrick Toben, på en nettside på en australsk server publisert artikler der hvor Toben fornektet at Holocaust var ekte. Etter tysk straffelov er denne typen materiale straffbart fordi det krenker minnet til ofrene for Holocaust (s. 189 StGB) og fornærmer overlevende (s. 185 StGB), men også fordi fornektelsen av Holocaust kan true den offentlige fred, jf. s.130 nr. 1, nr. 2, og / eller s.130 (3) StGB.

I Australia, da det ble reist påtale mot Toben i Tyskland, var Holocaustfornektelse bare «ulovlig» og underlagt strafferettslige sanksjoner, men ikke kriminalisert. Til tross for rettssituasjonen i hjemlandet, ble Toben fengslet under et opphold i Tyskland og dømt på tre punkter ved byretten i Mannheim.

Dommen ble anket til Forbundsdomstolen, og Forbundsdomstolen uttalte at «resultatet ifølge lovbrudett» etter s.130(3) StGB i henhold til s.9(1) tredje alternativ StGB ikke kunne likestilles med definisjonen «resultat» gitt i Tatbestandslehre, og at rettsgrunnlaget for strafferettslig jurisdiksjon i denne saken var s.9 StGB. Forbundsdomstolen viste til at formålet med denne bestemmelsen var at selv når en kriminell handling var begått i et fremmed land skulle tyske domstoler ha jurisdiksjon dersom innenlandske rettslige interesser som er lovbeskyttet av det aktuelle lovbruddet, har blitt skadet eller truet. Toben-saken legger med andre ord til grunn en veldig vid tilnærming til jurisdiksjon i saker der hvor handlingen truer sikkerheten i Tyskland og rammer tyske borgere og Tyskland som nasjon.

Som vist til tidligere så har det blitt foreslått at materialets publiseringsspråk kan være innvirkende på om handlingen faller inn under et lands jurisdiksjon eller ikke. I Toben-saken var dette tatt opp som et element i mot at Tyskland hadde jurisdiksjon da Toben hadde publisert materialet på engelsk. Forbundsdomstolen avviste i dette tilfellet anførselen da innholdet av materialet var av en slik karakter at den kunne anses for å være skadelig overfor minnet til ofrene for Holocaust og fornærmende overfor de som overlevde Holocaust. Forbundsdomstolen uttalte at siden Holocaust har en så nær tilknytning til Tyskland og tysk historie var dette tilstrekkelig for å gi grunnlag for tysk jurisdiksjon for handlingen.

Den norske Straffeloven har liknende ytringsstraffebud som tysk straffelov (Straffeloven §136, §183, §311 etc.), men norsk Straffelov legger til grunn at forbrytelsen er straffbar etter

norsk straffelovgivning såfremt lovbryteren var i Norge da publiseringen/nedlastningen/tilgjengeliggjøringen ble foretatt. Tyskland har valgt å ilegge en veldig vid tilnærming til jurisdiksjon når det gjelder denne typen forbrytelser fordi lovgivere mener disse type handlinger kan true den nasjonale sikkerheten og ramme tyske borgere og Tyskland som nasjon.

3.4 Internettkriminalitet og jurisdiksjon – USA

3.4.1 Introduksjon Internettkriminalitet og jurisdiksjon i USA

Før 1984 hadde USA ikke lover som spesifikt forbød nettverksforbrytelser, inkludert hacking, ondsinnet kodedisponering og tjenestenekt (DDoS).[91] I 1986 kom Computer Fraud and Abuse Act (CFAA). I senere tid har USA fått flere relevante lovverk som regulerer forskjellige aspekter ved datakriminalitet og Internettkriminalitet. Disse lovverkene er the «the Wiretap Act» (18 USC 2510) og The Electronic Communications Privacy Act (18 USC § 2701-2712). I tillegg kom en endring av U.S.A Patriot Act i etterkant av terrorangrepet 11. september 2001. I tråd med folkeretten baseres jurisdiksjonsbestemmelsene i disse lovverkene ut ifra territorialprinsippet.

USA sitt rettssystem og lovverk skiller seg veldig fra norsk, tysk og britisk rettssystem og lovverk. Sentrale deler av USA sitt rettssystem, særlig privatretten, strafferetten og prosessen, hører under enkeltstatene, og det er således 50 forskjellige rettssystemer. I tillegg til enkeltstaters egne rettssystemer kommer den føderale lovgivningen som regulerer blant annet konkursrett, sjørett, panterett og opphavsrett.[92]

Et par grunner til at geografisk jurisdiksjon er et så stort problem i USA er at lovbestemmelser (og jurisdiksjonsbestemmelser) varierer fra stat til stat, og fra stat til føderalt nivå. En handling som er ulovlig i en by, stat eller i nasjonen samlet, er kanskje ikke mot loven i en annen. Dette kompliserer ting hvis gjerningsmannen er på et sted der det han / hun gjør ikke er ulovlig - selv om det er en klar kriminalitet på stedet der offeret befinner seg. Ting kan videre kompliseres ved at gjerningspersonen befinner seg i en annen stat enn der handlingen hadde virkning.

For oversiktens skyld vil videre drøfting fokusere på USAs føderale jurisdiksjon.

[91] Beskrives som et koordinert angrep hvor man hindrer at noen eller noe får tilgang til informasjon eller ressurser de vil ha tilgang til ved å overbelaste offerets servere eller nettside. DDoS har vokst til å bli et problem på Internett. https://no.wikipedia.org/wiki/Tjenestenektangrep
[92] https://snl.no/Rettsvesen_i_USA

3.4.2 Jurisdiksjon Computer Fraud and Abuse Act of 1986

Computer Fraud and Abuse Act (CFAA) har som formål å beskytte konfidensialitet, integritet og tilgjengelighet av datamaskiner og nettverk. CFAA balanserer den føderale regjeringens interesse for Internettkriminalitet og statlige interesser for å straffe slike forbrytelser, dette ved å begrense føderal jurisdiksjon til de tilfellene der det foreligger en overbevisende føderal interesse (for eksempel i saker som gjelder nasjonal sikkerhet[93], andre alvorlige saker eller hvor det er en mellomstatlig forbindelse eller effekt på mellomstatlig handel.) I etterkant har det blitt lagt til nye paragrafer til CFAA, blant annet 18 USC § 1030(e)(2)(B), som åpner opp for at datamaskiner brukt til «foreign commerce or communication of the United States» kan forfølge internasjonale saker som innenrikslovbrudd.

I etterkant av terrorangrepet den 11. september 2001 ble det bestemt at det skulle gjøres en endring i U.S.A Patriot Act og CFAA. Endringene som ble gjort i 1996 ble ansett som ikke tilstrekkelige for å sikre at USA kunne forfølge hackere fra USA som angrep utenlandske datamaskiner. Lovgivere i USA uttalte videre at på grunn av den vage definisjonen gitt i CFAA så kunne de kanskje ikke kunne bistå andre land i deres nettkriminalitetsbekjempelse i de tilfellene hvor en datamaskin i USA bare var en "pass-through" (proxyserver, server mellom klient og annen server) for kriminell aktivitet med opprinnelse i utenlandske nasjoner.

For å rette opp tvetydigheten endret Kongressen CFAAs definisjon av «protected computer» for å inkludere datamaskin som er «... used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications in the United States …»[94] Denne forandringen var dels gjort for å gjøre det mulig USA å bistå i internasjonale etterforskninger.[95] Allikevel må det poengteres at lovregler om å søke, gripe inn eller få bevis utenfor USA er tvetydig og ubestemt.[96] Endringene i CFAA var gjort med den baktanke om at andre nasjoner skulle følge etter og utarbeide samsvarende lover slik at USA gjennom lovsamsvar kunne forfølge saker som har sitt opphav i andre nasjoner, men som påvirker amerikanske personer eller amerikanske interesser.

USAs antiterrorlover innebærer at amerikanske myndigheter har jurisdiksjon over all Internett-trafikk som er innom USA, dirigert via proxyservere. I teorien betyr dette at

[93] Kriangsak Kittichaisaree, *Public International Law of Cyberspace* side 94
[94] 18 USC § 1030(e)(2)(B)
[95] Bert-Jaap Koops, Susan W. Brenner, *Cybercrime and Jurisdiction*, side 320
[96] United States v. Verdugo- Urquidez, 494 US 259 (1990)

amerikanske myndigheter kan straffeforfølge all ulovlig Internett-trafikk som på en eller annen måte dirigeres via servere i USA. Dette er en vid tilnærming til jurisdiksjon, som er langt videre enn både den norske, britiske og tyske tilnærmingen til jurisdiksjon.

For å kunne forfølge og straffe kriminelle som begår Internettkriminalitet operer USA ofte med undercover sting operasjoner og internasjonalt gjennom utleveringsavtaler med andre land. Det er to tilfeller som best illustrerer USAs fremgangsmåte når det gjelder internasjonal Internettkriminalitet og jurisdiksjon. Den første saken involverte Alexey V. Ivanov og Vasiliy Gorshkov fra Russland i 2001. Den andre saken involverte Oleg Zezev fra Kazakhstan i 2003.

Ivanov-Gorshkov saken gjaldt to russiske statsborgere som kom til USA i håp om å få en jobb hos et nettverkssikkerhetsselskap kalt Invita. FBI hadde på forhånd sterke mistanker om at Ivanov og Gorshkov hadde vært innblandet i tidligere hackingtilfeller. Selskapet Invita var opprettet av FBI som en del av en stingoperasjon, noe som de russiske statsborgerne ikke var klare over. Da Ivanov og Gorshkov ankom USA og selskapet ble de spurt av undercover FBI agenter om de kunne demonstrere hackerferdighetene deres på en datamaskin som registrerte tastetrykkene deres. Ivanov og Gorshkov ble kort tid etter demonstrasjonen arrestert, på bakgrunn av at de to hadde skrevet ned flere kontonummer og passord som viste informasjon de to hadde lagret på deres datamaskiner i Russland. Etter arrestasjonen lastet FBI ned bevisene på mennenes PCer i Russland for å forsikre seg om at bevis ikke forsvant eller ble ødelagt av medhjelpere i Russland. Gorshkov hevdet at ransakelsen for det første var et brudd på USAs Fourth Amendment, og at det også var et brudd på russisk lov. En amerikansk domstol slo kort fast at siden Gorshkov var en russisk statsborger kunne han ikke påberope seg beskyttelse av Fourth Amendment og at den videre ikke kan påberopes på saker som gjelder internasjonale ransakelser mot ikke-borgere. Det ble også slått fast av domstolen at russisk lov ikke var brutt, og at det uansett var irrelevant for saker i USA. I etterkant av denne saken anmeldte Russland FBI for å sikre at de tradisjonelle grenser for jurisdiksjon skulle forbli intakt. Ivanov-Gorshkov saken demonstrerer veldig godt usikkerheten om hvordan jurisdiksjon for datakriminalitet og etterforskningen ved denne typen kriminalitet skal utøves, og hvor vid tilnærming til prosessuell jurisdiksjon USA benytter seg ved innhenting av bevis på fremmed lands territorium.

Den andre saken gjaldt Oleg Zezev som i 2003 ble dømt for utpressing og tvang relatert til forsøk på å hacke seg inn i Bloomberg finansnyhetsservice sine datasystemer. Zezev forsøkte å presse Michael Bloomberg for $200.000, og truet med å publisere konfidensiell informasjon han fikk tak i. Gjennom et samarbeid mellom Bloomberg, USA og Storbritannia ble det satt

opp et møte mellom Zezev og Bloomberg i London. I London ble Zezev arrestert av britisk undercoverpoliti og utlevert til USA. Denne saken er spesiell da den tilsynelatende tilhører enten Kazakhstans eller USAs jurisdiksjon. Men ved å arrangere et møte mellom den kriminelle og offeret i et tredje land ble den kriminelle handlingen (ekstorsjon) fullført i Storbritannia og falt derfor også under deres jurisdiksjon. Gjennom samarbeidsavtale mellom Storbritannia og USA ble Zezev videre utlevert til USA for å bli tiltalt.

USA har for det meste tatt en bred tilnærming til å bygge sin jurisdiksjon i føderale saker som har internasjonale forbindelser. Endringene i U.S. Patriot Act i 2001 forsikret at USA har myndighet til å forfølge også i internasjonale tilfeller der hvor nettverk eller datamaskiner i USA bare brukes som en proxyserver. USAs tilnærming til jurisdiksjon har vært kritisert internasjonalt[97] da USA gjerne ikke respekterer andre lands suverenitet når det kommer til innhenting av bevis på fremmed territorium i tilfeller av Internettkriminalitet. Mens USA forfølger kriminelle gjennom utlevering eller undercover stings, er situasjonen litt annerledes i Norge. Jf. utleveringsloven §2 kan ikke norske statsborgere utleveres til land utenfor Norden, og det er derfor viktig at den norske straffeloven sikrer at nordmenn som begår forbrytelser over Internett med virkning i utlandet kan pådømmes i Norge og sone her.[98]

3.4.3 Convention on Cybercrime (Datakrimkonvensjonen)

På en generell basis internasjonalt anses barnepornografi som en kriminell handling, og de aller fleste land har straffebud som regulerer dette. USA ratifiserte Datakrimkonvensjonen i august 2006.[99] Konvensjonen trådte i kraft 1. januar 2007. USA hadde på tidlig 2000-tallet en sak oppe for Høyesterett, der hvor avgjørelsen i saken ville ha vært i strid med Datakrimkonvensjonen artikkel 9 nr. 2 bokstav c dersom avgjørelsen hadde blitt stående som gjeldende rett på ratifiseringstidspunktet av konvensjonen.

Det fremstilles i Datakrimkonvensjonens artikkel 9 nr. 2 bokstav c et forbud mot barnepornografi også inkludert «any realistic images representing a minor engaged in sexually explicit conduct.» USA hadde i 1996 innført Child Pornography Prevention Act (CPPA) som var ganske lik Datakrimkonvensjonens art. 9 nr. 2 bokstav c, men amerikansk høyesterett dømte i 2002 i Ashcroft v. Free Speech Coalition at CPPA var grunnlovsstridig da den brøt med First Amendment, som omhandler prinsippet om ytringsfriheten. Høyesterettsavgjørelsen

[97] Se Ivanov-Gorshkov saken
[98] NOU 2003: 27 punkt 2.6.3.3
[99] McCullagh, Declan; Anne Broache (4 August 2006). "Senate Ratifies Controversial Cybercrime Treaty". Cnet

gjorde det med andre ord tillatt å fremstille eller være i besittelse av virtuell barnepornografi da dette måtte anses som en ytring beskyttet av ytringsfriheten i Fist Amendment. Kongressen svarte på denne avgjørelsen ved å vedta PROTECT Act 2003 for å endre den ugyldige CPPA, og å begrense forbudet mot enhver visuell fremstilling «that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct.» Hadde ikke Kongressen vedtatt PROTECT Act ville ikke virtuell barnepornografi vært straffbart i USA, og USAs forpliktelser etter Datakrimkonvensjonens artikkel 22 og artikkel 9 nr. 2 bokstav c om å forby alle former for barnepornografi ville ikke vært oppfylt.

4. Oppsummering og sluttord

4.1 Oppsummering Internettkriminalitet og jurisdiksjon

Måten å løse jurisdiksjonsspørsmålet når det kommer til Internettkriminalitet varierer sterkt fra land til land, men de aller fleste i utgangspunktet som hovedregel følger territorialprinsippet. Både Norge, Storbritannia, Tyskland og USA baserer hovedsakelig jurisdiksjon ut ifra territorialprinsippet, noe som viser til at man har harmonisert lovgivningen sin opp mot folkeretten og Datakrimkonvensjonen. Hvor langt hvert land utvider sin jurisdiksjon varier derimot veldig.

Som det kom frem under diskusjonen i punkt 2, med tilhørende underpunkter, kan norsk straffelov anvendes for kriminelle handlinger som anses som Internettkriminalitet dersom det faller innenfor norsk straffelovs jurisdiksjon som fremgår av straffeloven §§4-7.

Den norske tilnærming til jurisdiksjon tar i Straffeloven §4 utgangspunkt i territorialprinsippet og slår klart fast at handlinger begått på norsk territorium av norske borgere eller personer som bor i Norge faller inn under norsk Straffelovs jurisdiksjon. Videre bygger Straffelovens stedlige virksomhet på nasjonalitetsprinsippet – Straffeloven kan blant annet anvendes i tilfeller der hvor gjerningspersonen er norsk eller oppholder seg i Norge, jf. §5 første ledd bokstav a-c. Videre kan Straffeloven anvendes for handlinger begått av utlendinger dersom handlingen hadde virkning eller tilsiktet virkning i Norge (§7), eller handlingen forøvet i utlandet er straffbar etter gjerningsstedets rett (dobbel straffbarhet), jf. §5 første ledd nr.1. Straffelovens jurisdiksjonsbestemmelser er utformet slik at de er teknologinøytrale og kan derfor anvendes på flere typetilfeller.

Den norske tilnærmingen er på den snevre siden, men ikke for snever, da det av bestemmelsene i Straffeloven §§4-7 kan utledes et krav om at gjerningspersonen eller

handlingen må ha en form for tilknytning til Norge. Dersom det skal gjøres unntak må dobbel straffbarhet foreligge, jf. §5 første ledd nr.1. Det fremgår derimot av Straffeloven §5 første ledd nr. 9-11 og §6 at det i de nevnte unntakene kan utøves en utvidet jurisdiksjon, men at dette er unntak fra hovedregelen. For §§ 136, 183, 185 og 311 finnes flere grunnlag for utvidet jurisdiksjon. Disse grunnlagene kommer til anvendelse også når man mangler kunnskap om hvor gjerningspersonen var på det avgjørende tidspunktet.[100] Straffeloven §7 viser til at handlinger begått i utlandet som har virkning i Norge eller var tilsiktet å ha virkning i Norge, faller inn under jurisdiksjonsbestemmelsen.

I Storbritannia så vi at den britiske straffeloven har måtte tatt steget i retningen mot mer lovfestede rettsregler når det gjelder Internettkriminalitet, men at de fremdeles har en lang vei å gå ved videre utarbeidelse av mer oppdaterte rettsregler relatert til Internettkriminalitet og jurisdiksjon. Lovgivere i Storbritannia har kommet inn på en mer moderne forståelse ved fornying av hvordan jurisdiksjon skal forstås, ved at de nå tar utgangspunkt i at handlingen må ha skjedd på territoriet eller deler av handlingen var gjennomført på territoriet, men rettspraksis har ikke fulgt juridisk teori til punkt og prikke når det gjelder dette. Videre bestemmes jurisdiksjon ut ifra om den skyldige eller offeret befinner seg på britisk territorium, eller at handlingen eller skaden av handlingen hadde innvirkning på britisk territorium – handlingen må ha en tilknytning til britisk territorium.Lovgivere har tatt steget nærmere mot en harmonisering med Datakrimkonvensjonen, men at det fortsatt gjenstår mye for at kravene i konvensjonen skal kunne oppfylles.

Tysk straffelovgivning følger som en hovedregel en mer snever tilnærming til jurisdiksjon ved tilfeller av Internettkriminalitet, og bygger sin jurisdiksjon på territorialprinsippet, det aktive personalprinsipp og beskyttelsesprinsippet. Tysk straffelovgivning skiller seg fra norsk straffelovgivning da tysk straffelov har lovfestet offerprinsippet som en hovedregel, og ikke en unntaksregel som Norge har gjort i Straffeloven §5 femte ledd. Tilnærmingen til jurisdiksjon er derimot veldig vid i enkelte alvorlige situasjoner (som ved hatefulle ytringer, Holocaustfornektelse og spredning av barnepornografi og overgrepsmateriale), eksempel er Toben-saken. I situasjoner som dette gripes det ofte inn selv om tysk straffelov ikke tradisjonelt sett har jurisdiksjon. Grunnen til at tysk straffelov anvendes vidt i slike typetilfeller er at disse handlingene anses som «abstract endangerment offenses», altså tilfeller/handlinger som kan sette tyske borgere eller Tyskland som nasjon i fare. Tysk

[100] Inger Marie Sunde, *Datakriminalitet: En fremstilling av strafferettslige regler om datakriminalitet*, side 51

straffelovgivning følger de fleste bestemmelsene gitt i Datakrimkonvensjonen med hensyn til materiell straffelov, og trenger derfor kun noen få endringer for å være oppdatert og i tråd med Datakrimkonvensjonen. Tysk straffelovgivning er den som kanskje er mest i samsvar, og harmonisert, med Datakrimkonvensjonen.

I USA har det oppstått litt flere spørsmål rundt jurisdiksjon enn sammenliknet med Norge, Tyskland og Storbritannia, da alle de 50 statene i USA har en selvstendig jurisdiksjon og er avhengig av å måtte samarbeide mellom hverandre i enkelte tilfeller av Internettkriminalitet. USA har for det meste tatt en bred tilnærming til å bygge sin jurisdiksjon i føderale saker som har internasjonale forbindelser. Endringene i U.S. Patriot Act i 2001 forsikret at USA har myndighet til å forfølge også i internasjonale tilfeller der hvor nettverk eller datamaskiner i USA bare brukes som en Proxy server. USA forfølger kriminelle internasjonalt gjennom utlevering eller undercover stings. Ivanov-Gorshkov og Zezev-saken illustrerer at USA er et av de landene som opererer med den videste tilnærmingen til jurisdiksjon, og at de i enkelte tilfeller ikke følger folkerettens regler om innhenting av bevis på en annen nasjons territorium.

4.2 Sluttord: Veien videre for Internettkriminalitet og jurisdiksjon

Hvor bør veien gå videre for Norge og den norske straffeloven når det gjelder jurisdiksjon ved tilfeller av Internettkriminalitet? Høyesterett uttalte i Rt. 2004 s. 1619 at det ville være hensiktsmessig med lovregler som er spesielt utformet med tanke på datarelaterte overtredelser, altså en straffelov mer likt den tyske straffeloven.

Ved tiltredelsen av den nye straffeloven av 2005 ble det i kapittel 21 inkludert mer spesifikke straffebud som direkte regulerer datakriminalitet. Men når det gjelder jurisdiksjonsbestemmelsene har disse forblitt mer generelt utformet for å passe til flere typetilfeller, med unntak av straffeloven §5 første ledd nr. 9-11 som angir spesifikke straffebud der hvor det tillates å anvende en utvidet jurisdiksjon. For å ta hensyn til videre utvikling må enkelte straffebud utformes mer generelle enn andre. Legalitetsprinsippet setter derimot grenser for hvor generelt straffebud kan utformes. Dersom generaliserings- eller abstraksjonsnivået blir for høyt, fratas straffebudene også noe av de pedagogiske og opplysende funksjoner.[101] Den beste løsningen for Norge i den kommende tiden vil nok være å fortsette med harmoniseringen opp mot Datakrimkonvensjonen, og å jevnlig oppdatere straffelovgivningen for å passe på at den følger med den teknologiske utviklingen og å

[101] NOU 2007:2 s.43

fortsette samarbeid med andre nasjoner. Ellers fremstår straffebestemmelsene i §§4-7, med tilhørende forarbeider, som tilstrekkelig til å kunne regulere de fleste tilfeller av Internettkriminalitet.

Så lenge Internettkriminalitet, og datakriminalitet generelt, blir behandlet som en til tider grenseløs form for kriminalitet vil det alltids være spørsmål rundt jurisdiksjon og hvilket lands straffelov som kan anvendes. Selv om lovgivning når det gjelder datakriminalitet og Internett i stor grad har blitt utarbeidet i de enkelte land, har det i senere tid kommet flere internasjonale traktater, for eksempel Datakrimkonvensjonen, som til en viss grad stiller opp et minstekrav til regulering av datakriminalitet. Flere land har valgt å inkorporere eller harmonisere sin straffelovgivning opp mot bestemmelsene i Datakrimkonvensjonen, og gjennom slike inkorporeringer og harmoniseringer vil risikoen for etablering av jurisdiksjoner med manglende tilsvarende standard reduseres, og konvensjonen fører til en styrking av det internasjonale samarbeidet og harmoniseringen av straffebestemmelsene. Den beste løsningen for å bekjempe Internettkriminalitet vil nok være et felles internasjonalt regelverk som er gjeldende for medlemsland, som sikrer både en kriminalisering av Internettkriminalitet og muligheten for å faktisk gjennomføre straffeforfølgning. Et slikt felles regelverk vil være avgjørende dersom man skal greie å bekjempe trusselen som Internettkriminalitet representerer overfor det moderne samfunn.[102]

5. Litteraturliste

5.1 Lovverk

5.1.1 Norske lover

- Kongeriket Norges Grunnlov LOV-1814-05-17
- Lov om straff (straffeloven) LOV-2005-05-20-28
- Åndsverkloven 12.mai 1961 nr. 2

5.1.2 Internasjonale konvensjoner

- Wien-konvensjonen om traktatretten 23.mai 1969
- Datakrimkonvensjonen (Budapest Convention on Cybercrime) ETS 185

[102] NOU 2002:7 punkt 8.8

5.1.3 Lovverk Storbritannia

- Computer Misuse Act 1990
- Criminal Justice Act 1993
- Convention on Mutual Assistance in Criminal Matters 2000
- Sexual Offences Act 2003
- Budapest Convention on Cybercrime

5.1.4 Lovverk Tyskland

- Strafgesetzbuch 1986 [Criminal Code] (StGB)
- Budapest Convention on Cybercrime

5.1.5 Lovverk USA

- Computer Fraud and Abuse Act of 1986 (amendment 2001) [CFAA]
- The Electronic Communications Privacy Act (ECPA)
- U.S.A Patriot Act
- Budapest Convention on Cybercrime

5.2 Forarbeider

- NOU 1985:31 Datakriminalitet
- NOU 2003: 27
- NOU 2007:2 Lovtiltak mot datakriminalitet
- NOU 2009:15
- Ot.prp. nr. 22 (2008-2009)
- Ot.prp. nr. 90 (2003-2004)
- Innst. O. nr. 72 (2004-2005)

5.3 Rettspraksis

5.3.1 Norsk rettspraksis

- Rt. 2004 s. 1619
- Rt. 2003 s. 1770
- RG 2001 s. 219
- Rt. 1996 s. 654

5.3.2 Rettspraksis Storbritannia

- R v. Governor of Brixton Prison and another, ex parte Levin (1996)
- R v. Gold, Schifreen (1988, 2 All ER 186)

5.3.3 Rettspraksis Tyskland

- Toben-saken Dom 12. desember 2000 – 1 StR 184/00, BGHSt 46, 212)

5.3.4 Rettspraksis USA

- United States v. Ivanov (2001)
- United States v. Gorshkov (2001)
- United States v. Zezev (2003)
- Ashcroft v. Free Speech Coalition (2002)

5.4 Litteratur

- Inger Marie Sunde, *Datakriminalitet: En fremstilling av strafferettslige regler om datakriminalitet*, Fagbokforlaget Vigmostad & Bjørke AS (2016)
- Stein Schjølberg, *Cybercrime: Straffbare handlinger mot den alminnelige orden og fred i cyberspace*, cybercrimelaw.net (2006)
- Petter Gottschalk, *Datakriminalitet i Norge*, Unipub (2011)
- Kriangsak Kittichaisaree, *Public International Law of Cyberspace*, Springer (2017)
- Bert-Jaap Koops, Susan W. Brenner, *Cybercrime and Jurisdiction*, Asser Press (2006)
- David S. Wall, *Cyberspace Crime*, Ashgate Publishing Company (2003)
- Morten Ruud, Geir Ulfstein *Innføring i folkerett*. [Oslo]: Tano Aschehoug (1998).
- B. Heinrich, *The Location of the Criminal Result in Abstract Endangerment Offenses,* Goltdammer's Archiv für Strafrecht (1999)
- E. Hilgendorf, *Thoughts on the Interpretation of the Ubiquity Principle of Criminal Law in the Age og The Internet*, Neue Juristiche Wochenschrift (1997)

5.5 Artikler

- Jo Stigen, «Lokalisering av straffbare handlinger», Tidsskrift for strafferett nr. 2 2011 s. 141-190. (TFST-2011-141).

- Johnson and Post; *Law and borders – The rise of Law in Cyberspace*, Stanford Law Review, volum 48 nr.5 (1996)
- Council of Europe; Project on Cybercrime 8185 ETS www.coe.int/cybercrime (2010)
- Mørketallsundersøkelsen 2016

5.6 Referanser på Internett

- https://www.politiet.no/rad/datakriminalitet/
- https://en.wikipedia.org/wiki/Cybercrime
- https://snl.no/datakriminalitet
- https://www.nsr-org.no/moerketall/
- https://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/
- https://en.wikipedia.org/wiki/Convention_on_Cybercrime
- https://www.cnet.com/news/senate-ratifies-controversial-cybercrime-treaty/
- https://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/
- https://snl.no/territorialprinsippet_-_folkerett
- https://snl.no/Rettsvesen_i_USA
- https://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/
- www.coe.int/cybercrime
- https://snl.no/territorium
- https://en.wikipedia.org/wiki/Principle_of_Ubiquity
- https://jusleksikon.no/wiki/Rettskildel%C3%A6re
- https://no.wikipedia.org/wiki/Tjenestenektangrep