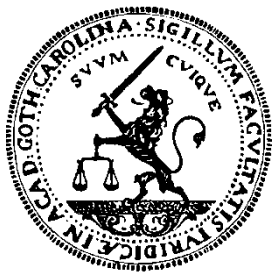

JURIDISKA FAKULTETEN
vid Lunds universitet

Martin Karlsson

Statssuveränitetens inverkan på transnationell insamling av digitala bevis

Om brottsbekämpande myndigheters rätt att tillgodogöra sig material lagrat inom en annan stats territorium

JURM02 Examensarbete

Examensarbete på juristprogrammet
30 högskolepoäng

Handledare: Christoffer Wong

Termin för examen: Period 1 VT2020

Innehåll

Summary

Modern technology has challenged the evidence-gathering function of law enforcement agencies. Digital evidence of relevance to a crime committed in one state can be stored on a server in another state. Furthermore, the geographical location of the evidence can be concealed by the use of anonymity tools. Traditionally, the Lotus principle has prevented agencies from independently collecting such evidence, but the inefficiency of available measures has led to the emergence of alternative solutions that defy international law.

The purpose of this thesis is to clarify whether Swedish law enforcement agencies, in the light of current international developments, have the right to autonomously carry out transnational collection of digital evidence. In addition, the intention is to reach a conclusion as to whether the Swedish legislator should enact legislation that explicitly allows such a procedure. Using the legal dogmatic method, the traditional sources of law have been examined to realize the purpose of the thesis.

Enshrined in an international case from 1927, the Lotus principle prohibits all governmental exercise of authority within the territory of another state. Although the principle still has a pronounced effect on this area of law, it is clear that states increasingly consider it outdated. The autonomous collection of evidence that is accessible to anyone (open source) is always considered permissible under international customary law. With regard to other digital evidence, law enforcement agencies state that acts in violation of the Lotus principle occur regularly in practice. Moreover, a majority of states have departed from the principle by establishing judicial precedents or through legislation.

This thesis concludes that transnational autonomous collection of digital evidence, with the exception of cases involving open source material, is contrary to applicable international law, although new international customary law is under development. However, the requirements placed on uniformity and continuity in state practice cannot be considered fulfilled at present. Some uniformity can be discerned, but the requirements are particularly high due to the importance of the Lotus principle and the sovereignty restricting character of the new state practice. Nevertheless, Sweden should introduce legislation contrary to the Lotus principle. Such legislation would be justified by a substantial positive impact on the effectiveness of law enforcement, by the possibility of exerting influence on the ongoing international legal development and due to empirical evidence not suggesting any negative impact on international relations.

Sammanfattning

Modern teknologi har lett till utmaningar för de brottsbekämpande myndigheternas utredande verksamhet. Digitala bevis av relevans för ett brott begånget i en viss stat kan lagras på en server i en annan stat. Bevisens geografiska position kan också döljas med anonymitetsverktyg. Traditionellt sett har Lotus-principen hindrat myndigheter från att självständigt samla in sådana bevis, men den ineffektivitet som präglat tillgängliga metoder har resulterat i att alternativa lösningar som trotsat folkrätten har trätt fram.

Syftet med arbetet är att, mot bakgrund av den förändring som har skett på ett internationellt plan, klargöra huruvida svenska myndigheter enligt gällande rätt självständigt kan genomföra transnationell insamling av digitala bevis. Därtill är avsikten att ta ställning till huruvida den svenska lagstiftaren bör stifta lag som uttryckligen tillåter att myndigheter självständigt samlar in digitala bevis lagrade i en annan stat. Genom att använda den rättsdogmatiska metoden har de traditionella rättskällorna granskats för att förverkliga uppsatsens ändamål.

Lotus-principen, som stadgats i ett internationellt rättsfall från år 1927, förbjuder all myndighetsutövning på en annan stats territorium. Även om principen alltjämt har en utpräglad inverkan på området står det klart att stater i allt större utsträckning uppfattar den som förlegad. Autonom insamling av bevis som är tillgängliga för alla via en webbläsare (open source) utgör redan internationell sedvanerätt. Vad gäller andra typer av digitala bevis uppger brottsbekämpande myndigheter att de i praktiken regelbundet agerar i strid med Lotus-principen. Därtill har ett flertal stater genom rättsliga avgöranden eller lagstiftning frångått principen.

Uppsatsens slutsats är att autonom insamling av digitala bevis lagrade i en annan stats territorium, med undantag för de fall som rör open source-material, strider mot gällande folkrätt, samtidigt som ny internationell sedvanerätt är under utveckling. De krav som ställs på enhetlighet och kontinuitet i statspraxis kan emellertid inte anses uppfyllda. Även om viss enhetlighet kan skönjas, innebär Lotus-principens centrala roll och det faktum att ny statspraxis inskränker statssuveräniteten att kraven är särskilt högt ställda. Trots att den skulle strida mot gällande folkrätt bör svensk lagstiftning som tillåter autonom insamling av digitala bevis lagrade i en annan stat införas. Sådan lagstiftning motiveras av en markant positiv inverkan på effektiviteten i brottsbekämpningen, möjligheten att utöva inflytande över pågående internationell rättsutveckling och att empirin talar för en utebliven negativ inverkan på internationella relationer.

Förord

Tack till min handledare Christoffer Wong. Du har med goda råd och värdefulla synpunkter lotsat mig genom denna process.

Tack till Abtin för god korrekturläsning och för ett genomgott hjärta.

Tack till alla vänner och kollegor i Repan och på Nätkurs. Ni har förvandlat en i övrigt grå vardag till en brokig affär. Simon K, Simon F, Sofia K och Sofia S – sluta aldrig hålla på som ni gör.

Tack till Joakim och André för all mat och alla samtal. Jocke, du är en komplex man. Där. Jag sade det. André, som du kan se nedan har jag i din ära skrivit en av mina två sammanfattningar på fullt gångbar danska. Weekend. Computer. Back-pocket-logo-embroidery.

Tack till Emma. Du är den roligaste människa som någonsin satt sin fot på denna planet.

Tack till Marija. Allt jag egentligen vill göra är att bara va med dig.

Martin Karlsson
Malmö, den 25 maj 2020

Förkortningar

art.	artikel
BrB	brottsbalken (1962:700)
CIC	Code d'instruction criminelle (Belgien)
CoE	Council of Europe
dir.	direktiv
Ds.	Departementsserien
EKMR	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
EU	Europeiska unionen
EUO	Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området
Europol	The European Union Agency for Law Enforcement Cooperation
FN	Förenta nationerna
FRCP	United States Federal Rules of Criminal Procedure
IDC	International Data Corporation
JB	jordabalken (1970:994)
JK	Justitiekanslern
JO	Justitieombudsmannen
kap.	kapitel
MLA	Mutual Legal Assistance
NIST	National Institute of Standards and Technology
PACE	Police and Criminal Evidence Act 1984 (England och Wales)
PCL	Cybercrime Law (Portugal)
prop.	proposition
RB	rättegångsbalken (1942:740)
RF	regeringsformen (1974:152)
sec.	section
SOU	Statens offentliga utredningar
StPO	Strafprozeßordnung (Tyskland)
SvJT	Svensk Juristtidning
Tor	The Onion Network

1 Inledning

1.1 Bakgrund

Världen har under de senaste decennierna i allt större utsträckning kommit att påverkas av teknologins ständigt ökande betydelse. ITU (International Telecommunication Union) uppskattade att cirka 4 miljarder människor hade tillgång till en internetuppkoppling vid 2019 års slut.[1] Kriminalitet utgör inte ett undantag från denna utveckling, utan har förändrats från att vara bunden till en analog värld till att allt oftare innehålla digitala inslag. Enligt Europol innefattar exempelvis majoriteten av de utredningar som berör internationell organiserad brottslighet digitala utredningsåtgärder.[2] För att kunna utreda och beivra brott på ett effektivt sätt måste brottsbekämpande myndigheter ha möjlighet att samla in bevismaterial.[3]

Chattkonversationer, foton lagrade på mobiltelefoner eller videofilmer som kan styrka ett händelseförlopp kräver att brottsbekämpande myndigheter kan bereda sig åtkomst till digitalt lagrat material. Sådant kan finnas tillgängligt på en server i utlandet, på en server vars position till följd av anonymitetstjänster inte kan identifieras eller i en molntjänst vars karaktär innebär att materialet kan finnas uppdelat på flera ställen samtidigt.[4] En folkrättslig grundpelare – statssuveräniteten – ställer här till med problem för de brottsbekämpande myndigheterna. Det är inte tillåtet att kränka suveräniteten tillhörande en annan stat.[5] Med det följer att myndighetsutövning inte får företas på en annan stats territorium om det inte föreligger samtycke från den motstående staten.[6] Eftersom transnationell bevisinsamling utan samtycke betraktas som myndighetsutövning på annan stats territorium utgör förfarandet en suveränitetskränkning.[7] Enligt detta synsätt blir materialets geografiska position avgörande – oavsett övriga omständigheter. [8] Rättslig hjälp har historiskt sett varit det tillvägagångssätt som myndigheter nyttjat för att tillgo-

[1] ITU (2019) under ”Elektroniska källor”.
[2] UNODC (2013), s. 45
[3] Begreppen ”samla in” och ”insamling” genomsyrar uppsatsen och används för att beskriva förfarandet när brottsbekämpande myndigheter använder tvångsmedel för att efterforska och omhänderta digital bevisning.
[4] Çalışkan m.fl. (2015), s. 7 ff.; Taylor m.fl. (2011), s. 7.
[5] Linderfalk (2012), s. 49.
[6] Helenius (2014), s. 207; Begreppet “motstående stat” kommer genomgående användas för att beskriva den främmande stat inom vilkens territorium det digitala beviset är lagrat.
[7] Oppenheim (1992), s. 384 f.
[8] de Hert (2006), s. 72.

dogöra sig sådant material på ett legalt sätt. Med denna metod anmodas motstående stat att ta över ansvaret för att samla in det digitala material som finns inom dess territorium för att sedermera skicka det till den anmodande staten.

För att komma runt de ineffektivitetsproblem som präglar rättslig hjälp har stater fokuserat på att hitta alternativa tillvägagångssätt. Det rör sig om multilaterala avtal, kreativa tolkningar av anknytningspunkter för exekutiv jurisdiktion i nationell praxis och utmanande nationell lagstiftning. I Sverige har det emellertid hänt väldigt lite på området. Det förekommer ingen relevant lagstiftning och frågan har inte hanterats i domstol. År 2017 genomfördes en statlig utredning som kom fram till att ett nytt förhållningssätt krävdes och att det borde utvecklas genom rättspraxis.[9] Per maj 2020 hade riksdagen fortfarande inte tagit ställning till de förslag som presenterats.

1.2 Syfte och frågeställningar

Syftet med uppsatsen är att klargöra rättsläget avseende exekutiv jurisdiktion vid transnationell insamling av digitala bevis. I dagsläget svävar svenska myndigheter i ovisshet kring huruvida de har rätt att autonomt[10] samla in digitala bevis lagrade i en motstående stat. Avsikten är att redogöra för och problematisera de verktyg som finns tillgängliga för myndigheter i behov av åtkomst till den aktuella typen av bevis. Det finns också skäl att återge ett antal folkrättsligt utmanande lösningar som andra länder har vidtagit för att hantera problemet. Det är av betydelse för att i vägledande syfte kunna illustrera modeller som har prövats och om de har gett upphov till internationella konflikter. En sammanställning kan också belysa de skiljaktigheter som observerats hos olika stater. Att uppmärksamma den bristande enhetligheten i förfarandet kan potentiellt leda till krafttag för att i större utsträckning nå ett gemensamt förhållningssätt.

Ett ytterligare mål är att ge den svenska lagstiftaren en fingervisning om huruvida det finns skäl att införa lagstiftning som tydligt klargör vad brottsbekämpande myndigheter får göra. Det här är av vikt mot bakgrund av den statliga utredning som föreslog att förändring bör ske genom praxis och att det finns motstående intressen vars tyngd kan vara svårbedömda utan en utförlig utredning.

[9] SOU 2017:100, s. 375.
[10] Begreppet ”autonomt” är återkommande och beskriver den situation då brottsbekämpande myndigheter samlar in digitalt bevis lagrat inom en annan stats territorium utan denna stats samtycke.

För att uppnå det beskrivna syftet har följande frågeställningar besvarats:

1. Har svenska brottsbekämpande myndigheter enligt gällande rätt möjlighet att autonomt samla in digitala bevis lagrade inom en annan stats territorium?
2. Vad gäller när bevisets geografiska position inte kan bestämmas?
3. Finns det skäl för Sverige att lagstifta om en sådan rätt mot bakgrund av effektivitetshänsyn och respekten för folkrättsliga förpliktelser?

1.3 Avgränsningar

Utöver de avgränsningar som följer av frågeställningarnas utformning följer ytterligare ett antal som särskilt bör nämnas nedan.

Vid insamling av bevismaterial i digitala miljöer används främst bestämmelserna om beslag och husrannsakan i RB. Även vid en internationell överblick framstår nyttjandet av dessa tvångsmedel som det primära tillvägagångssättet. Det är ett av skälen till varför hemliga tvångsmedel, som exempelvis brottsbekämpande myndighets rätt att enligt inhämtningslagen (2012:278) i hemlighet ta del av elektronisk kommunikation, inte kommer uppmärksammas. Ett annat är att den jurisdiktionsmässiga problematik som uppsatsen hanterar förblir opåverkad av att tvångsmedlet är hemligt.

Den fråga som ofta diskuteras vid bruk av hemliga tvångsmedel är den om den enskildes integritet. Utredningen som har gjorts har kretsat kring den folkrättsliga aspekten av digital bevisinsamling ur ett effektivitetsperspektiv.[11] Av den anledningen läggs ingen större vikt vid frågor om integritet. Det beror inte på att integritetsfrågor betraktas som oviktiga. Min uppfattning är att dessa frågor är viktiga nog att hanteras i en separat uppsats. Med det sagt är inte alla resonemang om integritet uteslutna. Effektivitet och integritet är inte ömsesidigt uteslutande och en förutsättning för bevarandet av varje enskilds integritet är att brott beivras.

Uppsatsens frågeställningar avser själva insamlingen av bevis. Andra aspekter, såsom möjligheten att presentera bevis inför rätten, har därför inte utretts. Detta beror på att principen om fri bevisföring gäller i Sverige och att det transnationella moment som utreds inte nödvändigtvis är en avgörande faktor i sammanhanget.

[11] Se avsnitt 1.4

Den lagstiftning och de rättsfall som lyfts fram är alla hämtade från Europa eller USA. Det beror delvis på att den bearbetade informationen har funnits tillgänglig på engelska, delvis på att en gränsdragning måste göras någonstans med beaktande av uppsatsens omfång. Syftet med redovisningen är till stor del att visa på existerande skiljaktigheter i sättet att hantera det juridiska problemet och således är en större kvantitet av rättsfall inte nödvändig.

1.4 Metod

För att besvara de frågeställningar som ställts upp har jag använt den rättsdogmatiska metoden. Enligt mig är den särskilt lämplig med hänsyn till hur frågeställningarna har utformats. Hur metoden ska tolkas tycks dock inte vara helt klarlagt. Jag tänker därför redogöra för hur jag har använt mig av den och vad den innebär för denna uppsats.

Den snäva traditionella tolkningen av rättsdogmatisk metod innebär att man, genom att objektivt granska de allmänt vedertagna rättskällorna, hittar svaret på ett rättsligt problem eller på hur en viss rättsregel ska tolkas i en viss kontext.[12] Genom att studera den lagstiftning, rättspraxis, lagförarbeten och juridisk doktrin som finns tillgänglig på ett visst område efterforskas svaret på ett konkret formulerat juridiskt problem.[13] Vilken rättskälla som tillmäts störst vikt följer inom svensk rätt av rättskälleläran som stadgar en inbördes hierarkisk ordning. Typiskt sett bär lagstiftning högst dignitet, följt av rättspraxis, lagförarbeten och slutligen doktrin. En stor del av uppsatsen kretsar kring internationell rätt och således har internationella rättskällor också granskats. Även här förekommer en hierarkisk ordning som återges i inledningen av arbetets fjärde kapitel. Enligt art. 38(1) i Internationella domstolens stadga består de traditionella rättskällorna av internationella konventioner, internationell sedvanerätt samt allmänna principer och rättsgrundsatser. Därtill kommer rättspraxis och folkrättslig doktrin. Eftersom de två inledande frågeställningarna tar sikte på att klargöra vad gällande rätt tillåter har relevanta rättskällor studerats och återgivits utan närmare ställningstagande till hur saker och ting bör vara. Istället drar jag, efter bästa förmåga, logiska slutsatser om vad gällande rätt innebär baserat på de rättskällor som granskats.

För att besvara uppsatsens tredje frågeställning kan en sådan snäv tolkning inte anses tillräcklig. Frågan är formulerad på ett sätt som förutsätter ett ställningstagande om hur gällande rätt bör vara. Enligt Lambertz kan ett utredningsarbete utföras med en konstruktiv rättsdogmatik de lege ferenda. Här

[12] Sandgren (2018), s. 49.
[13] Kleineman (2018), s. 21 ff.

avses en analytisk och konstruktiv granskning av ett regelsystem som resulterar i väl avvägda rekommendationer om hur regelsystemet bör ändras.[14] Även Jareborg anser att den rättsdogmatiska metoden kan innefatta en analys av rättskällorna i syfte att problematisera och dra en slutsats om hur rätten bör vara.[15] Genom att granska och sammanställa information från relevanta rättskällor har problem och motstående intressen framträtt. I femte kapitlets tredje avsnitt har dessa analyserats, vägts mot varandra och utmynnat i ett ställningstagande.

Det ska också poängteras att uppsatsen utgår från ett effektivitetsperspektiv. Med det avses inte att alla medel för effektivisering av brottsbekämpning har hanterats okritiskt. Jag har dock i regel fokuserat på myndigheternas önskan om en effektivisering av regelverket för att kunna tackla den teknologiska utvecklingen. För att exemplifiera redogör jag endast för remissyttranden avseende Beslagsutredningen som upprättats av instanser inriktade på brottsbekämpning. Genomgången av det material som legat till grund för mina slutsatser har varit präglad av ett intresse för hur stater har effektiviserat sina rättssystem genom lagstiftning och praxis. Samma utgångspunkt har påverkat granskningen av internationella överenskommelser. Målet har varit att i någon mån konstatera vad som är folkrättsligt acceptabelt samt hur Sverige bör förhålla sig till detta. Andra perspektiv kan således hamna i skymundan. Som framgår ovan har begränsat utrymme exempelvis tillägnats frågor om den enskildes integritet.[16]

1.5 Material

I syfte att ge läsaren en kort introduktion till den teknologi som ligger till grund för problematiken som avhandlas har jag, i kapitel två, studerat hur digitalt material lagras och varför det kan vara svårt att utreda var det finns. Presentationen är i stort baserad på litteratur från Stephen Mason, vars verk möjliggör att en lekman får inblick i relevanta funktioner. Hans bakgrund som barrister bidrar till att juridiska kopplingar kan göras. Viss information, särskilt avseende teknik som tillåter anonymitet online, har hämtats ur artiklar publicerade i teknologiska tidskrifter eller tidningar såsom Network Security.

Relevanta rättskällor som stadgar svenska brottsbekämpande myndigheters möjligheter att vidta relevanta tvångsåtgärder presenteras under kapitel tre. Här har Gunnel Lindbergs monografi om de straffprocessuella tvångsmedlen och Peter Fitgers kommentar till rättegångsbalken varit särskilt vägledande i att klargöra hur de traditionella reglerna om tvångsmedel kan appliceras på

[14] Lambertz (2002), s. 263 ff.
[15] Jareborg (2004), s. 8.
[16] Se avsnitt 1.4.

IT-miljöer. Även Kronqvist verk om digitala bevis och Åklagarmyndighetens handbok har bidragit till att belysa de svårigheter som teknologin för med sig i detta hänseende.

Det internationella rättsläget utreds i kapitel fyra. Ulf Linderfalk och Anders Henriksens verk har här varit centrala för förståelsen av de folkrättsliga ramar som stater har att förhålla sig till. Anna-Maria Osulas avhandling har fungerat som en språngbräda i jakten på material som särskilt berör uppsatsens frågeställningar. Den har också bidragit till värdefulla insikter om hur problemet kan kategoriseras. Särskilt nyttigt har varit att läsa CoE:s och FN:s rapporter för att utforska staters inställning till det aktuella problemet. Härigenom har en bild också skapats av hur brottsbekämpande myndigheter ur ett internationellt perspektiv arbetar i praktiken. Nationell lagstiftning och rättsfall har valts ut särskilt för att belysa vilka alternativa metoder som tillämpats internationellt och för att demonstrera den bristande enhetlighet som råder. Fokus har riktats mot stater med ett stort internationellt inflytande eller rättssystem som har infört, ur ett folkrättsligt perspektiv, särskilt utmanande lagstiftning. För att hitta rättsfall och lagstiftning som passar kriterierna har akademiska förlags sökmotorer, såsom Springer, använts – huvudsakligen tillsammans med sökorden ”digital search and seizure” och ”electronic search and seizure”. Kapitlet innehåller också en redogörelse för hur svensk rätt i allmänhet och myndigheter i synnerhet har förhållit sig till kärnfrågan. Detta har gjorts genom att granska Beslagsutredningen samt relevanta remissyttranden.

1.6 Forskningsläge

Anna-Maria Osula har i sin avhandling behandlat frågan om huruvida det är förenligt med folkrätten att en brottsbekämpande myndighet autonomt samlar in digitalt bevismaterial lagrat i ett annat land. Avhandlingen är emellertid tre år gammal, vilket på ett område under snabb utveckling är lång tid. Bland annat har fler länder anslutit sig till konventioner och ny nationell lagstiftning samt praxis har tillkommit. Mina efterforskningar har inte heller utvisat något material producerat av svenska skribenter eller med det svenska rättssystemet som infallsvinkel, utöver en av regeringen påkallad utredning från 2017.[17]

Bert-Jaan Koops har skrivit ett flertal artiklar om art. 32 b CoCC och hur konventionsbestämmelsen förhåller sig till aktuell folkrätt. Även de Hert har utvärderat frågan om territorialitet och exekutiv jurisdiktion i IT-miljöer, men nämnda verk gör inte anspråk på att slå fast gällande rätt genom en utförlig genomgång av relevanta rättskällor. Verken tar inte heller hänsyn till det svenska perspektivet.

[17] SOU 2017:100

1.7 Disposition

Uppsatsens andra kapitel introducerar läsaren till den teknologi som ligger till grund för det juridiska problemet. Kapitlet är relativt kortfattat och innehåller förklaringar av vissa återkommande begrepp. Bland annat görs en presentation av verktyg för lagring av digitalt material och av tjänster som anonymiserar materialets geografiska position.

I det tredje kapitlet behandlas tvångsmedel som inom svensk rätt är relevanta för insamling av bevis i allmänhet. En kort presentation av vilka förutsättningar som ska vara uppfyllda för dess tillämplighet följs av en förklaring på hur de förhåller sig till den digitala sfären.

Det fjärde kapitlet är omfattande och centralt för förståelsen av det internationella rättsläget. Initialt presenteras de folkrättsliga källorna med beskrivningar av vad de för med sig. Därefter kartläggs innebörden av exekutiv jurisdiktion och hur den förhåller sig till statssuveränitet samt en djupare problematisering av uppsatsens kärnfråga. I delavsnitt därefter utreds de folkrättsliga verktyg länder har att tillgå för insamling av bevis. Kapitlet innehåller också ett urval av nationell praxis och lagstiftning som visar på kreativa lösningar men bristande enhetlighet. Slutligen studeras beslagsutredningen med relevanta remissyttranden. Kapitlet avser belysa de folkrättsliga problem som har uppstått samt hur de har hanterats internationellt och i Sverige.

Kapitel fem är utformat efter den ordning frågeställningarna har presenterats ovan. Först behandlas frågan om insamling av digitalt bevismaterial när staten där materialet finns lagrat är känd. Nästa delavsnitt tar sikte på den situation då materialets position inte kan bestämmas. Det sista delavsnittet innehåller en diskussion om huruvida det finns skäl att lagstifta om frågan i svensk rätt.

Resultaten sammanfattas slutligen i kapitel sex. Här beskrivs kortfattat vad som har utkristalliserats i uppsatsens femte kapitel för att koncist runda av arbetet.

För att skapa tydlighet, stringens och lättöverskådlighet förekommer korta sammankopplande beskrivningar i inledningen av vissa avsnitt. Det här gäller framför allt avsnitt vars placering vid en första anblick inte nödvändigtvis förefaller uppenbar, men där jag efter reflektion har kommit fram till att de bör placeras.

2 Lagring av digitala bevis

2.1 Kortfattat om digitala bevis

Uppsatsen kärnfråga berör brottsbekämpande myndigheters exekutiva jurisdiktion när digitalt lagrat bevismaterial samlas in transnationellt.[18] För att förstå innebörden av problemet krävs en viss kunskap om teknologin som behandlas.

Digitalt lagrade bevis kan bestå av vilken information som helst som kan förvaras i ett datorsystem och som kan vara av betydelse för en utredning.[19] Det kan exempelvis röra sig om loggar över när en person har loggat in i ett program, laddat ner information eller kopplat upp mot en server.[20] Andra mer konkreta former av digitala bevis är filer innehållandes bilder, videor, textdokument eller statiskföring.[21] Det finns flera olika metoder för brottsbekämpande myndigheter att samla in sådan information. De kan exempelvis använda sig av metadata som tillåter en effektiv genomsökning av stora datorsystem eller mjukvara som möjliggör att raderad information restaureras om den inte i sin helhet förstörts.[22]

2.2 Server och serverleverantörer

Svenska brottsbekämpande myndigheter är verksamma inom landets gränser och därför är den exekutiva jurisdiktionen inte ett problem när digitala bevis finns tillgängliga via ett datorsystems lokala lagringshårdvara om den finns i Sverige. Det aktuella juridiska problemet tar emellertid sikte på en annan situation. Brottsbekämpande myndigheter kan via ett datorsystem i Sverige upptäcka digitalt lagrat material som ur bevishänsyn är intressant, men som finns beläget på en server i ett annat land. Vad en dator är och hur den vanligtvis används måste anses vedertaget, däremot är de tekniska detaljer som tillåter extern lagring av digitalt material inte självklara. Därför ges nedan en kortfattad beskrivning av vad en server är och hur det digitala materialets geografiska position kan vara bundet av serverns. I efterföljande avsnitt följer en presentation av hur digitalt material kan lagras i ”molntjänster” och via det

[18] Se avsnitt 4.2.2.
[19] Mason (2012), s. 13; Begreppet “datorsystem” kommer att användas för att beskriva den hårdvara, såsom stationära datorer, bärbara datorer, surfplattor och mobiltelefoner, som tillgängliggör det digitala beviset.
[20] Mason (2012), s. 12 f.
[21] Ibid, s. 12.
[22] Ibid., s. 14 f.

så kallade Tor-nätverket. Verktygens funktioner, som får anses än mindre vedertagna, gör att digitalt material svårligen kan lokaliseras. Detta ställer till särskilda problem för myndigheter som har att förhålla sig till den folkrättsliga synen på exekutiv jurisdiktion.

Datorsystem består av en rad olika hårdvarukomponenter som sträcker sig från chassi och fläkt till processor och moderkort. Det som är av huvudintresse vid utredningar av brott är vanligtvis inte hårdvaran i sig utan det material som kan finnas tillgängligt däri.[23] Det finns flera olika sorters komponenter som möjliggör lagring. Det kan vara ”random access memory” (RAM), ”hard disk drives” (HDDs) eller ”universal serial bus” (USB). Varianterna finns tillgängliga antingen i form av integrerad hårdvara, inbyggda i datorsystemet, eller som extern hårdvara som snabbt kan kopplas in och ut ur datorsystemet.[24]

En server beskrivs ofta som en mycket kraftfull dator vars syfte är att förse ett system, via lokala nätverk eller internet, med data. Utöver de fysiska komponenterna krävs någon form av mjukvara som är anpassad till serverns specifika ändamål.[25] Hur kraftfull datorn är kan emellertid inte anses avgörande för dess förutsättningar att verka som server. Avancerade processorer och hög lagringskapacitet bidrar till effektivitet, men nästintill alla datorer kan fungera som server för den information som finns lagrad på den. En mängd olika användningsområden för servrar existerar. Ett företag kan exempelvis placera basen för sin interna webbplatform eller för sin mailtjänst på en server. Dessa varianter är ofta slutna och kräver lösenord för åtkomst, men det finns också webbservrar vars innehåll är åtkomligt för alla som har en internetuppkoppling.[26] Det finns även företag, exempelvis Google, Yahoo! och Apple, som sysslar med att leverera serverutrymme till sina kunder. När en dator inte har tillräckligt lagringsutrymme, när användaren vill ha en platsoberoende åtkomst till sitt material eller när säkerhetskopior behövs passar tjänsten särskilt bra. Ofta innefattas också att företaget underhåller servern genom att lösa tekniska problem som kan uppstå.[27]

Varje datorsystem, inklusive serverdatorer, får vid uppkoppling till internet en särskild adress benämnd ”internet protocol” (IP). IP-adressen är ett tolv siffror långt nummer, unikt för det specifika datorsystemet, och utgör därför en form av digital identifikation.[28] När ett datorsystem kopplar upp mot ett

[23] Kronqvist (2013), s. 19 f.
[24] Mason (2012), s. 2 ff.
[25] Ibid., s. 16.
[26] Ibid., s. 17 f.
[27] IDC (2019) under “Elektroniska källor”; Mike Williams, Brian Turner (2020) under “Elektroniska källor”.
[28] Kronqvist (2013), s. 72.

nätverk eller ansluter till en webbsida lokaliserad på en server registreras datorsystemets IP-adress.[29] Det finns flera olika sätt att spåra en IP-adress och många metoder har utvecklats av företag, exempelvis Google.[30]

Vid upptäckten av potentialen i riktad marknadsföring skapades incitament att snabbt framställa metoder för efterforskning. Med kunskap om kunders geografiska position kan reklam skräddarsys.[31] En enkel metod är att be användare uppge sin geografiska position. Vanligare och pålitligare är ”IP geolocation” som möjliggör en teknisk spårning till ett ungefärligt område utan användarens samtycke. IP-adressen som sådan anger inte användarens personliga identitet men ofta kan den fastställas med hjälp av annan information som finns tillgänglig via serverleverantörers loggar – exempelvis meddelanden eller självangivna uppgifter.[32] IP-adresser kan visserligen vara föränderliga och en adress inte alltid är kopplad till samma datorsystem, men det finns olika spårningsmetoder för att ta sig runt detta problem.[33] Sammanfattningsvis kan en IP-adress påvisa en ungefärlig geografisk position. Den kan däremot inte ensamt ge klarhet i vem den faktiska användaren är.

2.3 Tjänster som försvårar lokalisering

2.3.1 Molntjänster

Ett alternativ till förvaring av material på enskilda fysiska servrar som tillhandahålls av särskilda serverleverantörer är molntjänster. På senare år har tekniken växt sig populär bland annat eftersom den erbjuder användaren betydande flexibilitet.[34] En av fördelarna är att användaren inte manuellt behöver flytta sitt material för det fall mer eller mindre utrymme behövs. Molntjänsten tillåter en nästan omedelbar ökning eller minskning av lagringsutrymme.[35] Ett exempel på molntjänst är Googles mailtjänst som tillåter användaren att genom sin webbläsare interagera med mailkorgen utan att dess innehåll sparas ner på användarens datorsystem. Istället fungerar Googles moln som lagringsutrymme.[36] Ofta används en definition framtagen av NIST. Enligt denna är molntjänster ”en modell för att vid behov (on-demand) möjliggöra allmänt tillgänglig och behändig nätverksaccess till en delad och gemensam mängd

[29] Kaechele (2019), s. 66.
[30] Burnett (2013), s. 466 f.
[31] Ibid., s. 465.
[32] Ibid., s. 467.
[33] Kaechele (2019), s. 68.
[34] Sehgal m.fl. (2020), s. 1.
[35] Ibid., s. 4 f.
[36] Ibid., s. 3.

av konfigurerbara datorresurser (exempelvis nätverk, servrar, datalagring, datorprogram och tjänster) som snabbt kan göras tillgängliga och frigöras med minimal insats och utan direkt interaktion med molntjänstleverantörer".[37]

Den första komponenten i en molntjänst är den mjukvara som tillåter en användare att interagera med tjänsten. Det är vanligtvis en applikation, exempelvis Google Drive, som finns tillgänglig oavsett om användaren brukar en mobiltelefon, surfplatta eller dator. Vanligt är också att tillgänglighet finns via webbläsare.[38] Utöver mjukvaran tillkommer en plattform på vilken användaren kan överföra andra applikationer, filer eller program som operativsystemet stödjer. Användaren styr och konfigurerar innehållet men leverantören av molntjänsten ansvarar för att underhålla operativsystemet.[39] Slutligen ställs den infrastruktur på vilken tjänsten är uppbyggd till användarens förfogande. Även fysiska servrar tillhandahålls och användaren behöver inte engagera sig i frågor om säkerhet eller underhåll.[40] Molntjänsten skiljer sig från den traditionella servertjänsten genom att "molnet" förser användaren med ett nät av applikationer och program. Nätet gör att den fysiska positionen för det material som finns tillgängligt via molntjänsten med svårhet kan bestämmas. Ofta kan materialet finnas utspritt på flera applikationer och program, vilka i sin tur kan finnas lagrade på en mängd servrar i olika länder.[41]

2.3.2 Tor-nätverket

Tor är en akronym för "The Onion Network" – ett nätverk som tillåter åtkomst till vad som kallas darkweb. Namnet anspelar på programvarans mångalgrade karaktär vars funktion tillåter nätverksanvändare att komma åt webbsidor som inte kan nås via vanliga sökmotorer såsom Google eller Bing.[42] Syftet med att begränsa åtkomsten till användandet av en särskild mjukvara är att anonymisera användarens geografiska position för att i förlängningen göra det svårt att efterforska dennes identitet. I den globala diskursen finns delade meningar om Tor som verktyg. Å ena sidan finns de som anser att verktyget möjliggör åsikts- och yttrandefrihet för människor som kanske inte annars hade kunnat tillgodogöra sig sådana rättigheter.[43] Å andra sidan har det uppmärksammats att Tor gör det svårt för brottsbekämpande myndigheter att utreda och stoppa brottslighet.[44] Det finns indikationer på att organiserad brottslighet på senare

[37] Edvardsson & Frydlinger (2013) s. 22.
[38] Faynberg m.fl. (2016), s. 4.
[39] Sehgal m.fl. (2020), s. 2; Faynberg m.fl. (2016), s. 4.
[40] Faynberg (2016), s. 4–5.
[41] Taylor m.fl. (2011), s. 7.
[42] Dingledine m.fl. (2004), s. 1–2; Çalışkan m.fl. (2015), s. 5 f.
[43] Çalışkan m.fl. (2015), s. 24 f.
[44] McGoogan (2016) under "Elektroniska källor".

år har upptäckt fördelarna med Tor – flera exempel på anonym näthandel med droger har uppmärksammats bara i Sverige.[45]

För att förstå hur Tor fungerar kan läsaren, som namnet antyder, föreställa sig en lök. När det yttersta lagret skalas bort nås nästa lager, vilket sker igen och igen till lökens mittpunkt nås. Tor-nätverket skapar en särskild, privat väg för användaren som anonymt vill komma åt en webbsida. Istället för att kopplas direkt till den webbsida som användaren önskar besöka (metoden för gemene internetbrukare), skickar Tor-nätverket användaren mellan olika tillfälliga anhalter (relay-servrar) innan slutdestinationen nås. Kopplingarna som finns mellan de olika anhalterna är krypterade och vid dekryptering av en enskild anhalt framgår endast information om kopplingen till föregående och nästkommande anhalt.[46] För att nå användarens utgångspunkt (datorsystemet) måste kedjan följas från första till sista anhalt. Eftersom varje enskild anhalt måste dekrypteras för att nå nästa punkt är efterforskning svår och ibland omöjlig att genomföra. Resurserna som krävs är direkt beroende av kedjans omfattning och hur avancerad krypteringen är – vilket i sig kan vara svårt att förutspå.[47]

[45] Larsson (2020) under ”Elektroniska källor”.
[46] Dingledine m.fl. (2004), s. 2.
[47] Çalışkan m.fl. (2015), s. 7 ff.

3 Nationell insamling av digitala bevis

3.1 Tvångsmedel i allmänhet

3.1.1 Kortfattat om ramen för tillämplighet

De brottsbekämpande myndigheterna har till uppgift att utreda brott och att se till att lagföra samt verkställa påföljd för personer som har gjort sig skyldiga till brott. För att kunna fullfölja sin uppgift har myndigheterna, huvudsakligen genom 23–28 kap. RB, rätt att vidta straffprocessuella tvångsmedel. Bestämmelserna utgör ett undantag från de grundläggande rättigheter som stadgas i 2 kap. RF.[48] Det framgår bland annat av 2 kap. 6 § RF att var och en är gentemot det allmänna skyddad mot kroppsligt ingrepp, husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse. Ett undantag från denna reglering förutsätter att ett antal kriterier är uppfyllda (mer härom under efterföljande avsnitt). Anledning till att en inskränkning av rättigheterna i 2 kap. RF i vissa fall motiveras beror på att intresset av en effektiv brottsbekämpning i vissa fall väger tyngre än de rättigheter som skyddas.[49] Utan möjligheten att vidta tvångsåtgärder skulle den brottsbekämpande verksamheten väsentligen begränsas.[50] Samtidigt ska undantag från de grundläggande rättigheterna om möjligt undvikas och förefaller ett mildare tillvägagångssätt vara ändamålsenligt får tvångsmedel inte vidtas.[51]

De tvångsmedel som finns att tillgå enligt RB är särskilt avsedda för att brukas inom ramen för en förundersökning.[52] Enligt huvudregeln som följer av 23 kap. 1 § RB ska en förundersökning inledas så snart det på grund av angivelse eller av annat skäl finns anledning att anta att ett brott som hör under allmänt åtal har förövats. Skulle ett beslut om tvångsåtgärd fattas i frånvaro av ett formellt beslut om inledande av förundersökning anses det förstnämnda enligt förarbeten vara likställt med att förundersökningen formellt inleds. Härom förekommer dock motstridiga uppfattningar i doktrin.[53] Eftersom för-

[48] Ekelöf m.fl. (2006), s. 38 f.
[49] Nordh (2007), s. 36.
[50] Ibid., s. 36 f.
[51] Ekelöf m.fl. (2006), s 38.
[52] Lindberg (2018) s. 6
[53] SOU 1995:47, s. 155; jfr Bring m.fl. (2019), s. 238 f. & Lindberg (2012), s. 7.

undersökningen i normalfallet fungerar som en yttre gräns för när tvångsmedel får användas måste en tvångsåtgärd upphöra i samma stund som förundersökningen läggs ned, oberoende av orsaken till detta.[54]

3.1.2 Grundläggande principer

Vid ett beslut om tvångsmedel ska en avvägning göras mellan den enskildes intressen och samhällets behov av en effektiv brottsbekämpande verksamhet. För att vägleda denna avvägning har beslutsfattaren ett antal allmänna principer att ta hänsyn till.[55] En central position har den i grundlag stadgade legalitetsprincipen som har en särskilt framträdande roll i straff- och straffprocessrättsliga sammanhang, men även ändamåls-, behovs-, och proportionalitetsprincipen kommer att redogöras för nedan.[56]

Tvångsmedel får inte vidtas i strid med legalitetsprincipen som stadgar att det måste finnas uttryckligt stöd i lag eller annan författning för ett sådant ingripande.[57] Principen slås fast i regeringsformen, primärt genom 2 kap. 10 § RF, som också stadgar de grundläggande friheter som är särskilt viktiga vid tillämpning av straffprocessuella tvångsmedel, exempelvis 2 kap. 6 § RF och 2 kap. 8 § RF. Sistnämnda bestämmelser innehåller ett skydd mot integritetskränkande ingrepp men de kan i enlighet med 2 kap. 20 § RF begränsas genom lag. Legalitetsprincipen följer även av artikel 5, 6 och 8 EKMR och innebär vidare att straffprocessuella bestämmelser inte får tolkas i strid med ordalydelsen. Med andra ord följer att bestämmelser om tvångsmedel inte ska tillämpas på situationer som faller utom en strikt tolkning av ordalydelsen. För att belysa hur detta påverkar den enskilde kan HD:s resonemang i NJA 1977 s. 403 anföras som ett exempel. I fallet konstaterades att ordalydelsen i bestämmelsen om beslagsförbud, 27 kap. 2 § RB, gav den enskilde ett mer omfattande skydd än vad som hade varit avsikten vid utformandet av regeln. Detta till trots ansåg sig domstolen, med hänvisning till legalitetsprincipen, vara förhindrad att döma i strid med ordalydelsen, eftersom det skulle vara till nackdel för den enskilde.[58] Legalitetsprincipen anses också innefatta ett förbud mot retroaktiv rättstillämpning och ett krav på att lagstiftaren undviker vaga och otydliga rekvisit för att tolkningen av dem inte ska bli för godtycklig.[59]

[54] SOU 1995:47, s. 157.
[55] Lindberg (2018), s. 20; Nordh (2007), s. 37.
[56] Nordh (2007), s. 36.
[57] Ekelöf m.fl. (2006), s. 47.
[58] Lindberg (2018), s. 20 f.
[59] Naarttijärvi (2013), s. 49.

Vidare ska tvångsmedel, i enlighet med ändamålsprincipen, endast användas för att uppnå de syften som framgår av lagstiftningen.[60] Eftersom tvångsmedlen innebär intrång i de friheter som stadgas i 2 kap. RF krävs, enligt 2 kap. 21 § RF med hänvisning till 2 kap. 20 § RF, att de vidtas endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Ytterligare en förutsättning som följer av samma bestämmelse är att begränsningar av rättigheterna aldrig får gå utöver vad som är nödvändigt med hänsyn till de ändamål som har föranlett begränsningsmedlet. För varje enskilt tvångsmedel, med undantag för de hemliga tvångsmedlen, finns ändamålen särskilt angivna som en del av bestämmelsens utformning.[61] Det innebär att myndigheten som fattar beslut om tvångsmedel har en tydlig ram att förhålla sig till, vilket bidrar till en minskad risk att fatta beslut i strid med grundlag.[62] Beslutsfattaren har alltid att göra en bedömning av huruvida den givna situationen tillåter ett beslut om tvångsmedel mot bakgrund av den ram som dess ändamål etablerar. Inte förrän frågan om tvångsmedlets ändamål är avgjord ska en proportionalitets- och behovsbedömning göras.[63]

Behovsprincipen stadgar att tvångsmedel endast får vidtas i situationer då ändamålet inte kan uppnås genom nyttjandet av andra medel som är mindre inskränkande och att det måste finnas ett påtagligt behov av att åtgärden vidtas.[64] En avvägning ska också göras i de fall det står klart att skäl för att vidta tvångsmedel föreligger. Är ett visst tvångsmedel som är mindre inskränkande tillräckligt för att uppnå ändamålet får inte ett mer inskränkande alternativ användas. För att exemplifiera får häktning inte beslutas om ett reseförbud är tillräckligt för att uppnå ändamålet.[65] Ändamålsprincipens krav på lagstadgande om vilka ändamål åtgärderna får vidtas i syfte att uppnå och behovsprincipens förbud mot åtgärd när skonsammare metoder anses tillräckliga bör sannolikt innefatta kravet på ett påtagligt behov. Om ett lagstadgat ändamål är för handen och inget tillvägagångssätt utom tvångsmedel är tillräckligt borde ett påtagligt behov föreligga, varför det uttryckliga angivandet av detta kan anses överflödigt. Det lyfts dock fram i doktrin varför det måste anses lämpligt att belysa även här.[66] För att ge ett exempel på behovsprincipens verkan får den verkställande myndigheten inte fatta beslut om husrannsakan i syfte att omhänderta ett visst föremål om det finns anledning att anta att personen i fråga självmant hade lämnat över objektet vid tillfrågan.[67] Av be-

[60] Nordh (2007), s. 37.
[61] SOU 1984:54, s. 76.
[62] Ekelöf m.fl. (2006), s. 47.
[63] Lindberg (2018), s. 23 f.
[64] Ibid., s. 25; SOU 1984:54 s. 77.
[65] Ekelöf m.fl. (2006), s. 47; Nordh (2007), s. 37.
[66] Lindberg (2018), s. 25.
[67] Lindberg (2018), s. 25 f.

hovsprincipen följer också att tvångsmedlet ska upphöra med omedelbar verkan både för det fall ändamålet har uppnåtts och i situationer då tvångsmedlets finns vara verkningslöst. Det gäller också om situationen förändras så att ett mildare, men tidigare otillräckligt, tvångsmedel blir tillräckligt för att uppfylla ändamålet.[68]

Slutligen ska proportionalitetsprincipen beaktas. Principen innebär att en bedömning av huruvida skälen till och målet med tvångsåtgärden står i proportion till det intrång som medföljer.[69] Det är otvivelaktigt att den till viss del överlappar med behovsprincipen men den särskiljer sig möjligtvis i att den uttrycker att inskränkningen mot den enskilde och eventuella tredje parter i sin helhet är av vikt. Hänsyn ska tas till tvångsmedlets art, räckvidd, varaktighet och kraft. Detta vägs sedan mot intresset av att vidta tvångsåtgärden.[70] Proportionalitetsprincipen finns uttryckligen angiven i 24-28 kap. RB, exempelvis 26 kap. 1 § 2 st. RB och 27 kap. 1 § 3 st. RB, men omfattar enligt förarbetet även tvångsmedel i 23 kap. RB.[71] För att knyta an till den bedömning som följer av behovsprincipen avseende skillnaden i inskränkning som de olika tvångsmedlen ger upphov till kan nämnas att åtgärder avseende egendom anses utgöra mindre intrång än sådana som avser personlig frihet. Vid en proportionalitetsbedömning påkallar en häktning således mer långtgående skäl än beslagtagandet av ett objekt tillhörande den enskilde.[72]

3.2 Husrannsakan

En tvångsåtgärd som inte är ovanlig under förundersökningar är husrannsakan. Det faller sig naturligt att brottsbekämpande myndigheter ofta behöver bereda sig tillträde till bostäder eller andra utrymmen i syfte att utreda förhållanden av intresse för utredningen.[73] Detta gäller även när det som eftersöks är digitalt bevismaterial. Många förvarar sina datorer och andra digitala hjälpmedel i hemmet eller i andra privata utrymmen.[74] Detta utgör skäl för den presentation av tvångsmedlet som följer nedan.

Beslut om husrannsakan fattas av åklagaren och inget godkännandes från rätten fordras. Nordh framhåller att det följer av att åtgärden vanligen vidtas i en tidig eller annars brådskande fas av utredningen. Enligt Westerlund föreligger

[68] Ekelöf m.fl. (2006), s. 48.
[69] Nordh (2007), s. 37.
[70] Lindberg (2018), s. 27 f.
[71] Prop. 1988/89:124, s. 28.
[72] Ekelöf m.fl. (2006), s. 48 f.
[73] Nordh (2007), s. 109.
[74] Kronqvist (2013), s. 107.

ofta ett behov av hastiga beslut för att åtgärden ska kunna vara av betydelse för utredningen.[75]

Tvångsmedlet regleras i 28 kap. RB och får, enligt 28 kap. 1 § RB, endast vidtas förutsatt att det sker i syfte att eftersöka föremål som är underkastat beslag eller för att utröna omständigheter som kan vara av betydelse för ett visst brott. Enligt samma bestämmelse ska beslutet avse hus, rum eller annat slutet förvaringsställe och det ska förekomma anledning att ett brott med fängelse i straffskalan har begåtts. Det innebär att tvångsmedlet inte får vidtas i syfte att förebygga eller upptäcka brottslig verksamhet utan endast med avsikt att beivra brott. Det måste föreligga någon konkret omständighet som ger anledning att anta att brott har begåtts. Sistnämnda krav innebär att en anonym anmälan inte är tillräcklig grund att stå på för beslutsfattaren.[76] Om en person är skäligen misstänkt är kravet uppfyllt och husrannsakan kan genomföras i syfte att uppnå de lagstadgade ändamålen.[77]

När husrannsakan vidtas i miljöer av digital natur är omständigheterna ofta något annorlunda i förhållande till normalfallet.[78] Det finns olika metoder för utredaren i fråga. Antingen kan ett beslag vidtas, eller också kan materialet speglas delvis eller i sin helhet.[79] Det senare innebär att materialet som finns tillgängligt direkt på datorsystemet kopieras. Vid en spegling bevaras materialets ägares åtkomst varför åtgärden av brottsbekämpande myndigheter anses vara mindre ingripande än ett vanligt beslag. Spegling av digitalt material används därför i större utsträckning. Detta synsätt är något kontroversiellt eftersom brottsbekämpande myndigheter i utredningssyfte ofta väljer att spegla materialet i sin helhet. Vid ett sådant förfarande följer allt tillgängligt material med, vilket ofta kan innebära en kränkning av den enskildes integritet.[80] Ett förslag om särskild lagstiftning för kopiering av digitalt material har presenterats i en offentlig utredning.[81] I dagsläget finns emellertid inga bestämmelser i 28 kap. RB som uttryckligen tar sikte på ett datorsystems materiella innehåll och vid en granskning av ordalydelsen är det inte självklart att digitalt material träffas. I doktrin förekommer emellertid uppfattningen att det är underförstått att bestämmelserna får tillämpas på IT-miljöer. Lindberg framhåller att ett datorsystems innehåll får undersökas om den finns i det fysiska utrymme som ett beslut om husrannsakan avser.[82] När det kommer till mobiltelefoner är läget ett annat. De förekommer ofta på andra ställen än de som

[75] Westerlund (2018), s. 173; Nordh (2007)., 109 f.
[76] Fitger m.fl. (2019), kommentaren till 28 kap. 1 § RB; Nordh (2007), s. 109.
[77] Westerlund (2018), s. 172.
[78] Kronqvist (2013), s. 107.
[79] Se avsnitt 3.3.
[80] SOU 2017:100, s. 182 f.
[81] Ibid., s. 149.
[82] Lindberg (2018), s. 621.

anges i 28 kap. 1 § RB och anses, enligt Åklagarmyndigheten, inte vara att betrakta som slutna förvaringsställen. Av den anledning hävdas att inget särskilt beslut om husrannsakan krävs för efterforskning.[83] Det kan observeras att en statlig utredning som föreslog särskild lagreglering för kopiering av digitalt material förhöll sig restriktiv i fråga om särskild reglering av husrannsakan i IT-miljöer.[84]

3.3 Beslag

För att utreda brott på ett effektivt sätt behöver brottsbekämpande myndigheter ha möjlighet att samla in material som tillhör en misstänkte, ett företag eller någon annan person. Sådant material kan under vissa förutsättningar beslagtas enligt 27 kap. RB. Reglerna kring beslag av bevismaterial är den grund brottsbekämpande myndigheter ofta står på för att kunna föra en utredning vidare. Mot bakgrund av att bestämmelserna är väldigt gamla är det inte helt säkert att de omfattar digitalt bevismaterial. Detta till trots tillämpas bestämmelserna, som nedan framgår, på IT-miljöer, varför det finns skäl för den sammanfattande beskrivning som följer.

Det stadgas i 27 kap. 1 § 1 st. RB att föremål som skäligen kan antas ha betydelse för utredning om brott eller vara avhänt någon genom brott eller förverkat på grund av brott får tas i beslag. Bestämmelsen omfattar tre olika typer av beslag som i doktrin benämns bevisbeslag, återställandebeslag och förverkandebeslag.[85] Ett ytterligare krav för beslag är att föremålet i fråga finns tillgängligt, vilket utesluter att tvångsmedlet används för att söka efter visst material. Föreligger ett sådant behov får istället andra tvångsmedel, exempelvis husrannsakan, vidtas. Med begreppet föremål avses i bestämmelsen lös egendom, vars innebörd ofta anses framgå motsatsvis av 1 kap. 1 § JB och således innefatta all egendom som inte är jord.[86] Det kan också poängteras att bestämmelsen, enligt 27 kap. 1 § 2 st. RB, skriftliga handlingar i de fall inget annat är stadgat.

Beviskravet som måste vara uppfyllt för att beslut om beslag ska kunna fattas är lågt ställt. Det måste endast vara mer sannolikt att föremålet kan ha betydelse för utredningen, än att så inte är fallet.[87] För att exemplifiera kan det röra sig om ett bevis i form av en kameraövervakning som har direkt bety-

[83] Lindberg (2018), s. 621.
[84] SOU 2017:100, s. 257.
[85] Nordh (2007), s. 92; jfr Fitger m.fl. (2019), kommentaren till 27 kap. 1 § RB.
[86] Åklagarmyndigheten (2010), s. 6.
[87] Nordh (2007), s. 92.

delse för den enskildes skuld men det kan också vara frågan om andra omständigheter som för utredningsarbetet framåt.[88] Vid beslut om beslag ska proportionalitetsprincipen beaktas, vilket 27 kap. 1 § 4 st. RB ger uttryck för. Tvångsmedel får beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse. Av principen följer att mindre inträngande åtgärder som är tillräckliga för att nå ändamålet ska vidtas i första hand. Är det tillräckligt att föremålet tas i förvar enligt 26 kap. RB ska det ske istället.[89]

Ett särskilt stadgande i 27 kap. 2 § 1 st. RB anger att skriftliga handlingar inte får tas i beslag om de kan antas innehålla uppgifter som en befattningshavare eller någon annan som avses i 36 kap. 5 § RB inte får höras som vittne om förutsatt att det är denne eller den som tystnadsplikten avser som innehar handlingen. Bestämmelsens är ett förbud mot beslag av meddelanden som har anförtrotts bland annat läkare, advokater eller psykologer i deras yrkesutövning. Förbudet gäller, enligt 27 kap. 2 § 2 st., också skriftliga meddelanden mellan den misstänkte och en närstående som avses i 36 kap. 3 § RB, eller mellan sådana närstående inbördes om inte något av de uppräknade undantagen är tillämpligt.

När tvångsmedlet appliceras på fysiska skriftliga handlingar såsom handelsböcker eller brev är regelverket, enligt Hallbäck, välutvecklat och lämpligt utformat.[90] Beträffande beslag i IT-miljöer ställs emellertid särskilda krav på de brottsbekämpande myndigheterna. Utöver teknisk expertis krävs exempelvis, i linje med 27 kap. 10 § 3 st. RB, att myndigheten ser till att materialet som tas i beslag vårdas på ett sätt som utesluter missbruk, förstörelse eller förändringar av materialet. I fråga om fysiska ting krävs ingen särskild kunskap för att uppfylla kravet men det kan vara betydligt svårare när materialet är digitalt.[91] När säkring av digitalt bevismaterial sker i praktiken fattas ofta ett beslut om husrannsakan och beslag. Ändamålet är att eftersöka och samla in det digitala materialet. Föremål för tvångsåtgärden är i dessa situationer inte data utan det fysiska datorsystemet. Det kan exempelvis röra sig om just en dator, men det kan också gälla en digitalt uppkopplad kopiator eller delar av ett datorsystem, såsom en hårddisk eller ett enklare minneskort.[92] När brottsbekämpande myndigheter samlar in digital information genom nämnda tvångsåtgärder ska förfarandet dokumenteras. Det är viktigt både för att samla in den information som finns tillgänglig i syfte att säkra bevis men också för

[88] Åklagarmyndigheten (2010), s. 4 f.
[89] Prop. 2007/08:68, s. 85.
[90] Hallbäck (2009), s. 27.
[91] Kronqvist (2013), s. 49.
[92] Ibid., s. 49 f.

att försäkra sig om att åtgärden inte strider mot 27 kap. 10 § 3 st. RB. Sammansättningen av datorsystemets komponenter kan ge en antydan om verksamhetens omfattning och digitalt material av betydelse ur bevishänsyn kan förekomma på skärmen. Datorsystem är ofta komplexa med flertalet komponenter och plockas det isär för att sedermera sättas ihop och granskas kan delar förväxlas eller på annat sätt förändras. Beslag av material i IT-miljöer kan därför kräva särskild noggrannhet.[93]

I sammanhanget bör särskild uppmärksamhet skänkas den situation då brottsbekämpande myndigheter utforskar ett datorsystem i syfte att komma åt mer material än det som finns direkt tillgängligt. Vid ett beslut om husrannsakan finns ingen särskilt angiven bestämmelse beträffande möjligheten att söka okänd information i ett datorsystem. Enligt Kronqvist är sådant efterforskande är emellertid tillåtet vid beslut om beslag.[94] Visserligen innehåller inte heller 27 kap. RB om beslag några särskilda bestämmelser om de beskrivna förhållandena, men JO har i ett beslut tagit ställning i frågan. Åklagaren hade i ett mål beslagtagit ett datorsystem och därefter sökt fram e-postmeddelanden mellan den misstänkte och dennes fru. Materialet i sig fick inte användas som bevis eftersom det för brottet inte var föreskrivet minst två års fängelse, 27 kap. 2 § 2 st. 1 p. RB, men det konstaterades att förfarandet i sig inte var otillåtet. Samma beslut från JO fastslår att det förbud som bestämmelsen stadgar även gäller elektronisk kommunikation, trots att det faller utom dess ordalydelse.[95] I beslutet hänvisar JO till ett JK-beslut som intar samma ställning i frågan och understryker att det föreligger ett behov av lagstiftning kring tillämpligheten av 27 kap. RB i fråga om annat än skriftliga handlingar. Det framhålls också att ett behov av klargörande kring rätten att efterforska annan information än den som är direkt tillgänglig föreligger.[96]

[93] Kronqvist (2013), s. 50.
[94] Ibid., s. 124.
[95] JO:s beslut dnr 2138-2007.
[96] JK:s beslut dnr 6373-07-31.

4 Transnationell insamling av digitala bevis

4.1 Det internationella ramverket

För att få grepp om det problem uppsatsen aktualiserar förutsätts en förståelse för vilka internationella verktyg som finns att tillgå. Därför kommer de folkrättsliga rättskällorna kortfattat presenteras nedan. En förståelse för rättskällorna leder i sin tur till insikten om att folkrätten är i ständig förändring. Denna insikt är central för att besvara uppsatsens frågeställningar.

När transnationella straffrättsliga problem uppstår måste varje suverän stat, för att undvika konflikt, ta hänsyn till de folkrättsliga rättskällor som bestämmer ramen för varje stats jurisdiktion.[97] Enligt Internationella domstolens stadga art. 38, som ofta anses ge uttryck för vilka de folkrättsliga källorna är,[98] ska rättskällorna beaktas enligt följande hierarkiska ordning:

1. Internationella multilaterala överenskommelser (traktat),
2. Internationell sedvanerätt,
3. Allmänna principer och rättsgrundsatser som erkänns av världens mest betydande rättssystem, och
4. Internationella domstolstolars avgöranden, internationell doktrin samt nationella domstolars tillämpning av internationell rätt.

Internationella multilaterala överenskommelser är mellanstatliga avtal som parterna (staterna) efter ratificering har att följa enligt principen om pacta sunt servanda. Att ingå en traktat är att inskränka sin egen suveränitet till förmån för avtalet. En stat kan inte hänvisa till nationell lagstiftning för att agera på ett sätt som strider mot avtalet. Det finns dock möjlighet att genom reservationer begränsa skyldigheten att följa de förpliktelser som stadgas i avtalet.[99]

Regleras ett förhållande inte av traktat kan en stat hänvisa till internationell sedvanerätt. Rättskällan skiljer sig från traktat bland annat genom att vara bindande för alla stater med undantag för det fall då en stat som inte vill bli bunden ihärdigt motsätter sig sedvanan. Två kriterier ska vara uppfyllda för etablerandet av internationell sedvanerätt: (1) det ska finnas en allmän och enhetlig praxis mellan stater och (2) denna praxis ska av staterna anses vara

[97] Helenius (2014), s. 200.
[98] Cassese (2003), s. 26 f.; Henriksen (2019), s. 22.
[99] Linderfalk (2012), s. 77 ff.; Helenius (2014), s. 201.

förpliktigande.[100] Kravet på allmän och enhetlig praxis är objektivt och innebär att saker ska göras på ett visst sätt samt att detta upprepar sig kontinuerligt. Det andra kravet är subjektivt och tar sikte på staternas inställning till praxisen (”opinio juris”). För etablerandet av ny sedvanerätt krävs att praxisen anses vara bindande, varför staternas inställning till den är avgörande. Det subjektiva kriteriet är särskilt intressant när ny sedvänja skapas eller när gammal sedvänja förändras, dess utformning innebär att ny praxis blir bindande och gammal icke-bindande vid en given punkt.[101] Det betyder i praktiken att en förändring av internationell sedvanerätt ofta innebär att stater i ett initialt skede bryter mot en etablerad regel.[102] Inget särskilt stadgande finns som klargör hur många stater som ska ha omfamnat ny praxis för att den ska bli bindande.[103] Det kan emellertid påpekas att vikten av den regel som är föremål för förändring spelar en roll. Ju viktigare regel, desto större enhetlighet och kontinuitet krävs i anammandet av ny praxis. Därtill kräver förändringar som inskränker statssuveräniteten generellt sett större enhetlighet och kontinuitet än regler som inte inskränker den.[104]

Allmänna rättsgrundsatser, eller ”allmänna, av de civiliserade folken erkända rättsgrundsatser”, tar sikte på rättsliga principer av allmän karaktär som genomsyrar rättssystemen i ett stort antal stater. Här kan exemplifieras med principer såsom ne bis in idem och legalitetsprincipen. Särskilt viktiga är de allmänna rättsgrundsatserna, tillsammans med internationell sedvanerätt, när det kommer till frågor om jurisdiktion.[105]

Slutligen tillkommer två sekundära rättskällor – ”rättsliga avgöranden” och ”de olika ländernas mest sakkunniga författares lärosatser”. Den första avser praxis i form av domslut från såväl internationella som nationella domstolar och skiljedomstolar som kan användas i syfte att konstatera gällande rätt. Den andra beskriver doktrin publicerad av folkrättens främsta forskare.[106] Doktrin kan få särskild betydelse för etablering eller förändring av internationell sedvanerätt. Publicerad forskning kan ofta förutspå förändringar eller leda lagstiftare in på ett visst spår.[107] Det anses dock vedertaget att doktrin inte ensamt kan etablera folkrättsliga regler.[108]

[100] Henriksen (2019), s. 24.
[101] Ibid., s. 26 ff.
[102] Dixon (2007), s. 36.
[103] Ibid., s. 31 f.
[104] Ibid., s. 32.
[105] Helenius (2014), s. 203.
[106] Dixon (2007), s. 43 ff.; jfr Helenius (2014), s. 202 f.
[107] Dixon (2007), s. 46 f.
[108] Ibid., s. 47.

4.2 Jurisdiktion

4.2.1 Statssuveränitet och exekutiv jurisdiktion

Begreppet exekutiv jurisdiktion är centralt när en diskussion förs om myndigheters möjligheter att utreda brott. Därför måste visst fokus läggas på att tydliggöra innebörden. Särskilt bör poängteras att exekutiv jurisdiktion har en nära koppling till staters territorium. Det första kan svårligen diskuteras utan ett omnämnde av det andra. En förklaring av hur de hänger ihop är således påkallad.

Den grundläggande principen om att alla stater är suveräna och likställda följer bland annat av FN-stadgan art. 2(1). Den innebär att alla stater har att respektera andra staters suveränitet och likställdhet. Ingen stat får kränka en annan stats territoriella överhöghet.[109] Varje stat har ensamrätt att utöva makt och att i allmänhet förfoga över sitt territorium. Här följer ett direkt förbud mot att utöva myndighet på ett sätt som kränker en annan stats territoriella suveränitet.[110]

När stater vidtar åtgärder för att verkställa beslut som har fattats av domstol eller av en rättskipande myndighet kan det talas om exekutiv jurisdiktion. Åtgärder av exekutiv karaktär kan vara insamling av bevis, häktning eller annan användning av våld. Jurisdiktionstypen är unik genom att vara nästan uteslutande bunden till statens territorium. Det är, i enlighet med idén om alla staters suveränitet och likställdhet, inte tillåtet med transnationell myndighetsutövning. Det gäller inte minst straffprocessuella förfaranden inom ramen för en förundersökning.[111]

För att förstå förhållandet mellan nationell straffrättslig jurisdiktion och folkrätten är Lotus-fallet viktigt. Fallet avsåg ett franskt fartyg, ”Lotus”, som kolliderade med ett turkiskt fartyg, ”Boz Kourt”, på internationellt vatten. Det franska fartyget klarade sig utan större skador medan det turkiska sjönk vilket resulterade i att åtta turkiska medborgare dog. När vakthavande officer på den franska båten klev i land i Turkiet anhölls han och dömdes sedermera för dråp till fängelse och böter. Frankrike invände och hävdade att Turkiet genom sitt handlade hade brutit mot det folkrättsliga regelverket kring jurisdiktion. Fallet togs upp i den Internationella mellanfolkliga domstolen och den väsentliga frågan rörde det som kallas judikativ jurisdiktion – omfattningen av nationell

[109] Linderfalk (2012), s. 49.
[110] Helenius (2014), s. 207.
[111] Linderfalk (2012), s. 49; Wong (2004), s. 59; SOU 2002:98, s. 73; Akehurst (1973), s. 146.

domstols rätt att utöva judikativ makt. Domstolen gjorde dock ett utlåtande av intresse gällande exekutiv jurisdiktion:

> ”Now the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.” [112]

Domstolen förde ytterligare resonemang om den nationella domstolens judikativa jurisdiktion och dömde till fördel för Turkiet. Fallet har givit upphov till den så kallad Lotus-principen, vilken innebär att varje stat har rätt att lagstifta om gränsöverskridande judikativ jurisdiktion förutsatt att den inte står i strid med traktat eller internationell sedvanerätt. Än viktigare för denna uppsats vidkommande är att principen stadgar ett förbud för stater att på något sätt utöva exekutiv jurisdiktion inom en annan stats territorium.[113] Med andra ord har stater typiskt sett inte möjlighet att verkställa beslut inom en annan stats territorium.[114] Det skulle, som ovan nämnt, vara en kränkning av statssuveräniteten att exempelvis låta brottsbekämpande myndigheter överträda yttre gräns mot en intilliggande stat och utföra myndighetsutövning. För att belysa omfattningen av förbudet kan Internationella domstolens ställningstagande i ”Arrest Warrant-fallet” uppmärksammas. Här ansågs att redan utfärdandet av en arresteringsorder var att anse som en exekutiv åtgärd.[115]

4.2.2 Exekutiv jurisdiktion och insamling av digitala bevis

Världen har till följd av den teknologiska utvecklingen kommit att förändras väldigt mycket under en relativt kort tid. ITU uppskattar att över fyra miljarder människor vid 2019 års slut hade tillgång till en internetuppkoppling.[116] Det innebär att brottsbekämpande myndigheter i större utsträckning har blivit tvingade att beakta de särskilda karaktärsdrag som tillhör datorsystem och internetuppkopplingar. Ett fenomen som har uppstått till följd av utvecklingen är IT-brotten.[117] För att ge exempel på IT-brott har medial uppmärksamhet tillägnats det att företag pressas på pengar genom en form av datorvirus som kallas ransomware. Viruset infiltrerar offrets datorsystem och gör det otill-

[112] S.S. Lotus (France v. Turkey), 1927 PCIJ (ser. A) No. 10, s. 18-19.
[113] Helenius (2014), s. 211 f.; jmf. Henriksen (2019), s. 93 f.
[114] Oppenheim (1992), s. 386 f.
[115] Case Concerning the Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium).
[116] ITU (2019) under ”Elektroniska källor”.
[117] Osula (2017), s. 7.

gängligt. För att offret ska återfå tillgången till sitt system begärs en lösensumma.[118] Det är även vanligt förekommande att mer traditionella brott begås över internet. Olaga hot kan skickas via mail eller chattfunktioner, ofredande kan bestå i att en person med hög frekvens kontaktar någon som inte vill bli kontaktad via sociala medier och narkotikaförsäljning kan förrättas.[119]

Utvecklingen har särskilt fört med sig att brottsbekämpande myndigheter utmanas i sitt arbete med att samla in bevis under brottsutredningar. En anledning till detta är att brotten som begås på olika sätt kan vara relaterade till olika geografiska områden och således även falla under olika staters jurisdiktion.[120] Bland annat rapporterade FN i en enkätstudie utställd till medlemsstaterna att de brottsbekämpande myndigheterna uppgav att mellan 30 och 70 % av IT-brottsutredningarna innehöll transnationella moment, såsom frågor om jurisdiktion och transnationell insamling av bevis.[121] Respondenterna angav också att kommunikation över internet nästan uteslutande innefattade transnationella dimensioner.[122] Av samma rapport framgick att Europol uppskattade att en stor majoritet av utredningar avseende internationellt organiserad brottslighet sannolikt förutsätter bruk av internet.[123]

En ytterligare faktor som komplicerar brottsutredningar är att bevismaterial ibland inte kan lokaliseras eller att de finns utspridda över flera geografiska punkter samtidigt.[124] I det senare av fallen har det i doktrin funnits en uppfattning om att varje stat har exklusiv exekutiv jurisdiktion över den del av materialet som finns inom dess territorium.[125] Denna ståndpunkt får också stöd av vad myndigheter uppgett i ovan nämnda FN-rapport.

Trots inställningen till frågan uppger myndigheter att transnationell insamling av digitala bevis utan samtycke sker regelbundet i praktiken.[126] Det föreligger möjligtvis en diskrepans mellan staters uppfattning av rättsläget och hur myndighetsutövandet går till.[127] En sådan diskrepans skulle kunna leda till spänningar, konflikter och oönskade hämndaktioner stater emellan.[128] Det skulle också kunna innebära att det har skett en förändring av statspraxis. Denna tes

[118] Larsson (2020) under ”Elektroniska källor”; Johansson (2017) under ”Elektroniska källor”.
[119] Polisen (2019) under ”Elektroniska källor”; Larsson (2020) under ”Elektroniska källor”.
[120] Osula (2017), s. 7.
[121] UNODC (2013), s. 23.
[122] Ibid., s. 5.
[123] Ibid., s. 45.
[124] Se avsnitt 2.3.
[125] Spoenle (2010) under “Elektroniska källor”.
[126] UNODC (2013), s. 220-223; CoE (2012) under “Elektroniska källor”.
[127] Osula (2017), s. 35.
[128] Osula (2015a), s. 59 f.

styrks av att inga tydliga mellanstatliga konflikter kan urskiljas vid en granskning av tillgängligt material.[129]

Som redogjorts för har exekutiv jurisdiktion traditionellt sett varit strikt begränsad till staters territorium. Enligt Internationella mellanfolkliga domstolens uttalande i Lotus-fallet får en stat inte på något sätt utöva makt inom en annan stats territorium utan en legitim folkrättslig grund. Att vidta en sådan åtgärd hade inneburit en kränkning av motstående stats statssuveränitet.[130] Som ovan beskrivits har brottsbekämpande myndigheter utmanat denna princip genom att vidta transnationella åtgärder som potentiellt skulle innebära en sådan kränkning. Med hjälp av teknologiska verktyg har externt lagrade bevis samlats in på distans utan nyttjande av de vedertagna legitima kanaler som finns att tillgå.[131] Så har varit fallet både i situationer då materialets geografiska position har varit välkänd och då det inte har kunnat lokaliseras.[132]

Något som följaktligen måste utredas är om den förändring som har skett i statspraxis kan anses förenlig med gällande rätt eller om den fortsatt strider mot Lotus-principen och således utgör en suveränitetskränkning. Detta blir särskilt intressant mot bakgrund av att digitalt lagrad bevisning kan inhämtas utan att insamlande myndigheter behöver befinna sig på utländskt territorium för att vidta en sådan åtgärd.[133]

Vid en granskning av doktrin framkommer två olika förhållningssätt till problemet. En inställning till insamling av digitala bevis lokaliserade i en annan stat är den strikta tolkningen av Lotus-principen.[134] Varje enskilt transnationellt försök att utöva exekutiv jurisdiktion är enligt detta att se som en kränkning av statssuveräniteten. Med ett sådant perspektiv kan varken efterforskande eller insamling av bevis som finns lokaliserat på en server i utlandet genomföras utan ett folkrättsligt legitimt samtycke.[135] Det spelar enligt detta synsätt ingen roll om den åtgärd som har vidtagits av den brottsbekämpande myndigheten faktiskt har resulterat i någon skada inom motstående stat jurisdiktion, exempelvis skador på digital infrastruktur såsom nätverk eller servrar.[136] Inställningen är återkommande i nationell praxis och i äldre doktrin förekommer resonemang om att slutresultatet är det som bör beaktas.[137] Eftersom genomsökandet av en hårddisk från distans kan anses ha samma effekt

[129] Se bland annat avsnitt 4.4.2.
[130] Oppenheim (1992), s. 384 f.
[131] Se exempelvis avsnitt 4.3.
[132] CoE (2012) under "Elektroniska källor".
[133] Cassese (2003), s. 51.
[134] de Hert (2006), s. 71 f.
[135] Ibid., s. 72.
[136] Koops & Goodwin (2016), s. 61 ff.
[137] Se United States v. Microsoft under avsnitt 4.4.2.

som gängse fysiska genomsökningar av utrymmen bör den också straffprocessuellt betraktas som en sådan.[138] Ett problem med ett sådant strikt förhållningssätt är att det riskerar att leda till frekventa folkrättsliga övertramp.[139] De myndigheter som i ovan nämnda FN-rapport angett att insamling av digitala bevis har skett autonomt har, enligt synsättet, i varje enskilt fall gjort sig skyldiga till kränkningar av statssuveräniteten.

En annan inställning är att tillåta efterforskning och insamling av digitala bevis i situationer då åtgärderna inte resulterar i någon skada på digital infrastruktur inom den andra statens territorium.[140] En tolkning av denna inställning är att en kränkning endast uppstår om förfarandet leder till materiell skada av en viss magnitud. Mindre skador skulle således vara acceptabla.[141] En annan är att tillåta all efterforskning och insamling av digitalt lagrade bevis under förutsättning att ingen materiell skada uppstår på infrastruktur som faller under statlig immunitet, exempelvis servrar tillhörande statsmakten.[142] Risken med dessa förhållningssätt är att de skulle kunna urvattna den traditionella samarbetsmetoden för transnationella brottsutredningar och för insamling av bevis över gränserna. Stater skulle också i större utsträckning kunna missbruka friheten av att kunna agera utom den ram som följer av ett striktare synsätt.[143] Även här kan, som ovan, lyftas att brottsbekämpande myndigheter i praktiken redan agerar enligt föreskrivna modell. Vad gäller den situation då det digitala materialet inte kan lokaliseras framhåller de Hert särskilt att en uppfattning baserad på utfallet i Lotus-fallet är förlegad. Det argumenteras för att det hål som uppstår i förlängningen tillåter brottslingar att undkomma lagföring genom att med digitala verktyg dölja materialets position.[144]

4.3 Rättslig hjälp

När en brottsbekämpande myndighet behöver samla in material beläget i en annan stat har rättslig hjälp traditionellt sett varit vägen att gå för att undvika konflikt ur ett jurisdiktionshänseende. Genom MLA, baserade på direkta avtal mellan två stater eller genom multilaterala avtal, assisterar stater varandra med att vidta efterfrågade åtgärder. Den anmodade staten kan exempelvis samla in bevis inom dess territorium åt den anmodande staten.[145] Problemet med den här typen av avtal är att de förutsätter en process mellan staterna som

[138] Wilske & Schiller (1997), s. 174.
[139] Osula (2015b), s.723 f.
[140] Ibid., s. 727.
[141] Goldsmith (2001), s. 108.
[142] Osula (2015b), s. 726.
[143] Goldsmith (2001), s. 116.
[144] de Hert (2006), s. 72; Se avsnitt 2.3.
[145] Osula (2017), s.8 f.

kan vara långsam, utdragen och resurskrävande. Det finns inte heller enhetlighet i hur processen hanteras.[146] Vissa länder kräver att en förfrågan om rättslig hjälp skickas till styrande myndigheter såsom Justitiedepartementet medan andra tillåter att förfrågan skickas direkt till verkställande myndighet, exempelvis Åklagarmyndigheten. Enligt en rapport från det internationella organet CoE förekommer också en diskrepans mellan kraven på detaljer i förfrågan. Somliga länder kräver att det material som efterfrågas finns specificerat medan det i andra länder är tillräckligt med generella beskrivningar av det som efterfrågas.[147]

Ytterligare problem uppstår i de situationer då avtalet inte täcker den typ av utredningsåtgärd som är aktuell, när länder inte har resurser eller saknar samarbetsvillighet och då materialet som behöver samlas in inte kan lokaliseras. I sistnämnda situation kan en förfrågan om rättslig hjälp inte skickas eftersom ingen motstående stat kan identifieras. Skulle en insamlande åtgärd ändock vidtas föreligger en risk för att den i ett senare skede kan visa sig ha utgjort en suveränitetskränkning.[148] Svenska brottsbekämpande myndigheter skulle exempelvis kunna beslagta en datafil vars position är dold med Tor-nätverket eftersom den misstänks tillhöra den som är föremål för utredningen. Sådana åtgärder är inte ovanliga, eftersom digitalt material lätt kan modifieras, förflyttas eller förstöras.[149] Skulle myndigheten vid ett senare tillfälle lyckas spåra relay-kedjan till ursprungskällan, kan det visa sig att datafilen fanns på en server inom en annan stats territorium.

Effektiviteten i förfarandet kan också vara bristfällig av andra skäl. Förfrågningar kan komma att skickas fram och tillbaka mellan länder eftersom riktlinjerna kring vad den ska innehålla är oklara – ofta till följd av språkförbristningar. Myndigheter uppger också att det kan vara problematiskt att få en bekräftelse på att förfrågan har nått rätt myndighet i mottagarlandet eller att i allmänhet få kännedom om statusen på förfrågan.[150] I praktiken har det inneburit att de utredande myndigheterna stundtals har underlåtit att överhuvudtaget fullfölja förfarandet vilket kan resultera i att bevismaterial av vikt för en utredning inte samlas in.[151]

[146] Osula (2015a), s. 47.
[147] CoE (2014) under "Elektroniska källor".
[148] Osula (2017), s. 11.
[149] Se exempelvis avsnitt 4.4.1.2.
[150] CoE (2014) under "Elektroniska källor".
[151] Ibid., s. 7.

4.4 Alternativa lösningar i Europa och USA

4.4.1 Multilaterala avtal

4.4.1.1 CoCC

Till följd av den utveckling som fortlöper på det tekniska området och mot bakgrund av den kritik som har riktats mot det konventionella förfarandet med rättslig hjälp har olika alternativa lösningar kommit att träda fram. CoE har upprättat ett multilateralt avtal, benämnt CoCC, och EU har utfärdat ett direktiv om europeisk utredningsorder. Det förekommer också att nationella domstolar tolkar internationell rätt på nya sätt och i ett flertal fall har länder infört utmanande lagstiftning som reglerar frågan. Nedan följer en mer detaljerad genomgång av ett antal exempel på hur ineffektivitetsproblemet har hanterats i Europa och i USA.

Merparten av de traktat och konventioner som rör mellanstatlig assistans vid utredning av brott utgår från den traditionella synen på statssuveränitet och territorialitet. Enligt Verdelho utesluter de alla typer av autonomt myndighetsutövande av en stat i en annan.[152] Den av CoE upprättade Budapest-konventionen (härefter CoCC) skiljer sig från merparten av övriga konventioner genom att till viss del frångå det konventionella förhållandet till territorialitet. Därför kommer en genomgång av ett antal utvalda bestämmelser följa nedan. Det bör påpekas att konventionen i april 2020 hade ratificerats av 65 länder och att ytterligare tre hade signerat traktaten. En granskning av konventionen och tillhörande rapporter kan således ge en fingervisning kring rättsläget. Här kan lyftas att Sverige signerade konventionen den 23 november 2001 men konventionen har fortfarande inte ratificerats.[153]

Konventionen avser IT-relaterad brottslighet och innehåller regler som ställer krav på medlemsländerna att kriminalisera vissa typer av brott, såsom datorrelaterat bedrägeri, art. 8 CoCC, och barnpornografibrott, art. 9 CoCC. Den reglerar emellertid även vissa processuella förfaranden i fråga om insamling av bevis. Varje medlemsstat ska exempelvis upprätta processuella regler som explicit ger utredande myndigheter rätt att söka upp och samla in digitalt bevismaterial inom dess territorium, art. 19(1) CoCC. Enligt art. 22 CoCC ska de processuella reglerna vara utformade för att etablera jurisdiktion inom statens territorium, över fartyg som bär statens flagg, över luftfartyg registrerade i staten och över dess medborgare om brottet var straffbart där det begicks

[152] Verdelho (2019), s. 138; jfr Linderfalk (2012), s. 49.
[153] CoE (2020a) under "Elektroniska källor".

eller om det har skett utom alla staters territorium. Tanken är att de straffprocessuella reglerna ska säkerställa efterlevandet av det mellanstatliga samarbete som konventionen eftersträvar.[154] Detta kan vara särskilt nödvändigt mot bakgrund av att en FN-rapport har konstaterat att sedvanliga straffprocessuella bestämmelserna sällan är anpassade till digitalt lagrat bevismaterial.[155]

Det som huvudsakligen gör konventionen intressant för uppsatsens vidkommande är att den särskilt reglerar territoriella frågor när digitalt bevismaterial samlas in. Enligt art. 23 CoCC stadgas en grundprincip om att staterna i utförligaste mån ska assistera varandra i mellanstatliga straffrättsliga frågor för att optimera utredningsförfarandet och särskilt för att kunna samla in digitala bevis. Vidare förekommer vissa särskilda bestämmelser som ställer mer precisa krav på medlemsstaterna i ett försök att effektivisera samarbetsprocessen. För att exemplifiera ska staterna enligt art. 35 CoCC införa en särskild kontaktpunkt som ska finnas tillgänglig 24 timmar om dygnet och varje dag i veckan för att snabbast möjligt kunna hantera förfrågningar om assistans i vissa fall. I enlighet med art. 31 CoCC ska varje stat agera särskilt skyndsamt när en förfrågan om assistans inkommer, och det finns anledning att anta att bevismaterialet i fråga kan försvinna eller modifieras. Det förekommer dock inga särskilt angivna tidsramar som slår fast hur fort det ska gå.

Art. 32 a CoCC stadgar vidare att en medlemsstat har rätt att utan samtycke från den stat där bevismaterialet finns lokaliserat samla in det om det faller under det som benämns som ”open source”. Det innebär att materialet ska vara tillgängligt för vem som helst via en webbläsare.[156] Art. 32 b CoCC anger vidare att medlemsstaterna har rätt att, med legalt och frivilligt samtycke från den som har rätt till det, samla in materialet. Således stadgas här två situationer då en stat kan söka upp och samla in bevismaterial som finns lokaliserat i en annan stat utan att efterfråga ett uttryckligt samtycke utöver det som följer av konventionens bindande verkan.[157] Den första avser allt material som omfattas av open source. Den andra kan illustreras med den situation då den brottsbekämpande myndigheten upptäcker ett visst material av intresse som finns på en webmail-server inom en annan stats territorium. Enligt bestämmelsen har den utredande staten rätt att kontakta serverleverantören med en förfrågan om att få tillgång till materialet. Samtycker serverleverantören kan materialet överföras utan att motstående stat involveras.

[154] CoE (2001) under “Elektroniska källor”.
[155] UNODC (2013), s. 122.
[156] Verdelho (2019), s. 138.
[157] Ibid., s. 138.

I ett vägledande dokument från CoCC-kommittén angavs särskilt att art. 32 b var att se som ett undantag från principen om territorialitet.[158] Detta till trots har inga stater gjort förbehåll eller reservationer kring bestämmelsen.[159] Rapporten tog inte på samma sätt ställning till art. 32 a vilket kan antyda att insamlande av open source-material redan är att betrakta som förenligt med internationell sedvanerätt. Det förekommer också stöd för denna uppfattning i doktrin.[160] Art. 32 b är av särskilt intresse då det brottsutredande förfarandet kräver att myndigheten i fråga skyndsamt kan beredas tillgång till materialet som finns lagrat. Den aktualiseras också när materialets position inte kan bestämmas till följd av att användaren brukar anonymitetstjänster såsom Tor. Dessa situationer påkallar särskilt att utredande myndigheter har en möjlighet att frångå det traditionella förfarandet med rättslig hjälp.[161] Att kunna rikta sig direkt till den som har rätt till bevismaterialet, exempelvis en serverleverantör, erbjuder en sådan möjlighet för de utredande myndigheterna.[162] Nedan följer också exempel på när stater har samlat in material direkt från serverleverantörer och resonemang om vilka problem som kan uppstå.[163]

4.4.1.2 EUO

EU har tillkännagivit att det föreligger ett behov för att effektivisera de verktyg som medlemsstaterna kan nyttja för att få åtkomst till digital bevisning som finns lokaliserad i utlandet. Anledningen är att ett långsamt förfarande innebär en risk för att bevismaterial förstörs, modifieras eller förflyttas.[164] I ett försök att hantera problemet har EU år 2014 utfärdat ett direktiv om europeisk utredningsorder som medlemsstaterna skulle ha genomfört senast den 22 maj 2017. Det ska uppmärksammas att direktivet inte uteslutande berör digitala bevis men ett antal centrala artiklar presenteras nedan.

Enligt art. 1 EUO är en europeisk utredningsorder ett rättsligt beslut som har verifierats av en auktoritet, i Sverige exempelvis åklagare eller domstol[165], om en eller flera utredande åtgärder i en annan medlemsstat i syfte att samla in bevisning i enlighet med direktivet.

Enligt art. 5 EUO stadgas ett antal krav på utförandet och innehållet i en europeisk utredningsorder. Bland annat ska den vara utfärdad och påskriven av rätt organ. Den ska också innehålla en beskrivning av den brottsliga gärning

[158] CoE (2014) under "Elektroniska källor".
[159] CoE (2020b) under "Elektroniska källor".
[160] Verdelho (2019), s. 139; Koops (2013), s. 655.
[161] Osula (2017), s. 23 f.
[162] Ibid., s. 24.
[163] Se avsnitt 4.2.2.
[164] Osula (2017), s. 20.
[165] Ds. 2015:57, s. 11.

som avses, vem som är föremål för utredningsåtgärden och vilka straffrättsliga bestämmelser i den utfärdande staten som är applicerbara.

Vidare följer av art. 6 EUO att den utfärdande staten endast får utfärda en europeisk utredningsorder under vissa förutsättningar. Bland annat ska den utfärdande staten, enligt art. 6(1) göra en bedömning av nödvändigheten av åtgärden och huruvida den är proportionerlig i förhållande till den enskildes rättigheter. Enligt art. 6(3) ska den mottagande staten kontakta den utfärdande staten för det fall kriterierna inte anses uppfyllda.

Art. 9 EUO konstaterar att den mottagande staten som huvudregel och i enlighet med principen om ömsesidigt erkännande, utan ytterligare formella krav, ska verkställa den efterfrågade åtgärden i enlighet med direktivet. Art. 11 EUO stadgar ett antal grunder på vilka den mottagande staten kan välja att underlåta att vidta den efterfrågade åtgärden eller att inte erkänna utredningsordern. Bland annat om brottet i fråga inte är kriminaliserat i det mottagande landet eller om åtgärden i fråga, enligt mottagande stats rättssystem, inte får vidtas för det beskrivna brottet.

Slutligen följer av art. 12(1) EUO att verkställigheten av den utredande åtgärden ska vidtas med samma prioritet som nationella utredningar i övrigt inom ramen för de tidsbegränsningar som följer av samma bestämmelse. Har den mottagande staten inte direkt tillgång till det material som utredningsordern avser ska den, enligt art. 12(4), inom loppet av 90 dagar vidta den utredningsåtgärd som efterfrågas.

Direktivet är ett led i att effektivisera de brottsbekämpande myndigheternas möjligheter att tillgodogöra sig digitala bevismaterial. Det löser dock inte de problemet som tidigare har diskuterats i fråga om MLA.[166] Art. 12 EUO som stadgar regeln om att mottagande stat ska agera inom 90 dagar och kraven på utformande och innehåll enligt art. 5 och 6 EUO, ger upphov till stelbenthet. Situationen då brottsbekämpande myndigheter snabbt behöver få tillgång till material för att undvika att det förstörs, modifieras eller flyttas förblir ett problem.[167]

4.4.2 Nationell praxis

Som framgår av den FN-rapport innehållandes en anonym enkätstudie utställd till medlemsstaternas brottsbekämpande myndigheter är det inte sällsynt att transnationell insamling av bevis sker utan samtycke.[168] Således

[166] Se avsnitt 4.3.
[167] Osula (2017), s. 21.
[168] Se avsnitt 4.2.2.

borde det finnas många praktiska exempel där frågan hanterats av nationella domstolar. Detta till trots är praxis på området inte särskilt utbredd, men det finns anledning att redogöra för några av de nationella avgöranden som finns att tillgå. Enligt Oppenheim har nationella domar en viss inverkan på rättsutvecklingen avseende jurisdiktion.[169] Vid en granskning av det material som finns att tillgå tycks denna uppfattning särskilt ta sikte på judikativ jurisdiktion som har utforskats förhållandevis grundligt. Detta innebär dock inte att nationella avgöranden saknar inflytande på rättslägets utveckling i fråga om exekutiv jurisdiktion. Om inte annat så kan de vara vägledande i att utröna hur den aktuella staten agerar i praktiken och i att konstatera statens inställning till det problem som hanteras.[170] Något som tydligt framgår vid en överblick är att de fall som når domstol oftast involverar den aktuella staten och en motstående enskild part som tillhandahåller en digital tjänst. Det står också klart att det inte finns ett enhetligt förhållningssätt till vilken vikt territorium och exekutiv jurisdiktion ska tillmätas.

I somliga fall kan en utredande myndighet vara i behov av information eller bevismaterial som finns lagrad hos en serverleverantör.[171] När en serverleverantör har sitt säte eller en berörd server i den stat myndigheten är verksam kan nationella straffprocessuella regler om tvångsmedel nyttjas.[172] I fall då serverleverantören har sitt säte i utlandet kräver avtal om rättslig hjälp typiskt sett att den utredande myndigheten går via myndigheter i berörda stat istället för att rikta sig direkt till serverleverantören.[173]

I ett belgiskt rättsfall från 2013 hade brottsbekämpande myndighet skickat en begäran om utlämnande av digitalt lagrad information, i form av e-post-meddelanden, direkt till Yahoo!. Bolaget hade varken säte eller dotterbolag lokaliserade i Belgien. Genom att påpeka att de belgiska myndigheterna hade att nyttja rättslig hjälp för att få åtkomst till materialet motsatte sig Bolaget begäran. Bolaget fälldes i första instans och vid prövning i överinstans angav rätten att det faktum att bolaget inte hade säte eller dotterbolag i Belgien var irrelevant.[174] Vid en slutlig prövning i den belgiska kassationsdomstolen konstaterades att det var tillräckligt att Yahoo! tillhandahöll den aktuella tjänsten inom Belgiens territorium, varför efterfrågan av det digitala materialet inte kunde anses transnationell. Utan hänsyn till var bolaget hade sitt säte eller var materialet i fråga fysiskt fanns lagrat ansågs förvägran utgöra ett brott inom

[169] Oppenheim (1992), s. 457.
[170] Se avsnitt 4.1.
[171] Se avsnitt 2.2.
[172] Velasco, Hörnle & Osula (2016), s. 469.
[173] UNODC (2013), s. 217; jfr art. 32 CoCC som tillåter att utredande myndighet kontaktar serverleverantörer i en annan stat.
[174] *Yahoo! Inc* [2013] Belgium Court of Appeal of Antwerp, 12th chamber for criminal cases 2012/CO/1054.

belgiskt territorium.[175] Domstolen fann här att myndigheterna hade rätt att begära utlämning av material med en exekutiv jurisdiktion baserad på var bolagets tjänst tillhandahölls. Enligt ovan nämnda rapport tillhörande CoCC skulle avgörandet strida mot Lotus-principen.[176]

En annan situation är den då brottsbekämpande myndigheter vänder sig till en serverleverantör som har säte inom dess territorium, men där materialet i fråga finns lagrat på en server i utlandet.[177] I ett fall från 2016, där territorialitet blev avgörande, hade amerikanska myndigheter riktat sig direkt till Microsoft med ett beslut om husrannsakan där innehållet i e-post-meddelanden från en viss person efterfrågades. Microsoft hävdade att de inte behövde lämna ut innehållet eftersom det fanns lagrat på en server placerad inom irländskt territorium. Beslutet om husrannsakan ansågs vara verkanslöst eftersom amerikanska myndigheter enligt Lotus-principen inte kan utöva exekutiv jurisdiktion på Irland. Underinstansen fällde Microsoft, men överinstansen friade och framhöll att nationella domstolar inte alltid har rätt att med hjälp av husrannsakan kräva serverleverantörer på e-post-meddelanden. Domstolen påpekade särskilt att de avsedda e-post-meddelandena var skickade eller mottagna av en irländsk medborgare, inom irländskt territorium via en tjänst som marknadsförts och tillhandahållits på Irland. Det framhölls också att beslag generellt ska anses ha ägt rum på den plats där e-post-meddelanden är fysiskt lagrade och vid den tidpunkt en kopiering av bevismaterialet sker.[178] Grunden för jurisdiktion tycks i det här fallet vara baserad på en samlad bedömning av medborgarskap, var meddelanden skickats och mottagits, hur tjänsten har riktats samt var det aktuella materialet fanns fysiskt lagrat, vilket ligger i linje med Lotus-principen.

I slutet av 2014 inledde amerikanska myndigheter en utredning av en barnpornografihemsida vid namn Playpen som endast fanns tillgänglig via Tornätverket för att anonymisera användarna.[179] Eftersom Tor dolde användarens reella IP-adress planterade amerikanska myndigheter via Playpen ett ”malware”, en förkortning på ”malicious software”, på användarnas datorsystem. Hemsidan togs över och när användare loggade in installerades ett program som rapporterade information som tillät utredarna att följa slingan av relayservrar tillbaka till ursprungsanvändarna.[180] Utredningen resulterade i flertalet rättsfall där det bevismaterial som myndigheterna kommit över med hjälp

[175] *Yahoo! Inc* [2015] Court of Cassation of Belgium P.13.2082.N.
[176] Se avsnitt 4.4.1.1.
[177] Velasco, Hörnle & Osula (2016), s. 470 f.
[178] *United States v. Microsoft Corporation. In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp.*, No. 14-2985 (2d Cir. 2016).
[179] Se avsnitt 2.3.2.
[180] Allen m.fl. (2020), s. 810 f.

av denna metod bedömdes vara otillåtet och således avvisades.[181] Eftersom Tor-nätverket maskerade användarnas geografiska position kunde utredarna inte vid tillfället då åtgärden vidtogs (installationen av malware och sökandet efter bevismaterial i användarnas datorer betraktades som en husrannsakan), ha haft vetskap om huruvida de befann sig inom en annan stats territorium. De hade av samma anledning inte möjlighet att specificera det avsedda föremålet för husrannsakan.[182] Rättsfallet problematiserar tydligt den situation då nationella myndigheter inte har möjlighet att utröna den geografiska positionen för det eftersökta digitala materialet. Situation utgör ett låst läge där åtgärden att lokalisera materialet bedöms vara folkrättsligt otillåten samtidigt som lokalisering krävs för att kunna rikta en förfrågan om rättslig hjälp till en annan stat – vilket skulle vara det traditionellt sett riktiga tillvägagångssättet. Autonom insamling av digitala bevis accepteras i detta fall inte överhuvudtaget.

I ett rättsfall från danska Højesteret konstaterades att straffprocessuella regler om tvångsmedel, i detta fall husrannsakan, kunde tillämpas för att efterforska information på Facebook-profiler och i chattmeddelanden skickade via Facebook Messenger. Trots att Danmark inte har några särskilda regler om insamling av digitalt lagrat material i utlandet ansågs den brottsbekämpande myndigheten ha agerat inom ramen för lagstiftningen.[183] Myndigheten hade kommit över lösenordet till en persons Facebook-konto genom hemlig telefonavlyssning. Därefter loggade myndigheten in och kartlade den information som fanns tillgänglig. Domstolen framhöll särskilt att utredningsåtgärden inte krävde att en annan stat bistod danska myndigheter och att det från vilken dator som helst gick att tillgodogöra sig informationen med hjälp av lösenordet. Højesteretet tog ingen särskild hänsyn till att det digitala bevismaterialet fanns lagrat inom en annan stats territorium.[184] Här förefaller dansk rätt behandla materialet som att det faller under begreppet open source.[185] Insamlande av sådant material anses generellt inte utgöra en inskränkning av statssuveräniteten. En förutsättning för detta är dock att vem som helst kan bereda sig åtkomst till materialet via en webbläsare. Så kan inte anses vara fallet om åtkomsten kräver angivandet av ett lösenord. Accepteras detta resonemang har domstolen öppnat upp för autonom transnationell insamling av bevis oavsett om motstående stat kan identifieras.

[181] Se t.ex. *United States v. Horton*, 863 F3d 1041 (8th Cir. 2017); *United States v. Levin*, 874 F.3d 316 (1st Cir. 2017); *United States v. Krueger*, 809 F3d 316 (1st Cir. 2017).
[182] Osula (2017), s. 43 f.
[183] SOU 2017:100, s. 372 f.
[184] Højesterets kendelse af 10. Maj 2012 (sag 129/2011).
[185] Se avsnitt 4.4.1.1.

4.4.3 Nationell lagstiftning

För att hantera den ovisshet som råder och för att brottsbekämpande myndigheter ska få tydliga riktlinjer har vissa länder lagstiftat om transnationell insamling av digitalt lagrade bevis. En redogörelse för hur sådan lagstiftning har utformats kan bidra till en helhetsbild ur vilken de lege lata på ett internationellt plan eventuellt kan utrönas. Mot bakgrund av Beslagsutredningen och uppsatsens tredje frågeställning finns också skäl att granska hur andra länder har utformat lagstiftning. Således följer nedan en presentation av utvald nationell lagstiftning på området.

Enligt belgisk straffprocessuell lagstiftning, art. 39bis § 1–2 CIC, kan brottsbekämpande myndigheter kopiera, frysa eller ta bort digitalt lagrad information förutsatt att ett beslut om husrannsakan har fattats. Bestämmelsen tar särskilt sikte på digitalt lagrad information som finns tillgänglig på den plats som husrannsakan omfattar. Skulle ett genomsökande av exempelvis en dator som finns på platsen leda till upptäckten av externt lagrat digitalt material måste den brottsbekämpande myndigheten ansöka om ytterligare tillstånd för att få samla in det. Detsamma gäller om det initialt påträffade datorsystemet är kopplat till ett datorsystem som inte finns på platsen om det senare ska utforskas. Enligt art. 39bis § 3–6 CIC (tidigare art. 88ter CIC) kan ett tillstånd att gå vidare utfärdas förutsatt att det finns utredningsmässiga skäl som är proportionerliga i förhållande till intrånget och om det finns anledning att anta att materialet kan försvinna. Av samma bestämmelse följer att förfarandet är begränsat till datorsystem och material som finns direkt tillgängligt via det initiala datorsystemet, men det tillåter exempelvis utforskandet av webmailkonton.[186] Brottsbekämpande myndigheter är vidare begränsade till att kopiera materialet för det fall det skulle visa sig vara lagrat inom en annan stats territorium. I sådant fall ska motstående stat också informeras. Här kan påpekas att svårigheten i att lokalisera data i praktiken har inneburit att motstående stat sällan informeras om förfarandet. [187] Belgisk rätt tillåter således i vissa fall att externt lagrat digitalt material efterforskas och autonomt samlas in – även när motstående stat har identifierats. Lagstiftning är inte direkt tillämplig på den situation som hanteras i det belgiska rättsfallet avseende Yahoo! men inställning till territorium framstår som densamma.[188] Osula framhåller att lagstiftningen, som strider mot den traditionella inställningen till exekutiv jurisdiktion, inte tycks ha gett upphov till mellanstatliga konflikter.[189]

[186] Royer, Conings & Marlier (2019), s. 209.
[187] de Hert & Boulet (2013), s. 23 f.
[188] Se avsnitt 4.4.2.
[189] Osula (2016), s. 366 ff.

Enligt sec. 19 PACE ska brottsbekämpande myndigheter i England och Wales se till att ha materiella förutsättningar för att efterforska och beslagta datorutrustning. För att en sådan åtgärd ska kunna vidtas måste tillstånd, i enlighet med sec. 9 PACE, ha utfärdats av en ”justice of the peace”, som inte nödvändigtvis är juridiskt skolad.[190] Ställning ska tas till huruvida det föreligger skäl att tro att objektet för åtgärden innehåller bevis av betydelse för ett relevant brott. Traditionell husrannsakan regleras av sec. 19(1–3) PACE och slår fast en generell rätt att beslagta objekt som skäligen kan antas innehålla bevismaterial, förutsatt att det är nödvändigt för att undvika att det förvanskas, försvinner eller förstörs. I fråga om digitalt lagrat bevismaterial har sec. 19(4) PACE särskilt införts. Bestämmelsen slår fast en rätt att efterforska och beslagta elektroniskt lagrad information oavsett form, under förutsättning att den är tillgänglig från objektet för husrannsakan och kan medbringas i läsbar eller synlig form. Ytterligare krav är att det ska vara relevant som bevis för ett brott och, vad gäller beslag, att det är nödvändigt för att bevismaterialet, enligt ovan, inte ska gå förlorat. Eftersom det material som finns tillgängligt direkt på en dator som finns på platsen för husrannsakan omfattas av sec. 19(3) PACE kan det konstateras att sec. 19(4) PACE är särskilt avsedd för situationer då materialet finns externt lagrad.[191] Med denna bestämmelse har brottsbekämpande myndigheter möjlighet att autonomt efterforska och beslagta bevis lagrade i utlandet, oavsett om motstående stat har identifierats, förutsatt att det är tillgängligt från platsen för husrannsakan.[192]

I Tyskland omfattas utforskandet av datorsystem och beslag av digitalt material av de traditionella straffprocessuella reglerna kring husrannsakan, sec. 98(1) & sec. 105(1) StPO. Särskilda bestämmelser som tillåter att myndigheter i ett senare skede utforskar datorsystem de kommit över via traditionell husrannsakan har dock införts, sec. 110(3) StPO. Efterforskandet kan ske via myndighetens egna datorer. Skulle ett datorsystem ge åtkomst till separata datorsystem och digitalt material inom en annan stat kan myndigheten utforska, ladda ner eller kopiera även dessa, förutsatt att det föreligger en risk att materialet går förlorat och att det är av betydelse för utredningen. Det bör uppmärksammas att rättslig hjälp i första hand ska tillämpas om materialets geografiska position kan bestämmas, något som i praktiken kan vara svårt att göra på förhand.[193] Här kan konstateras att lagstiftningen uttryckligen tillåter autonom insamling av digitalt lagrat bevismaterial när motstående stat inte kan identifieras, men att rättslig hjälp i annat fall ska vidtas.

[190] Gillespie (2019), s. 332.
[191] Gillespie (2019), s. 332 f.
[192] Poullet m.fl. (2011), s. 404.
[193] Se ovan resonemang om belgisk lagstiftning samt avsnitt 2.3.

I kölvattnet av Playpen-fallen höjdes röster för att utvidga amerikanska myndigheters möjligheter att vidta straffprocessuella tvångsmedel i den digitala sfären.[194] Genom en ändring av Rule 41 FRCP infördes möjligheten för domare att fatta beslut om efterforskande och beslag av digitalt material lagrat på datorsystem. Enligt bestämmelsen kan åtgärden vidtas på distans. Husrannsakan kan avse datorsystem både inom och utom den brottsbekämpande myndighetens distrikt. Vidare kan husrannsakan nyttjas för att få åtkomst till material vars geografiska position har dolts med teknologiska hjälpmedel. Således tillåts även insamling av digitalt bevismaterial som finns lagrat i en annan stat, förutsatt att lokalisering omöjliggjorts genom teknologiska hjälpmedel.[195] Kritik riktades mot ändringen av bestämmelsen. Särskilt framhölls att en kortsiktig effektivisering av nationell brottsbekämpning skedde på bekostnad av långsiktiga internationella relationer.[196]

Portugal har infört särlagstiftning som innebär ett klart avsteg från Lotusprincipen. Lagstiftningen är framför allt avsedd att verka som ett led i att hantera de lokaliseringsproblem som har uppstått i takt med att molntjänster och darkweb används i ökad utsträckning.[197] Genom art. 25 PCL tillåts andra stater att genom datorsystem lokaliserade inom deras territorium efterforska och samla in digitala bevis som finns lagrade på servrar inom portugisiskt territorium om ägaren av materialet eller datorsystemet har samtyckt. Bestämmelsen är ett inkorporerande av art. 32 b CoCC och kan inte anses folkrättsligt kontroversiell eftersom den är en frivillig inskränkning av den egna statssuveräniteten. Mer intressant är utvidgandet av de traditionella straffprocessuella reglerna om tvångsmedel. Enligt art. 15(5) PCL kan brottsbekämpande myndigheter vid undersökning av ett datorsystem i Portugal utvidga efterforskandet till ett externt datorsystem som finns tillgängligt via den första datorn. Det här möjliggör exempelvis genomsökandet av e-post-meddelanden lagrade i en webmailtjänst. Bestämmelsen är oberoende av den fysiska positionen av det material som efterforskas och samlas in.[198] Således kan portugisiska brottsbekämpande myndigheter autonomt bereda sig åtkomst till datorsystem belägna i andra stater oavsett om motstående stat har identifierats. Enligt en rapport från portugisiska åklagarmyndighetens avdelning för IT-brott har bestämmelsen kommit att användas i stor utsträckning. Den har haft en särskilt stor effekt i de fall brottsbekämpande myndigheter behöver agera fort för att säkra bevisning. Det lyfts också fram att viss typ av material som tidigare varit helt oåtkomlig numera kan samlas in som bevis.[199]

[194] Pilkington (2014) under “Elektroniska källor”; se avsnitt 4.4.2.
[195] Se avsnitt 2.3.
[196] Reitman (2016) under “Elektroniska källor”.
[197] Verdelho (2019), s. 139 f.
[198] Ibid., s. 142.
[199] Ibid., s. 143.

4.5 Det svenska förhållningssättet

4.5.1 Beslagsutredningen

Även i Sverige har problematiken avseende brottsbekämpande myndigheters möjligheter att efterforska och samla in digitalt material lagrat i utlandet väckt uppmärksamhet. Frågan hanterades särskilt i en offentlig utredning från år 2017. För att besvara uppsatsens tredje frågeställning krävs en redogörelse för relevanta delar av det förslag som presenterats i utredningen. I syfte att utvärdera förslaget följer också en sammanfattning av yttranden från remissinstanser med inriktning på brottsbekämpning.

För att anpassa de regler om beslag och husrannsakan, som inte ändrats sedan 1940-talet, till det exponentiellt ökande användandet av digitala verktyg, som datorer och mobiltelefoner, beslutade regeringen år 2016 att tillsätta en sakkunnig och ett flertal experter för att genomföra en offentlig utredning.[200]

Utredningen framhöll initialt att datorer och mobiltelefoner ofta används under förberedelse och genomförande av brott. Således har tvångsmedel som utformats i en huvudsakligen icke-digitaliserad värld applicerats på IT-miljöer.[201] Reglerna har varit utformade för att hantera en fysisk värld, men det faktum att digital information har funnits lagrad på fysiska föremål har möjliggjort att bestämmelserna trots allt har kunnat tillämpas. Målsättningen för uppdraget var att optimera förutsättningarna för brottsbekämpande myndigheter att driva effektiva men rättssäkra förundersökningar. Uppdraget innefattade uttryckligen målsättningen att ”anpassa bestämmelserna om beslag och husrannsakan till modern teknik och ta ställning till om kopiering av beslagtaget material bör regleras”. Som en allmän utgångspunkt hölls att bevarandet av allmänhetens förtroende för rättsväsendet förutsätter att straffprocessuella regler är anpassade till modern teknik.[202] Ur ett effektivitetsperspektiv konstaterades att brottsbekämpande myndigheter måste ha möjlighet att tillgodogöra sig elektroniskt lagrad information och att regelverket är lättillämpat.[203]

Ett delavsnitt av utredning tog särskilt sikte på problematiken med statssuveränitet och territoriella begränsningar av exekutiv jurisdiktion. Utredningen konstaterade att den svenska inställningen har varit att folkrätten förbjuder brottsbekämpande myndigheter att med teknologiska hjälpmedel autonomt

[200] Dir. 2016:20, s. 1; SOU 2017:100, s. 3 & 27.
[201] SOU 2017:100, s. 27.
[202] Ibid., s. 28.
[203] Ibid., s. 29.

efterforska och samla in digitalt material lagrat i ett annat land.[204] Det konstaterades också att denna syn har gjort det svårt för brottsbekämpande myndigheter att tillgodogöra sig central bevisning även i fall då brottet som utreds har begåtts av svenska medborgare i Sverige. De brottsbekämpande myndigheterna har saknat exekutiv jurisdiktion.[205]

Utredningen redogör vidare för olika tolkningar av territorialitet när det kommer till insamling av digitalt bevismaterial. Bland annat framhålls Danmark som ett exempel där alternativa anknytningsgrunder, andra grunder för jurisdiktion, genom praxis har applicerats på förfarandet.[206] Här poängteras också att det inte förekommit några rättsliga savgöranden i Sverige som resonerar kring problematiken med information lagrad i utlandet, men att alternativa anknytningspunkter bör utforskas.[207] Den traditionella synen på jurisdiktion ifrågasätts mot bakgrund av att ny teknik försvårar eller omöjliggör att materialets geografiska position kan bestämmas. Särskilt diskuteras molntjänster och att en användare avsiktligen kan välja att förvara material på en server inom en annan stats territorium.[208]

Slutligen ansåg utredarna att det krävdes en förändring av den traditionella synen på territorialitet vid transnationell insamling av digitalt lagrade bevis.[209] En särskild anledning till detta var den utveckling som skett i nationell rätt runtom i världen, men särskilt poängterades att de ändringar som föreslogs för att anpassa bestämmelserna om beslag och husrannsakan till en modern värld riskerade att få en begränsad verkan till följd av de territoriella restriktionerna. Det konstaterades sammanfattningsvis att förändringen borde ske genom utveckling av praxis och att den inte lämpade sig för lagstiftning.[210]

4.5.2 Tillhörande remissyttranden

I ett remissvar från Polismyndigheten framhölls en positiv inställning till en ändrad syn på tolkningen av exekutiv jurisdiktion och statssuveränitet. Den brottsbekämpande verksamheten skulle, enligt polisen, effektiviseras avsevärt om det fanns en möjlighet att bereda sig åtkomst till digitala bevis lagrade i en annan stat.[211] Farhågor lyftes dock kring förslaget att låta en förändring

[204] SOU 2017:100, s. 362 f.; se avsnitt 4.2.3.
[205] SOU 2017:100, s. 363.
[206] Ibid., s. 373 f.
[207] Ibid., s. 374.
[208] Ibid., s. 376; se avsnitt 2.2 och 2.3.1.
[209] SOU 2017:100, s. 374 f.
[210] Ibid., s. 375.
[211] Polismyndighetens remissyttrande, s. 1.

ske genom praxis. Enligt Polismyndigheten skulle det innebära en beaktansvärd risk för att tillämpningen av förslaget skulle bli begränsad utan tydligt lagstadgade riktlinjer. Det har, likt utredningen underströk, inte förekommit några rättsliga avgöranden och utsikten för när det skulle kunna ske är oklar. För Polismyndigheten skulle det innebära stora negativa konsekvenser för den brottsbekämpande verksamheten. I utevaro av lagstiftning efterfrågades åtminstone klara förslag på alternativa anknytningspunkter för jurisdiktion som skulle kunna ligga till grund för ett eventuellt rättsligt avgörande.[212]

Polisförbundet ställde sig positivt till utredningens förslag om ändring av inställning till exekutiv jurisdiktion. Det ställde sig dock tveksamt till utredningens ställningstagande om att förslaget om en ändrad syn inte var lämpat för lagstiftning. Enligt Polisförbundet är frågan komplex varför den ur rättssäkerhetssynpunkt bör regleras i lag.[213]

Åklagarmyndigheten angav i ett yttrande att frågan om exekutiv jurisdiktion vid insamling av digitalt material lagrat i utlandet eller vars geografiska position inte kan bestämmas bör regleras i lag. I den senare situationen konstaterades särskilt att åklagare inte på förhand kan veta om en undersökningsåtgärd är lagenlig. Att överlåta uppgiften att utveckla alternativa anknytningspunkter till rättspraxis skulle, enligt Åklagarmyndigheten, vara problematiskt bland annat eftersom det ansågs oklart i vilken utsträckning en sådan rättslig prövning skulle kunna ske.[214]

Ekobrottsmyndigheten förhöll sig positiv till en förändrad inställning till den traditionella synen på exekutiv jurisdiktion i situationer då digitalt material är lagrat i ett annat land. Särskilt poängterades att vissa brott i nuläget inte kan utredas överhuvudtaget eftersom en framställan om rättslig hjälp förutsätter att den motstående staten identifieras, vilket i vissa fall inte låter sig göras. Även Ekobrottsmyndigheten ansåg att lagstiftning borde införas, särskilt rörande situationer då det digitala materialets position inte kan bestämmas.[215]

[212] Polismyndighetens remissyttrande, s. 1.
[213] Polisförbundets remissyttrande, s. 2.
[214] Åklagarmyndighetens remissyttrande, s. 3.
[215] Ekobrottsmyndighetens remissyttrande, s. 1.

5 Rätten att samla in digitala bevis

5.1 Insamling när bevismaterialet kan lokaliseras

Uppsatsens frågeställningar kommer i detta kapitel besvaras enligt den ordning de är ställda. Avsikten med de två inledande frågeställningarna är att fastställa gällande rätt genom att analysera det som framgått av relevanta rättskällor. Den tredje frågeställningen besvaras genom en argumentation kring motstående intressen för att nå en slutsats om huruvida specifik lag bör stiftas som tillåter transnationell insamling av digitala bevis. Första avsnittet kommer hantera frågan om svenska myndigheters möjligheter att autonomt samla in digitalt bevismaterial lagrat inom en annan stats territorium. Grundfrågan kan brytas ned i två delfrågor: (1) tillåter svensk rätt insamling av digitala bevis och (2) är det förenligt med folkrätten att samla in digitala bevis som är lagrade inom en annan stats territorium?

Det måste initialt utredas huruvida svensk lagstiftning överhuvudtaget tillåter att brottsbekämpande myndigheter samlar in digitala bevis. Det bör observeras att relevant straffprocessuell lagstiftning utformades för att vara anpassad till en analog värld och att IT-miljöer således kan vara svåra att hantera. För att exemplifiera stadgar 27 kap. 1 § RB att föremål kan tas i beslag. Mot bakgrund av legalitetsprincipens krav på att bestämmelser inte får tillämpas på situationer som faller utom en strikt tolkning av ordalydelsen kan det ifrågasättas huruvida digitalt bevismaterial faller inom ramen för begreppet ”föremål”. Typiskt sett avser begreppet fysiska ting. Visserligen kan hävdas att all materia, även elektroniska signaler, har en fysisk form, men det framstår som osannolikt att lagstiftarens avsikt var begreppet skulle omfatta annat än dess typiska betydelse. Ett annat exempel kan illusteraras genom att betrakta 28 kap. 1 § RB om husrannsakan. Enligt bestämmelsen ska ett beslut om husrannsakan avse hus, rum eller annat slutet förvaringsställe. Med samma resonemang kan det inte sägas vara självklart att ett genomsökande av det materiella innehållet i ett datorsystem omfattas av ordalydelsen. Det begrepp som närmast träffar ett datorsystem är ”annat slutet förvaringsställe”. Ett datorsystem fungerar visserligen som ett utrymme i vilket användaren förvarar elektroniskt material, men om åtkomsten inte kräver ett lösenord kan det ifrågasättas om det är slutet. Därtill är den typiska betydelsen för ordet ”ställe” en plats eller en position.

Med beaktande av doktrin och att insamling av digitala bevis regelbundet sker i praktiken tycks det emellertid vara klarlagt att tvångsmedlen går att applicera på digitalt lagrat bevismaterial. Att förfarandet är förenligt med gällande rätt stöds även av uttalanden från JO och JK.[216] Det kan ifrågasättas huruvida det är lämpligt att dessa källor, istället för uttrycklig lag, ska stadga tvångsmedlens omfattning. Doktrin och praxis kan med lätthet förändras vilket kan bidra till en oförutsebarhet. Detta till trots kan alltså brottsbekämpande myndigheter, inom ramen för en förundersökning, samla in digitalt bevismaterial enligt bestämmelserna om husrannsakan och beslag, även om det inte nödvändigtvis följer direkt av ordalydelsen. Det bör dock poängteras att vidtagande av tvångsmedel är en inskränkning av den enskildes grundlagsskyddade rättigheter varför vissa grundläggande principer, såsom proportionalitets- och ändamålsprincipen, ska respekteras.

I ett andra steg ska en slutsats dras om huruvida digitalt material som finns lagrat inom en annan stats territorium kan samlas in med ett autonomt förfarande (utan samtycke från motstående stat). Frågan rör omfånget av den exekutiva jurisdiktionen – ett begrepp för åtgärder som vidtas av stater i syfte att verkställa beslut som fattats av domstol eller rättskipande myndigheter. Den traditionella syn som länge har dominerat området gavs uttryck för i Lotus-fallet och gav upphov till Lotus-principen. Den internationella mellanfolkliga domstolen slog fast att ingen makt får utövas inom en annan stats territorium i utevaro av en specifik regel som tillåter det. Resonemanget bottnar i principen om alla staters likställdhet och suveränitet, som bland annat följer av FN-stadgan.

En parentes som bör nämnas är att det går att ifrågasätta insamling av digitalt bevismaterial lagrat i en annan stat överhuvudtaget kan betraktas som en transnationell exekutiv åtgärd. Brottsbekämpande myndigheter har teknologi som tillåter att material samlas in på distans, utan att någon yttre gräns överträds. Digitala bevis har inte heller en fysisk karaktär som går att likställa med andra typer av bevis. Trots detta är det tydligt att relevanta auktoriteter är av uppfattningen att beteendet faktiskt utgör en exekutiv åtgärd på annan stats territorium. Detta styrks av granskad praxis och av myndigheternas uppgifter i FN:s enkätstudie.[217] Visst stöd följer också av avgörandet i Arrest Warrant-fallet, enligt vilket endast utfärdandet av en arresteringsorder var en otillåten exekutiv åtgärd. Således får uppfattningen anses accepterad.

I takt med den digitala utvecklingen har brottsbekämpande myndigheters arbete med insamling av bevismaterial utmanats. Modern teknologi tillåter att

[216] Se avsnitt 3.3.
[217] Se avsnitt 4.2.2.

digitala bevis med lätthet kan lagras i en annan stat än den där brottet begicks. Det kan också förstöras, modifieras eller flyttas till en tredje stats territorium inom loppet av ett fåtal knapptryck. Av uppenbara skäl ställer det till med problem mot bakgrund av den traditionella synen på exekutiv jurisdiktion. För att samla in bevismaterial utan att strida mot Lotus-principen har internationell rättslig hjälp tidigare nyttjats regelbundet. Förfarandet är emellertid präglat av ineffektivitet vilket i praktiken har inneburit att stater ofta helt har avstått från att samla in bevis.[218] Försök har gjorts, exempelvis genom EUO, att utveckla effektivare metoder för mellanstatlig hjälp utan att förändra den traditionella synen på exekutiv jurisdiktion. Sådana försök har dock inte hindrat alternativa lösningar som utmanat Lotus-principen från att träda fram. Resterande analys kommer därför klargöra huruvida det kan ha skett en förändring av gällande folkrätt som tillåter en gränsöverskridande autonom insamling av digitala bevis.

Gällande rätt kan exempelvis förändras genom att stater ratificerar internationella multilaterala överenskommelser. Den enda som berör det aktuella juridiska problemet på ett relevant sätt är CoCC som har ratificerats av 65 stater. Avtal har härigenom slutits om att till viss del, om än begränsad, inskränka statssuveräniteten. Konventionens art. 32 b tillåter att brottsbekämpande myndigheter, med legalt och frivilligt samtycke från den som har rätt till det berörda materialet, samlar in digitala bevis även om dess geografiska position är i en motstående stat. I en rapport tillhörande konventionen angavs att en sådan handling stred mot Lotus-principen, men inga av de stater som har ratificerat konventionen har gjort förbehåll eller reservationer avseende bestämmelsen. Det bör dock uppmärksammas att Sverige inte har ratificerat CoCC. Med andra ord kan svenska myndigheter inte hänvisa till någon konvention som stöd för att autonomt samla in digitala bevis lagrade inom en annan stat.

Folkrätten kan även förändras genom att internationell sedvanerätt bildas. Denna rättskälla är bindande för alla stater som inte ihärdigt motsätter sig den. För att ett beteende ska betraktas som internationell sedvanerätt krävs följande: (1) att det finns en allmän och enhetlig praxis stater emellan och (2) att denna praxis av staterna anses vara förpliktigande. Därtill måste vikten av den regel som är föremål för förändring beaktas. I det här fallet rör det den väletablerade Lotus-principen som förbjuder all myndighetsutövning inom en annan stats territorium. Således måste ny statspraxis sannolikt vara väl utspridd samt präglas av en hög kontinuitet och enhetlighet för att anses etablerad. Det ska också poängteras att särskilt höga krav ställs på statspraxis som innebär en inskränkning av statssuveräniteten.

[218] Se avsnitt 4.3.

Något som initialt kan slås fast är att material som faller under begreppet ”open source” kan samlas in autonomt och utan beaktande av territorium. Av det granskade materialet att döma kan detta kategoriseras som etablerad internationell sedvanerätt. Det har bland annat förklarats i ovan nämda CoCC-rapport och uppfattningen får återkommande stöd i doktrin. Innebörden är att material som finns tillgängligt via vilken webbläsare som helst, utan skydd av exempelvis lösenord, fritt kan samlas in. En betraktelse som kan lyftas fram här är att stater tycks ha frångått den strikt hållna Lotus-principen av praktiska skäl. Den enda logiska förklaringen är att det anses orimligt att brottsbekämpande myndigheter inte ska kunna bereda sig åtkomst till material som är tillgängligt för vilken enskild som helst. Vad gäller material som inte träffas av begreppet måste ytterligare diskussion föras.

Som framgår av de avsnitt som avser nationell lagstiftning och praxis är det uppenbart att ny statspraxis ha börjat ta form även avseende material som inte kan kategoriseras som open source.[219] Danmark har genom praxis etablerat ett nytt förhållningssätt enligt vilket transnationell insamling av digitala bevis i stor omfattning kan ske autonomt, oberoende av var materialet är lagrat. Enligt Højesteret var det tillräckligt att det lösenordsskyddade materialet var tillgängligt från vilken dator som helst och att den brottsbekämpande myndigheten inte var i behov av någon annan stats bistånd. Detta förhållningssätt innebär ett tvärt avsteg från Lotus-principen eftersom nästan allt material tillgängligt via internet passar kriterierna. Särskilt mot bakgrund av brottsbekämpande myndigheters teknologiska resurser.

Även Belgien har anlagt ett alternativt förhållningssätt till exekutiv jurisdiktion. I Yahoo!-fallet konstaterades att materialets geografiska position inte var av relevans. Var det aktuella brottet hade begåtts blev istället avgörande för frågan om belgiska myndigheter kunde begära att vissa e-post-meddelanden lämnades ut. Vidare tillåter belgisk lagstiftning, enligt art. 39bis CIC, att bevismaterial samlas in i de fall då ett beslagtaget datorsystem på belgiskt territorium ger åtkomst till ett annat datorsystem, oavsett var det senare är beläget. Detta förutsätter att det finns en risk att materialet kan gå förlorat samt att en domare har fattat beslut om förfarandet. Lagstiftningen kan inte anses förenlig med Lotus-principen.

Portugal och delar av Storbritannien har också infört lagstiftning som utmanar den traditionella synen på exekutiv jurisdiktion. Straffprocessuella regler i England och Wales, sec. 19(4) PACE, tillåter att bevismaterial lagrat i en annan stat samlas in autonomt under vissa förutsättningar. Dels ska materialet finnas tillgängligt via ett datorsystem som är objekt för husrannsakan, dels

[219] Se avsnitt 4.4.2 och 4.4.3.

ska materialet kunna tas med i läsbar eller synlig form. Även här ska hänsyn tas till om materialet i fråga riskerar att förvanskas, försvinna eller förstöras. Eftersom digitala bevis, som ovan nämnt, lätt kan modifieras, flyttas eller raderas får bestämmelsen ett brett omfång. Portugisiska myndigheter kan också samla in digitala bevis lagrade inom en annan stats territorium förutsatt att det görs från ett datorsystem som är föremål för straffprocessuella tvångsmedel i Portugal, art. 15(5) PCL. De brottsbekämpande myndigheterna framhåller i en rapport att bestämmelsen används i stor utsträckning och att den får särskild effekt när de måste agera fort för att säkra bevisning. Även här är det tydligt att lagstiftningen är oförenlig med Lotus-principen.

Ytterligare stöd för en förändring av mellanstatlig praxis går att finna i en FN-rapport.[220] Här uppgav brottsbekämpande myndigheter att transnationell insamling av digitala bevis regelbundet sker i praktiken, utan att samtycke söks hos motstående stat. Något som dock står klart är att det inte finns en enhetlighet i det exakta utformandet av denna nya statspraxis, mer än att den innebär ett klart avsteg från Lotus-principen.

Det förekommer också nationell lagstiftning som endast delvis strider mot Lotus-principen, men som håller sig inom dess ramar när en motstående stat kan identifieras. Enligt den federala lagstiftning som modifierades efter Playpen-fallet, Rule 41 FRCP, tillåts efterforskning och insamling av digitala bevis endast om motstående stat inte kan identifieras till följd av att dess position avsiktligen har dolts med hjälp av teknologiska verktyg. Ett liknande förhållningssätt följer av det tyska straffprocessuella regelverket, 110(3) StPO, enligt vilket internationell rättslig hjälp ska vidtas i första hand om det går att klargöra vilken den motstående staten är. Reglernas utformning antyder att Lotus-principen fortfarande beaktas när en motstående stat kan identifieras.

Mot bakgrund av det anförda står det klart att det finns indikationer på en förskjutning av statspraxis, samtidigt som kraven för att ny internationell sedvanerätt ska anses etablerad inte kan sägas vara uppfyllda. Både Lotus-principens tyngd och det faktum att den nya sedvanerättsliga regeln innebär en inskränkning av statssuveräniteten måste beaktas. Under sådana förutsättningar fordras en särskilt utpräglad enhetlighet och kontinuitet i den nya statspraxisen. Det finns visserligen ett flertal exempel på stater som frångått Lotus-principen, men det kan ifrågasättas huruvida tillräckligt många har gjort det. Det kan också konstateras att det varken föreligger kontinuitet eller enhetlighet i utformandet av denna nya praxis. Nationell lagstiftning och praxis har utformats på olika sätt i nästan alla granskade fall. Det första kravet för ny internationell sedvanerätt kan således inte anses vara uppfyllt.

[220] Se avsnitt 4.2.2.

Trots att kravet på en allmän och enhetlig praxis med kontinuitet inte är uppfyllt ska det andra kravet för etablerad internationell sedvanerätt behandlas kortfattat. Staterna måste vara av den subjektiva uppfattningen att praxisen är bindande. Konstaterandet av att det första kravet inte är uppfyllt innebär visserligen att det inte finns en specifik praxis att förhålla sig till, men det är av intresse att utreda staternas inställning till att frångå Lotus-principen.

Majoriteten av de brottsbekämpande myndigheterna anförde i en FN-rapport att de ansåg att den stat där det digitala materialet fanns lagrat hade exklusiv jurisdiktion över det.[221] Uppfattningen av rättsläget ligger i linje med det som följer av Lotus-principen, vilket kan anses talande för att kravet på en subjektiv uppfattning av statspraxis som bindande inte är uppfyllt. Något som ger ytterligare stöd för detta är ett uttalande från en rapport tillhörande CoCC.[222] Enligt rapporten är konventionens art. 32 b att se som en inskränkning av principen om territorialitet och statssuveränitet. Bestämmelsen rör myndigheters möjlighet att gå direkt till den som har rätt till materialet för att med dennes legala och frivilliga samtycke få det utlämnat, även om materialet är lagrat i en annan stat. Bestämmelsen utgör ett förhållandevis blygsamt utökande av den exekutiva jurisdiktionen, men anses alltjämt innebära en inskränkning av statssuveräniteten. Mot bakgrund av detta kan slutsatsen dras att fullständigt autonom insamling av digitala bevis lagrade i en annan stat betraktas som folkrättsstridigt av medlemsstaterna. Medlemsstaterna har inte heller försökt införa nya bestämmelser som ytterligare inskränker statssuveräniteten. Sammantaget tycks det inte finnas en subjektiv uppfattning hos staterna som innebär att ett frånsteg från Lotus-principen är bindande.

Doktrin faller under övriga behandlade rättskällor i hierarkin och kan inte ensamt anses ligga till grund för att slå fast gällande rätt. Vid en granskning av den framträder inte heller något som ger stöd för att gällande rätt har förändrats. Det förekommer emellertid två olika uppfattningar kring frågan om exekutiv jurisdiktion och statssuveränitet vid insamling av digitala bevis. Den första är en strikt tolkning av Lotus-principen som förbjuder all myndighetsutövning på en annan stats territorium. Enligt detta synsätt kan digitalt lagrat bevismaterial aldrig samlas in autonomt om det finns beläget i en annan stat.

Den andra är ett alternativt förhållningssätt de lege ferenda som tar sikte på huruvida efterforskning och insamling av bevis resulterar i skada på digital infrastruktur i motstående stat. Förhållningssättet kan delas upp i två tolkningar. Den första tolkningen är att förfarandet endast utgör en kränkning om

[221] Se avsnitt 4.2.2.
[222] Se avsnitt 4.4.1.1.

det leder till skador som inte är av mindre karaktär. Den andra tolkningen är att förfarandet utgör en kränkning enbart i de fall då skador uppstår på digital infrastruktur som åtnjuter statlig immunitet, exempelvis servrar tillhörande statsmakten. Vid den granskning som har gjorts har inget ytterligare stöd funnits för att dessa tolkningar har vunnit inflytande över staters uppfattning av rättsläget eller agerande i praktiken.

Sammanfattningsvis kan konstateras att svenska brottsbekämpande myndigheter, enligt svensk rätt, kan samla in digitala bevis. Under förutsättning att materialet faller under begreppet ”open source” är det också förenligt med folkrätten att insamling sker autonomt trots att det är lagrat i utlandet. För andra typer av digitala bevis utgör Lotus-principen dock fortfarande gällande rätt. All annan autonom insamling av digitala bevis lagrade i en identifierad motstående stat utgör därmed en suveränitetskränkning

5.2 Insamling när bevismaterialet inte kan lokaliseras

Den moderna teknologi som tillåter att digitalt material kan lagras på flera platser samtidigt eller att materialets position omöjligen kan bestämmas ställer särskilda krav på brottsbekämpande myndigheter. Mot bakgrund av detta ska ställning tas till om svenska brottsbekämpande myndigheter kan samla in sådant material på ett sätt som är förenligt med gällande rätt. Även här kan grundfrågan behandlas som två delfrågor: (1) finns det lagstöd i svensk rätt som tillåter insamling av digitala bevis och (2) är det förenligt med folkrätten att samla in digitalt bevismaterial vars fysiska position inte kan bestämmas? Den första delfrågan har besvarats i föregående avsnitt. Det konstaterades att digitala bevis faller under tillämpningsområdet för bestämmelserna om husrannsakan och beslag samt att de grundläggande principer som avser skydda den enskilde ska beaktas. Således kommer detta avsnitt särskilt behandla den andra delfrågan.

Den folkrättsliga utgångspunkten är densamma. Som följer av Lotus-principen har all myndighetsutövning som vidtagits inom en annan stats territorium ansetts utgöra en kränkning av statssuveräniteten. Stater har därför haft att nyttja det folkrättsliga instrument som möjliggör insamling av sådant bevismaterial – internationell rättslig hjälp.[223] Den anmodande myndigheten har genom förfarandet kontaktat relevant auktoritet i motstående stat i hopp om att den senare samlar in det aktuella materialet för att sedermera skicka det till förstnämnda stat.

[223] Se avsnitt 4.3.

Rättslig hjälp har kritiserats för att vara ineffektivt eftersom motstående stat kan sakna samarbetsvilja eller resurser. Det kan också förekomma kommunikationsbrister som leder till ett utdraget förfarande. Särskild ineffektivitet framträder när det avsedda digitala bevismaterialet inte kan lokaliseras. I den situationen finns det ingen motstående stat som en förfrågan om rättslig hjälp kan skickas till. Vid en strikt tillämpning av Lotus-principen kan sådant material aldrig samlas in. Molntjänster och anonymitetsverktyg såsom Tor har försatt stater i en situation där de står handfallna om de respekterar Lotus-principen. Skulle en myndighet välja att samla in ett digitalt bevis trots att dess position inte kan bestämmas, kan det i ett senare skede visa sig att den har begått en suveränitetskränkning. För att illustrera kan läsaren föreställa sig att svenska myndigheter beslagtar ett informationsdokument tillgängligt via ett datorsystem som är föremål för husrannsakan. Datorsystemet har givit direkt tillgång till en annars lösenordsskyddad darkweb-hemsida där informationsdokumentet är uppladdat. Det föreligger alltid en risk för att digitalt material modifieras eller förstörs varför myndigheten inte kan invänta en resurskrävande spårning av relay-servrar som potentiellt, men inte garanterat, kan lokalisera webbsidans server. Utredningen fortlöper och slutligen kommer myndigheten över information som visar att servern är belägen i Ryssland, vilket innebär att myndigheten, enligt Lotus-principen, har kränkt rysk statssuveränitet.

Problematiken med att lokalisera material har särskilt bidragit till att stater har försökt skapa alternativa lösningar för att effektivisera brottsbekämpningen. Den enda konvention som tar sikte på problematiken är CoCC som genom art. 32 b tillåter att brottsbekämpande myndigheter samlar in bevismaterial beläget inom en annan stats territorium om den som har rätt till materialet har lämnat sitt frivilliga samtycke. Insamlingen enligt bestämmelsen förutsätter dock att den som avses kan identifieras och att denne är samarbetsvillig – vilket ofta kan uteslutas när vederbörande nyttjar anonymitetstjänster.[224] I vissa fall kan bestämmelsen dock vara av nytta. Molntjänster kan göra det svårt att lokalisera en specifik webbmails geografiska position. I sådana fall kan serverleverantören, exempelvis Yahoo!, kontaktas i hopp om att material kan lämnas ut. Serverleverantörer är dock måna om sitt rykte gentemot konsumenter och är inte nödvändigtvis samarbetsvilliga.[225] Även här ska uppmärksammas att Sverige inte har ratificerat konventionen, varför den inte kan ligga till grund för att rättfärdiga en sådan åtgärd.

I utevaro av internationella överenskommelser som reglerar området blir det återigen avgörande att ta ställning till huruvida internationell sedvanerätt kan

[224] Se exempel under avsnitt 4.1.1.
[225] Se exempelvis 4.4.1.

anses ha genomgått en förändring. Som ovan konstaterats förutsätts att (1) en allmän och enhetlig praxis har utvecklats och att (2) staterna uppfattar denna praxis som bindande. Kraven på kontinuitet och enhetlighet är också större när den regel som är föremål för förändring är central och om den nya regeln innebär en inskränkning av statssuveräniteten. Lotus-principens omfattande inflytande på området måste därför beaktas.

Som följer av föregående avsnitt betraktas material som faller under begreppet open source som tillgängligt för insamling oavsett vem som samlar in och var det sker. Att samla in open source-material borde emellertid strida mot Lotus-principen vid en tillämpning av samma strikta tolkning som har varit gällande i övrigt. Som anförts ovan tycks stater här ha kommit överens om att det är praktiskt ohållbart att myndigheter inte snabbt och lätt kan tillskansa sig digitala bevis som alla andra internetanvändare har tillgång till via en sökmotor. Det framstår under dessa förhållanden som anmärkningsvärt att ingen liknande överenskommelse har nåtts avseende material som inte kan lokaliseras, men vid en granskning av rapporter och doktrin förefaller ingen sådan existera.

Vid en överblick av det studerade materialet tycks dock en förändring ha skett i statspraxis. Enligt uppgifter från brottsbekämpande myndigheter i en FN-rapport förekommer regelbunden insamling av digitalt material utan samtycke i praktiken.[226] De begränsade folkrättsliga förutsättningarna har också lett till utmanande nationell lagstiftning och praxis.

I Playpen-fallet aktualiserades problematiken särskilt. En barnpornografihemsida hade upprättats på darkweb genom nyttjande av Tor-nätverket.[227] Anonymitetsverktyget omöjliggjorde att användarna som publicerade material på hemsidan kunde spåras och identifieras. För att komma runt problemet planterade amerikanska brottsbekämpande myndigheter ett malware som infiltrerade användarnas datorsystem och efterhand rapporterade information som kunde användas för att gripa och åtala ett flertal amerikanska medborgare. Bevisningen som lades fram avvisades på den grund att myndigheten inte hade kännedom om användarnas geografiska position när åtgärden vidtogs varför förfarandet ansågs oförenligt med folkrätten. Fallet ledde till stor uppståndelse och federal lagstiftning infördes för att motverka att liknande situationer skulle uppstå. Enligt Rule 41 FRCP kan domare numer besluta om efterforskande och beslag av digitala bevis som inte kan lokaliseras. Tillämpning av bestämmelsen förutsätter dock att materialets geografiska position har dolts med teknologiska hjälpmedel.

[226] Se avsnitt 4.2.2.
[227] Se avsnitt 2.3.2.

Övrig nationell lagstiftning som har studerats har också bidragit till bilden av att en förskjutning av statspraxis har skett för att hantera problemet. Utöver USA tillåter Belgien, Tyskland, England, Wales och Portugal att digitalt lagrad bevisning samlas in om dess geografiska position inte kan bestämmas. Den portugisiska lagstiftningen upprättades särskilt som ett led i att komma runt de problem som följer av molntjänster och darkweb. Även de rättsfall som presenterats bidrar till denna slutsats. Bland annat har Danmark, genom praxis från högsta instans, etablerat en rätt att under alla förhållanden samla in digitala bevis, förutsatt att inget transnationellt bistånd behövs.

Mot bakgrund av presenterad nationell lagstiftning och praxis är det klarlagt att en allmän praxis är under utveckling. Den kan också anses enhetlig på så sätt att den har inneburit ett frånsteg från en strikt tolkning av Lotus-principen. Ett karaktärsdrag som de flesta exempel har gemensamt vad gäller det praktiska utformandet av ny praxis är att åtkomst ska vara möjligt via ett initialt datorsystem som är objekt för husrannsakan inom statens territorium. Även det faktum att en viss utpekad auktoritet fattar beslut om ytterligare efterforskning är gemensamt. Det förekommer dock en bristande enhetlighet på andra punkter. Vissa stater, som England och Wales, tillåter all insamling av digitala bevis förutsatt att den riskerar att förstöras. Andra stater, som USA, tillåter endast insamling av digitala bevis om dess geografiska position aktivt har dolts genom teknologiska verktyg. Därtill kommer ytterligare variation i stater som Belgien, där motstående stat ska informeras i efterhand, och Portugal, som infört särlagstiftning utom ordinarie straffprocess. Som konstaterats ovan måste Lotus-principens centrala position beaktas vid en bedömning. Därtill inskränker ny praxis statssuveräniteten, varför kraven på enhetlighet och kontinuitet är särskilt stora. Vid en samlad bedömning uppfyller inte ny statspraxis den enhetlighet och kontinuitet som fordras.

Det är också svårt att dra en slutsats om staternas subjektiva uppfattning av nämnda praxis eventuellt bindande karaktär. Enligt CoE:s rapport anser brottsbekämpande myndigheter att all insamling av digitalt lagrad bevisning inom en annan stats territorium, med undantag för open source-material, utgör en inskränkning av statssuveräniteten. Det faktum att 60 stater har ratificerat CoCC som till viss del inskränker statssuveräniteten antyder dock att en sådan uppfattning finns. Vidare kan påpekas att omständigheterna gör att stater som inte är villiga att agera i strid med folkrätten står handfallna när digitalt material inte kan lokaliseras. En sådan utsatt position borde logiskt sett bidra till en önskan om ett förändrat läge. I brist på uppdaterade enkätstudier och mot bakgrund av övriga tillgängliga källor kan det inte konstateras att stater anser den statspraxis som är under utveckling vara bindande. Det finns

med andra ord inte tillräckligt mycket stöd för att den statspraxis som har växt fram ska kunna anses utgöra internationell sedvanerätt.

Även i detta avseende kan doktrin spela en roll för att få en uppfattning av rättsläget, men dess dignitet som rättskälla gör att den inte ensamt kan ligga till grund för att konstatera gällande rätt. Det finns ett utbrett stöd för att Lotus-principen fortfarande gäller, men även andra inställningar förekommer. Bland annat framhåller de Hert att ett snart 100 år gammalt rättsfall inte borde få ligga till grund för inställningen till de problem som uppstår i en digital värld. Enlig de Hert bör det kryphål som uppstått täppas till, eftersom brottslingar annars kan undvika lagföring genom att flytta, modifiera eller förstöra bevis. Denna uppfattning kan dock inte sägas vara enhetlig och vitt spridd. Som ovan nämnt kan den inte heller ligga till grund för en slutsats om gällande rätt.

Sammanfattningsvis kan konstateras att svenska brottsbekämpande myndigheter, enligt svensk rätt, kan samla in digitala bevis oavsett om dess position kan bestämmas. Skulle materialet emellertid visa sig ha varit beläget inom en motstående stats territorium har Sverige gjort sig skyldigt till en suveränitetskränkning.

5.3 Det svenska förhållningssättet – försiktighet eller effektivitet

De frågeställningar som har besvarats har kretsat kring att slå fast gällande rätt avseende två specifika juridiska problem. I detta avsnitt kommer den tredje frågeställningen besvaras. Den skiljer sig från de föregående på så sätt att den innebär en avvägning av motstående intressen som sedermera utmynnar i ett personligt ställningstagande. Mot bakgrund av det som framgått kring det folkrättsliga läget och vad som följer av Beslagsutredning med tillhörande remissyttrande dras en slutsats om huruvida Sverige bör införa särskild lagstiftning som tillåter insamling av digitala bevis lagrade inom en annan stats territorium, vilket också omfattar bevis som inte kan lokaliseras.

Vid första anblick kan ett antal slutsatser dras baserade på Beslagsutredningen och dess ställningstagande i frågan. De som bedrev utredningen hade till uppgift att ta fram förslag på hur den straffprocessuella regleringen kunde utformas för att bättre anpassas till den digitala världen.[228] En av utgångspunkterna berörde just frågan om exekutiv jurisdiktion och territorialitet. Således fanns en önskan från uppdragsgivaren (regeringen) att utveckla det svenska förhållningssättet. Det slogs fast att Sverige länge förhållit sig till den traditionella

[228] Se avsnitt 4.5.1.

syn på statssuveränitet och territorialitet som följer av Lotus-principen. Utredningen öppnade dock, med hänvisning till den utveckling som skett internationellt, upp för en förändring av den svenska inställningen till exekutiv jurisdiktion och territorialitet. Slutligen anfördes att uppgiften att förändra inställningen borde överlåtas till rättspraxis, men skälen härtill presenterades inte.

Inställningen präglas av en försiktighet med beaktande av att utredningen tidigare konstaterat att det inte fanns någon praxis från Högsta domstolen och att de få rättsfall från underinstanser som berörde området inte innehöll resonemang om frågan. Remissinstanserna påpekade också att när och hur frågan skulle dyka upp i praxis var oförutsägbart.[229] Polismyndigheten framhöll att det skulle förbli svårt att tillämpa nya riktlinjer om de inte stadgades tydligt i lag. Andra poängterade att frågan var för komplex för att överlåtas till rättspraxis och att lagstiftning var önskvärd särskilt avseende de fall då det digitala materialets position inte kunde bestämmas. Ekobrottsmyndigheten påpekade att vissa brott i nuläget inte kunde utredas överhuvudtaget och att övriga förslag om uppdaterad lagstiftning skulle förbli verkningslösa om territorialitetsfrågan inte klarlades. Det konstaterades också att internationell rättslig hjälp inte fungerade i praktiken. Att överlåta avgörandet till rättspraxis skulle, enligt nämnda remissinstanser, ha en stor negativ inverkan på den brottsbekämpande verksamheten ur ett effektivitetsperspektiv.

Alternativa tillvägagångssätt, såsom att ratificera CoCC, skulle vara ett steg i en effektiviserande riktning.[230] Art. 32 b CoCC tillåter visserligen direkt kontakt med den som har rätt till det digitalt lagrade materialet, men dennes samtycke är fortfarande avgörande för möjligheten att samla in det. Således är CoCC av begränsad nytta när den brottsbekämpande myndigheten snabbt behöver tillgodogöra sig digitalt bevismaterial. Sverige omfattas vidare av EUO som möjliggör utfärdandet av europeisk utredningsorder, men direktivet träffas också av den kritik som har riktats mot förfarandet om rättslig hjälp.[231] Art. 5 EUO föreskriver att förfrågan om utredningsåtgärd måste innehålla specifik information, bland annat om den brottsliga gärningen och om den som är föremål för åtgärden. Det finns utrymme för olika tolkningar av vad som ska betraktas som tillräckligt specifikt. Det ska också göras en proportionalitetsbedömning enligt art. 6 EUO som skulle kunna ge upphov till problem. Om den mottagande staten har anledning att anta att kriteriet inte är uppfyllt krävs ytterligare handläggning och kommunikation mellan staterna. Därtill kommer art. 12 EUO som föreskriver att stater har 90 dagar på sig att

[229] Se avsnitt 4.5.2.
[230] Se avsnitt 4.4.1.1.
[231] Se avsnitt 4.4.1.2.

besvara en förfrågan. Således är direktivet av begränsad nytta i de fall brottsbekämpande myndighet har ett behov av att snabbt kunna tillgodogöra sig digitalt bevismaterial. Vad gäller möjligheten att beslagta material som inte kan lokaliseras förblir EUO ett uddlöst verktyg.

Det kan således anses klarlagt att det finns uppenbara kortsiktiga fördelar med att lagstifta om en rätt att autonomt samla in digitala bevis oberoende av dess geografiska position, men när beslut fattas om reglering i lag är det viktigt att kontemplera eventuella konsekvenser som kan följa av dess utformning. Det kan eventuellt vara värt att låta effektiviteten i den brottsbekämpande verksamheten bli lidande för att undvika komplikationer. Denna kritik riktades exempelvis mot ändringen av Rule 41 FRCP som numer tillåter insamling av digitalt lagrad bevisning vars position dolts med anonymitetsverktyg. Bestämmelsens nya utformning kritiserades för att vara en kortsiktig effektivisering på bekostnad av långsiktiga internationella relationer.[232]

För att illustrera att det hela utgör en till synes svår avvägning mellan motstående intressen som mynnar ut i ett moraliskt ställningstagande kan argumentet genom ett hypotetiskt exempel dras till sin spets.

Den nya lagen skulle kunna effektivisera brottsbekämpningen så till den grad att ett visst antal barn skonas från brott såsom trafficking eller barnpornografibrott genom ökad möjlighet att utreda, lagföra och i förlängningen avskräcka från brott. Den skulle också kunna leda till att internationella relationer tar så mycket skada att krig utbryter. Om lika många barn omkommer i kriget som skonas från de nämnda brotten, var det i retrospektiv rätt att införa lagstiftningen? Svaret på denna filosofiska fråga är inte uppenbar och moraliska avvägningar hade sannolikt lett till vittspridda slutsatser, vilket hade motiverat den kritik som riktades mot Rule 41 FRCP. Väljer man däremot att beakta den empiri som finns tillgänglig blir svaret för de flesta sannolikt uppenbart. Av studien framkommer inget som tyder på att de länder som agerat i strid med Lotus-principen genom att lagstifta om en rätt att autonomt samla in digitala bevis lagrade inom en annan stats territorium har äventyrat internationella relationer – i synnerhet inte till den grad att risk för krig skulle föreligga.[233] Här ska beaktas att det förekommer ett stort antal exempel på sådan lagstiftning och att brottsbekämpande myndigheter angivit att förfarandet används regelbundet i praktiken. I ett sådant scenario är det svårt att föreställa sig andra potentiella konsekvenser som skulle vara allvarliga nog att motivera utebliven lagstiftning. Det bör också särskilt beaktas att portugisiska

[232] Se avsnitt 4.4.3.
[233] Se avsnitt 4.2.2 och 4.4.3.

myndigheter framhåller att sådan lagstiftning tillåter utredning av brott i situationer då det tidigare varit omöjligt. Även remissinstansernas inställning till Beslagsutredningen stödjer denna uppfattning.

Det finns ytterligare skäl som talar för att lagstiftning bör införas. Även här är internationell sedvanerätt särskilt intressant. Som framgår ovan ska ett objektivt och ett subjektivt rekvisit vara uppfyllt för att ett visst beteende ska anses utgöra etablerad internationell sedvanerätt.[234] Internationell sedvanerätt är under ständig förändring och präglas av staters beteenden och deras inställning till beteendet. Alla stater som inte ihärdigt motsätter sig utveckling inom internationell sedvanerätt anses vara bundna av den. Här finns utrymme för den svenska lagstiftaren att påverka pågående rättsutveckling genom att införa tydlig lagstiftning. På så sätt kan ett visst inflytande, om än begränsat, utövas över framtida rättsutveckling. Det finns med andra ord utrymme att agera för att den förändring som oundvikligen sker på området bär drag som är förenliga med de värderingar den svenska lagstiftaren värnar. Även detta skäl väger tungt mot bakgrund av att förfarandet i praktiken inte har lett till bakslag i form av bristande internationella relationer. Det ska också beaktas att en förändring av internationell sedvanerätt ofta förutsätter ett trotsande av en tidigare regel.

Sammanfattningsvis bör Sverige stifta lag som tillåter autonom insamling av digitala bevis. Lagstiftningen bör omfatta både den situation då materialet inte kan lokaliseras och den då det finns lagrat inom en annan stats territorium. Skälen härtill är att det skulle innebära en betydande effektivisering av den brottsbekämpande verksamheten, att det skulle ge den svenska lagstiftaren en möjlighet att påverka den internationella rättsutvecklingen och att det inte finns empiri som stödjer att det skulle leda till bristande internationella relationer.

[234] Se avsnitt 4.1.

6 Sammanfattande kommentarer

För att runda av uppsatsen följer här en summering av det som utkristalliserats vid besvarandet av uppsatsens frågeställningar enligt den ordning som etablerats ovan.

Målet med uppsatsens första frågeställning var att slå fast huruvida det är förenligt med gällande rätt att svenska myndigheter autonomt samlar in digitala bevismaterial inom motstående stats territorium. Det som framkommit är att svensk rätt inte innehåller något direkt hinder för ett sådant förfarande. Lagstiftningen är visserligen gammal och bestämmelsernas ordalydelser måste töjas för att appliceras på digitala bevis, men den har ansetts tillämplig av JO samt JK och i praktiken använts regelbundet i detta syfte. Vid en granskning av de internationella rättskällorna framkom att material som faller under begreppet open source (tillgängligt via vilken webbläsare som helst) alltid kan samlas in. För andra typer av material gäller fortfarande att insamling innebär en suveränitetskränkning. En anledning till det är att Sverige inte har ratificerat den enda konvention, CoCC, som i viss utsträckning tillåter sådana åtgärder. En annan är att en förändring av internationell sedvanerätt ännu inte kan anses etablerad, trots att det finns tydliga indikationer på att en sådan är på gång. Detta beror på den bristande enhetligheten i ny statspraxis, särskilt i ljuset av Lotus-principens tyngd och den nya statspraxisens suveränitetsinskränkande karaktär.

Uppsatsens andra frågeställning formulerades i syfte att klargöra huruvida svenska myndigheter kan samla in digital bevisning i situationer då dess geografiska position inte kan bestämmas. Här dras samma slutsats om svensk lagstiftning. Digitala bevis omfattas av de traditionella straffprocessuella reglerna även om det till viss del kan ifrågasättas. Vad gäller den folkrättsliga aspekten framkom att situationen ställer till särskilda problem eftersom Lotus-principen omöjliggör all insamling av den aktuella typen av bevis. Mot bakgrund av att insamling av open source-material, sannolikt av praktiska skäl, har ansetts utgöra internationell sedvanerätt fanns skäl att tro att ett sådant synsätt kunde tillämpas även när andra typer av bevis inte kan lokaliseras. Inget stöd för denna tes framkom av studien. Ett flertal stater har emellertid utformat lagstiftning särskilt i syfte att hantera digitala bevis vars position dolts genom molntjänster eller darkweb. Ytterligare exempel bidrar till slutsatsen att ny statspraxis, som innebär ett frånsteg från Lotus-principen, har trätt fram. Trots att den är relativt utpräglad och till viss del enhetlig, kan den inte anses uppnå de krav som ställs för att ny internationell sedvanerätt

ska anses etablerad. Även här måste Lotus-principens centrala roll och det faktum att den nya statspraxisen innefattar en suveränitetsinskränkning beaktas. Således utgör insamling av digitala bevis som inte kan lokaliseras, med undantag för open source-material, alltjämt en suveränitetskränkning om det skulle framkomma att det var lagrat inom en annan stats territorium.

Den tredje och sista frågeställningen utformades med avsikten att ta ställning till huruvida Sverige bör införa lagstiftning som särskilt etablerar en rätt för brottsbekämpande myndigheter att autonomt samla in digitala bevis som inte kan lokaliseras eller som finns lagrade i en annan stat. Vid en granskning av Beslagsutredningen framkom att ett förslag presenterats om att etablera ett nytt förhållningssätt som skulle tillåta aktuell insamling, men att rättsutvecklingen borde överlåtas till rättspraxis. Remissinstanserna var positivt inställda till den effektivisering som skulle följa av en förändring men ställde sig starkt kritiska till att överlåta utformandet till praxis och efterfrågade lagstiftning. Vid en undersökning av övrigt presenterat material framkom att kritik riktats mot aktuell typ av lagstiftning eftersom den gynnar en kortsiktig effektivisering av den brottsbekämpande verksamheten på bekostnad av långsiktiga internationella relationer. Efter en samlad bedömning av motstående intressen nåddes slutsatsen att Sverige bör lagstifta om en rätt för brottsbekämpande myndigheter att autonomt samla in digitala bevis transnationellt, trots att sådan lag hade stridit mot Lotus-principen. Lagstiftningen motiveras av att den hade lett till en markant effektivisering av den brottsbekämpande verksamheten och att det inte finns stöd för att hävda att den hade lett till bristande internationella relationer. Därtill kommer ytterligare fördelar i form av möjligheten att påverka den internationella rättsutvecklingen.

Käll- och litteraturförteckning

Offentligt tryck

Propositioner

Prop. 1988/89:124 Regeringens proposition om vissa tvångsmedelsfrågor

Prop. 2007/08:68 Regeringens proposition om förverkande av utbyte av brottslig verksamhet

Statens offentliga utredningar

SOU 1984:54 Tvångsmedel – anonymitet – integritet

SOU 1995:47 Tvångsmedel enligt 27 och 28 kap. RB samt polislagen

SOU 2002:98 Internationella brott och svensk jurisdiktion

SOU 2017:100 Beslag och husrannsakan – ett regelverk för dagens behov

Departementsserien

Ds. 2015:57 En europeisk utredningsorder

Utredningsdirektiv

Dir. 2016:20 Moderna regler om beslag och husrannsakan

Remissyttranden

Ekobrottsmyndigheten, remissyttrande över betänkandet Beslag och husrannsakan – ett regelverk för dagens behov (SOU 2017:100), 2018-04-03, Dnr EBM2018-66

Polisförbundet, remissyttrande över betänkandet Beslag och husrannsakan – ett regelverk för dagens behov (SOU 2017:100), 2018-04-19, Dnr 2017/09710/Å.

Polismyndigheten, remissyttrande över betänkandet Beslag och husrannsakan – ett regelverk för dagens behov (SOU 2017:100), 2018-04-20, Dnr A038.507/2018.

Åklagarmyndigheten, remissyttrande över betänkandet Beslag och husrannsakan – ett regelverk för dagens behov (SOU 2017:100), 2018-04-20, Dnr 2018-223.

Litteratur

Akehurst, Michael, "Jurisdiction in International law" i Waldock, Humphrey, Jennings, R.Y. (red.), *The British yearbook of international law 1972-73*, vol 46, 1973, s. 145–258.

Allen, Ronald Jay, Hoffman, Joseph L., Livingston, Debra A., Leipold, Andrew D., & Meares, Tracy L., *Comprehensive Criminal Procedure: investigation and right to counsel,* 5. uppl., Wolters Kluwer, New York, 2020

Bring, Thomas, Diesen, Christian & Andersson, Simon, *Förundersökning,* 5. uppl., Norstedts juridik, Stockholm, 2019

Burnett, Jerusha, "Geographically Restricted Streaming Content and Evasion of Geolocation: The Applicability of the Copyright Anticircumvention Rules", *Michigan Telecommunications and Technology Law Review*, vol. 19, nr. 2, 2013, s. 461–468.

Cassese, Antonio, *International Criminal Law*, Oxford University Press, Oxford, 2003

Çalışkan, Emin, Minárik, Tomáš & Osula, Anna-Maria,"Technical and Legal Overview of the Tor Anonymity Network", NATO Cooperative Cyber Defence Centre of Excellence*,* Tallin, 2015

De Hert, Paul, "Cybercrime and Jurisdiction in Belgium and the Netherlands: Lotus in Cyberspace – Whose Sovereignty is at Stake?" i Brenner, Susan W. & Koops, Bert-Jaap (red.), *Cybercrime and jurisdiction: a global survey*, T.M.C. Asser, The Hague, 2006

De Hert, Paul & Boulet, Gertjan, "Cloud Computing and Trans-Border Law Enforcement Access to Private Sector Data: Data Challenges to Sovereignty, Privacy and Data Protection" i *Workshop Paper Collection 'Big Data and Privacy: Making Ends Meet'*, 10 September 2013, CA Stanford Law School: Future of Privacy Forum and the Center for Internet and Society, s. 23–26

Dingledine, Roger, Mathewson, Nick & Syverson, Paul, "Tor: The Second-Generation Onion Router", *Proceedings of the 13th Usenix Security Symposium*, Tor Project, 2004

Dixon, Martin, *Textbook on international law*, 6. uppl., Oxford University Press, Oxford, 2007

Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, Norstedts juridik, Stockholm, 2013

Ekelöf, Per Olof, Bylund, Torleif & Edelstam, Henrik, *Rättegång H. 3.* 7., [rev.] uppl., Norstedts juridik, Stockholm, 2006

Faynberg, Igor, Lu, Hui-lan & Skuler, Dor, *Cloud Computing : business trends and technologies*, Wiley Publishing, New Jersey, 2016

Fitger, Peter, Sörbom, Monika, Eriksson, Tobias, Hall, Per, Palmkvist, Ragnar & Renfors, Cecilia, *Särtryck ur rättegångsbalken: Uppdaterade t.o.m. supplement 85*, Norstedts juridik, Stockholm, 2019

Gillespie, Alisdaire A., "Substantive and Procedural Legislation in England and Wales to Combat Webcam-Related Child Sexual Abuse" i Hof, Simone van der, Georgieva, Ilina, Schermer, Bart & Koops, Bert-Jaap (red.), *Sweetie 2.0: using artificial intelligence to fight webcam child sex tourism*, Asser Press, Den Haag, 2019

Goldsmith, Jack L., "The internet and the Legitimacy of Remote Cross-birder Searches", *University of Chicago Public Law & Legal Theory Working Paper*, nr. 16, University of Chicago, 2001

Hallbäck, Håkan, "Digitala beslag och spaning undercover", *Nordisk Tidsskrift for Kriminalvidenskab*, 2009, s. 26–34.

Helenius, Dan, *Straffrättslig jurisdiktion*, Soulmalainen Lakimiesyhdistys, Diss. Helsingfors : Helsingfors universitet, 2014, Helsinki, 2014

Henriksen, Anders, *International Law*, 2. uppl., Oxford University press, Oxford, 2019

Kaechele, Celia, "Traditional Notions of Fair Play and Substantial Justice in the Age of Internet Interconnectivity: How Masking an IP Address Could Constitute Purposeful Availment", *Yale Journal of Law and Technology*, 2019, s. 59–105.

Kleineman, Jan, "Rättsdogmatisk metod" i Nääv, Maria & Zamboni, Mauro (red.), *Juridisk metodlära*, 2 uppl., Studentlitteratur, Lund, 2018

Koops, Bert-Jaap, "Police Investigations in Internet Open Sources: Procedural-Law Issues", *Computer Law and Security Review*, vol. 29, nr. 6, 2013, s. 654–665.

Koops, Bert-Jaap & Goodwin, Morag, "Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The limits and Possibilities of International Law", *Tillburg Law School Legal Studies Research Paper Series*, nr. 5, Tillburg University, 2016

Kronqvist, Stefan, *Brott och digitala bevis: en handledning,* 3. uppl., Norstedts Juridik, Stockholm, 2013

Lambertz, Göran, *Nyttig och onyttig rättsvetenskap*, SvJT 2002, s. 261–278.

Lindberg, Gunnel, *Straffprocessuella tvångsmedel: när och hur får de användas?* 3., [rev.] uppl. Karnov Group, Stockholm, 2018

Linderfalk, Ulf (red.), *Folkrätten i ett nötskal*, 2., [utök. och uppdaterade uppl.], Studentlitteratur, Lund, 2012

Mason, Stephen (red.), *Electronic evidence*, 3 uppl., 2012

Naarttijärvi, Markus, *För din och andras säkerhet: konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel,* Iustus, Diss. Umeå : Umeå universitet, 2013, Uppsala, 2013

Nordh, Roberth, *Tvångsmedel: kvarstad, häktning, beslag, husrannsakan m.m.,* Iustus, Uppsala, 2007

Oppenheim, L.F.L., *Oppenheim's international law*, 9. uppl., Longman, Harlow, 1992

Osula, Anna-Maria, "Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data", *Masaryk University Journal of Law and Technology*, vol 9, 2015, s. 43–64.

Osula, Anna-Maria, "Transborder Access and Territorial Sovereignty", *Computer Law & Security Review*, vol. 31, nr. 6, 2015, s. 717–828.

Osula, Anna-Maria, "Remote Search and Seizure i Domestic Criminal Procedure: Estonian Case Study", *International Journal of Law and Information Technology*, vol. 24, nr. 4, 2016, s. 343–373.

Osula, Anna-Maria, *Remote search and seizure of extraterritorial data*, University of Tartu Press, Tartu, 2017

Poullet, Yves, van Gyesghem, Jean-Marc, Moiny, Jean-Philippe, Gérard, Jaques & Gayrel, Claire, "Data Protection in the Clouds" i Leenes, Ronald, De Hert, Paul, Poullet, Yves & Gutwirth, Serge, *Computers, Privacy, and Data Protection: An Element of Choice* [Elektronisk resurs], Springer Netherlands, 2011

Royer, Sofie, Conings, Charlotte & Marlier, Gaëlle, "Substantive and Procedural Legislation in Belgium to Combat Webcam-Related Sexual Child Abuse" i Hof, Simone van der, Georgieva, Ilina, Schermer, Bart & Koops, Bert-Jaap (red.), *Sweetie 2.0: using artificial intelligence to fight webcam child sex tourism*, Asser Press, Den Haag, 2019

Sandgren, Claes, *Rättsvetenskap för uppsatsförfattare: ämne, material, metod och argumentation*, 4 uppl., Stockholm, 2018

Schmitt, Michael N. & Vihul, Liis (red.), *Tallin manual 2.0 on the international law applicable to cyber operations: prepared by the international group of experts at the invitation of the NATO cooperative cyber defence centre of excellence*, 2. uppl.., Cambridge University Press, Cambridge, 2017

Sehgal, Naresh Kumar, *Cloud Computing with Security,* Springer International Publishing, 2020

Taylor, Mark, Haggerty, John, Gresty, David & Lamb, David, "Forensic Investigation of Cloud Computing Systems", *Network Security*, vol. 2011, nr. 3, 2011, s. 4–10.

Velasco, Cristos, Hörnle, Julia & Osula, Anna-Maria, "Global Views on Internet Jurisdiction and Trans-Border Access" i Gutwirth, Serge, Leenes, Ronald & Hert, Paul De (red.), *Data Protection on the Move Current Developments in ICT and Privacy/Data Protection*, Springer Netherlands, Dordrecht, 2016

Verdelho, Pedro, "Obtaining digital evidence in the global world", *EU Law Journal,* vol. 5, nr. 2, 2019, s. 136–145.

Westerlund, Gösta, *Straffprocessuella tvångsmedel: en studie av rättegångsbalkens 24 till 28 kapitel och annan lagstiftning*, 6 uppl., Bruuns bokförlag, Stockholm, 2018

Wilske, Stephan & schiller, Teresa, "International Jurisdiction in Cyberspace: Which States May Regulate the Internet", *Federal Communications Law Journal,* vol. 50, nr. 1, 1997, s. 119–133.

Wong, Christoffer, *Criminal Act, Criminal Jurisdiction and Criminal Justice*, Polpress, Diss. Lund : Univ., 2004, Kraków, 2004

Åklagarmyndigheten, *Beslag: en handbok,* Utvecklingscentrum, Malmö, 2010

Elektroniska källor

CoE, "Chart of signatures and ratifications of Treaty 185", *coe.int*, 17 april 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=XwHU9dGd, hämtad den 20 april 2020.

CoE, "Explanatory Report to the Convention on Cybercrime (ETS No. 185)", *coe.int*, 23 november 2001, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b, hämtad den 17 april 2020.

CoE, ”Reservations and Declarations for Treaty No.185”, *coe.int*, 6 maj 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=eouaccuw, hämtad den 6 maj 2020.

CoE, “T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime”, *coe.int*, 3 december 2014, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c, hämtad den 7 april 2020.

CoE, “T-CY Guidance Note #3 Transborder access to data (Article 32)”, *coe.int*, 3 december 2014, https://rm.coe.int/16802e726a, hämtad den 14 april 2020.

CoE, “T-CY Transborder access and jurisdiction: What are the options?”, *coe.int*, 6 december 2012, https://rm.coe.int/16802e79e8, hämtad den 6 april 2020.

IDC, ”Wordwide Server Market Revenue Declined 11,6% Year Over Year in the Second Quarter of 2019, According to IDC”, *idc.com*, 4 september 2019, https://www.idc.com/getdoc.jsp?containerId=prUS45482519, hämtad den 9 mars 2020.

ITU, ”Statistics”, *itu.int*, 31 december 2019, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, hämtad den 6 april 2020.

Johansson, Jessica, ”Så skyddar du dig mot Ransomeware-attacker”, *svt.se*, 12 maj 2017, https://www.svt.se/nyheter/inrikes/sa-skyddar-du-dig-mot-ransomware-attacker, hämtad den 5 april 2020.

Larsson, Linus, “Droghandeln på darknet omsatte miljoner”, *DN.se*, 1 mars 2020, https://www.dn.se/nyheter/sverige/droghandeln-pa-darknet-omsatte-miljoner/, hämtad den 9 mars 2020.

Larsson, Linus, ”Hackarnas ’storviltjakt’ kan kosta hundratals miljoner”, *dn.se*, 20 januari 2020, https://www.dn.se/ekonomi/hackarnas-storviltsjakt-kan-kosta-hundratals-miljoner/?forceScript=1&variantType=large, hämtad den 5 april 2020.

McGoogan, Cara, “Darkweb browser Tor is overwhelmingly used for crime, says study”, *telegraph.co.uk*, 2 februari 2016, https://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/, hämtad den 9 mars 2020.

Pilkington, Ed, “FBI Demands New Powers to Hack into Computers and Carry out Surveillance”, *theguardian*.com, 29 oktober 2014, https://www.theguardian.com/us-news/2014/oct/29/fbi-powers-hacking-computers-surveillance, hämtad den 26 april 2020

Reitman, Rainey, ”With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Government”, *eff.org*, 30 april 2016, https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government, hämtad den 26 april 2020.

Spoenle, Jan, “Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?”, *coe,int*, 31 augusti 2010, https://rm.coe.int/16802fa3df, hämtad den 6 april 2020

UNODC, “Comprehensive Study on Cybercrime, *unodc.org*, februari 2013, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, hämtad den 6 april 2020.

Williams, Mike, Turner, Brian, “Best dedicated server hosting providers of 2020”, *techradar.com*, 29 februari 2020, https://www.techradar.com/news/best-dedicated-server-hosting-providers, hämtad den 9 mars. 2020.

Förteckning över rätts- och myndighetspraxis

Sverige

Högsta domstolen

NJA 1977 s. 403

Avgöranden
Justitiekanslern

JK:s beslut dnr 6373-07-31

Justitieombudsmannen

JO:s beslut dnr 2138-2007

International Court of Justice

Case Concerning the Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium)

Permanent Court of International Justice

S.S. Lotus (France v. Turkey), 1927 PCIJ (ser. A) No. 10

Belgien

Yahoo! Inc [2013] Belgium Court of Appeal of Antwerp, 12th chamber for criminal cases 2012/CO/1054

Yahoo! Inc [2015] Court of Cassation of Belgium P.13.2082.N

Danmark

Højesterets kendelse af 10. Maj 2012 (sag 129/2011).

USA

United States v. Horton, 863 F3d 1041 (8th Cir. 2017)

United States v. Krueger, 809 F3d 316 (1st Cir. 2017)

United States v. Levin, 874 F.3d 316 (1st Cir. 2017)

United States v. Microsoft Corporation. In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. 2016).