Högsta domstolen
Box 2066
103 12 Stockholm

HA./. riksåklagaren ang. genomsökning på distans

(Göta hovrätts beslut den 1 september 2022 i mål Ö 3245-22)

Högsta domstolen har förelagt riksåklagaren att skyndsamt svara på HA:s överklagande och yttra sig över yrkandet om inhibition. Följande anförs.

Min inställning

Jag bestrider ändring av hovrättens beslut men tillstyrker prövningstillstånd i frågan om vilka anknytningsfaktorer som kan utgöra grund för svensk jurisdiktion med stöd av territorialitetsprincipen när det gäller åtkomst till elektronisk information med tvångsåtgärder (exekutiv jurisdiktion).

Yrkandet om inhibition bör avslås.

Bakgrund

Åklagaren begärde att tingsrätten skulle besluta om genomsökning på distans avseende mobiltelefoner och datorer som tagits i beslag från HA.

HA motsatte sig begäran och invände bl.a. att det oklara rättsläge som råder avseende frågan om exekutiv jurisdiktion starkt talade för att tingsrätten av försiktighetsskäl borde lämna åklagarens begäran utan bifall. Detta för att den misstänkte inte skulle riskera att lida framtida rättsförlust då potentiellt otillåtet åtkommen bevisning skulle kunna komma att åberopas emot honom vid en eventuell framtida huvudförhandling.

Tingsrätten meddelade den 26 augusti 2022 ett beslut om att genomsökning på distans fick ske och angav bl.a. följande skäl för beslutet.

> Det är inte känt var den lagrade informationen finns lagrad. Frågan om så kallad exekutiv jurisdiktion har berörts i förarbetena (se a. prop. s. 85 f.) där det bl.a. konstateras att en utredning om datalagring vid brottsbekämpning bl.a. ska titta på om det bör införas en särskild lagreglering för territorialprincipen vid exekutiv jurisdiktion som också tar hänsyn till andra anknytningsfaktorer än var data lagras. Brottet har begåtts i Sverige och det är här brottsutredningen pågår med tillämplig av svensk lag. Den som kan misstänkas för brottet har hemvist här och är svensk medborgare. De avläsningsbara informationssystemen som kan vara aktuella är tillgängliga från Sverige. Annat har inte framkommit än att avtal om tjänsten träffats från Sverige. Informationen kan hämtas från Sverige utan hjälp av utländska myndigheter och ett tvångsmedelsbeslut kan verkställas på svenskt territorium.

Tingsrätten konstaterar att frågan om exekutiv jurisdiktion är under fortsatt utredning. Lagstiftarens avsikt måste dock rimligen anses ha varit att den nya lagstiftningen om bl.a. genomsökning på distans ska kunna tillämpas även i fall där det är okänt var den lagrade informationen befinner sig eftersom lagstiftningen annars skulle vara helt verkningslös. Det är svårt att tänka sig fall där det skulle kunna slås fast att den lagrade informationen finns i Sverige, särskilt eftersom lagringsplatsen kan ändras mycket snabbt. Det kan också noteras att Lagrådet bedömde att det föreslagna tvångsmedlet genomsökning på distans utgör en proportionerlig åtgärd för att möta det behov som finns till följd av den tekniska utvecklingen och att några invändningar kring frågan om exekutiv jurisdiktion inte framfördes.

Hovrätten, som instämde i tingsrättens bedömning, fastställde tingsrättens beslut.

Överklagandet

HA har yrkat att Högsta domstolen ska undanröja hovrättens beslut om genomsökning på distans. Han yrkar vidare att hovrättens beslut om genomsökning på distans tills vidare inte ska få verkställas (inhibition).

Som skäl för prövningstillstånd har han gjort gällande att det är av vikt för ledning av rättstillämpningen att Högsta domstolen klargör om svenska myndigheter har exekutiv jurisdiktion vid beslut om genomsökning på distans då det inte är känt var den lagrade informationen finns och vidare vilken betydelse territorialitetsprincipen har vid beslut om genomsökning på distans.

Grunderna för min inställning

Genomsökning på distans

Bestämmelser om genomsökning på distans infördes i 28 kap. rättegångsbalken den 1 juni 2022 (se prop. 2021/22:119).

Skälet för att införa genomsökning på distans som ett nytt tvångsmedel var att de befintliga reglerna inte ansågs vara anpassade efter samhällets, och brottslighetens, allt bredare digitalisering och att det behövdes effektivare verktyg för de brottsbekämpande myndigheternas arbete. (A. prop. s. 75 f.)

Genomsökning på distans innebär att söka efter handlingar (jfr. definitionen i 2 kap. 3 § tryckfrihetsförordningen) som finns lagrade i ett avläsningsbart informationssystem utanför den elektroniska kommunikationsutrustning som används för att utföra genomsökningen. (28 kap. 10 a § rättegångsbalken.)

Med ett ”avläsningsbart informationssystem” avses en elektronisk kommunikationsutrustning - till exempel en mobiltelefon, surfplatta och dator - eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av en kommunikationstjänst, lagringstjänst eller liknande tjänst (jfr 1 § lagen [2020:62] om hemlig dataavläsning). Det är endast de delar av informationssystemet som den som utsätts för åtgärden har behörighet till som

de brottsbekämpande myndigheterna ges tillgång till genom tvångsmedlet. (A. prop. s. 76 f. och 177 f.)

En genomsökning på distans får endast avse uppgifter som är lagrade vid tidpunkten för åtgärden, dvs. tvångsmedlet får inte användas för löpande övervakning eller för ännu inte lagrad information även om det kan antas att informationen kommer att lagras (a. prop. s. 78 och 177.).

Om det finns anledning att anta att ett brott har begåtts på vilket fängelse kan följa får en genomsökning på distans utföras för att söka efter handlingar som kan vara av betydelse för utredning om brottet eller om förverkande av utbyte av brottslig verksamhet enligt 36 kap. 1 b § brottsbalken. Genomsökning på distans får utföras i ett avläsningsbart informationssystem som den som skäligen kan misstänkas för brottet kan antas ha använt. Även i annat fall får en genomsökning på distans utföras om det finns synnerlig anledning att anta att det går att påträffa handlingar som avses i första stycket. Genomsökning på distans får endast utföras genom autentisering i det avläsningsbara informationssystem som åtgärden avser. (28 kap. 10 b § rättegångsbalken.)

Med ”autentisering” avses att tillgång till informationssystemet skapas med hjälp av till exempel användarnamn och lösenord, biometrisk autentisering eller flerstegsautentisering, det vill säga två eller flera sätt att identifiera användaren av tjänsten (såsom inloggning i en internettjänst följt av en personlig kod som skickas till användaren). Ett annat fall kan vara att informationssystemet är omedelbart tillgängligt med hjälp av en applikation i den mobiltelefon som används, utan att inloggning krävs eller utan att en förnyad inloggning behöver göras. Det enklaste sättet att få tillgång till informationssystemet är i den situationen att klicka på en applikation eller ange ett för myndigheten känt lösenord och därigenom få tillgång till innehållet i informationssystemet. De brottsbekämpande myndigheterna får förlita sig på spaningsarbete och, i de fall det är aktuellt, hemliga tvångsmedel för att skaffa sig kännedom om sådana lösenord och inloggningsuppgifter. Den som utför en genomsökning på distans är därmed begränsad till att skaffa sig tillgång till informationssystemet genom den autentiseringsprocess som informationssystemet tillhandahåller. Bestämmelsen tillåter alltså inte installation av mjuk- eller hårdvara för att kringgå en nödvändig autentisering. Det är inte heller tillåtet att bryta eller kringgå systemskydd eller att utnyttja tekniska sårbarheter för att få åtkomst till ett system. (A. prop. s. 79 och 179.)

Exekutiv jurisdiktion

Allmänt

Folkrätten skiljer vanligen mellan legislativ, judiciell och exekutiv jurisdiktion. Med legislativ jurisdiktion avses avgränsningen av den nationella lagstiftningens tillämpningsområde, med judiciell jurisdiktion de rättstillämpande organens

tillämpning av den nationella rätten och med exekutiv jurisdiktion avses verkställigheten av beslutade åtgärder (se t.ex. SOU 2002:98 s. 73).

Rätten till exekutiv jurisdiktion är i princip alltid territoriellt begränsad. Utgångspunkten i folkrätten är att det råder ett förbud för stater att vidta verkställighetsåtgärder inom andra staters territorier, t.ex. använda tvångsmedel där. Detta är ett utflöde av den s.k. territorialitetsprincipen. Tanken med territorialitetsprincipen är att ingen stat ska kränka en annan stats territoriella integritet (suveränitet).

Den svenska tvångsmedelslagstiftningen saknar i huvudsak reglering om exekutiv jurisdiktion vid verkställighet. I regelverket för det internationella samarbetet finns dock vissa bestämmelser, grundade på bakomliggande avtal mellan stater, som uttryckligen ger svenska myndigheter möjlighet att verkställa beslutade åtgärder. Frågan om exekutiv jurisdiktion avgörs i övrigt genom en tolkning av territorialitetsprincipen. Enligt den traditionella tolkningen av territorialitetsprincipen i svensk rätt anses brottsbekämpande myndigheter sakna exekutiv jurisdiktion om de vill verkställa åtgärder för att komma åt elektroniska uppgifter som finns lagrade i ett annat land eller beträffande vilka lagringsstället är okänt.

Om svenska myndigheter saknar jurisdiktion och det inte heller finns något avtal med berörd stat kan åklagare vid tillämpning av den svenska tvångsmedelslagstiftningen begära rättslig hjälp för verkställighetsåtgärd på annans stats territorium (se t.ex. 1 kap. 7 § lagen om internationell rättslig hjälp i brottmål).

Förarbetena till bestämmelserna om genomsökning på distans

I frågan om de brottsbekämpande myndigheternas möjligheter att genom undersökning på distans bereda sig åtkomst till elektronisk information som är lagrad i ett annat land gjorde *Beslagsutredningen* (Ju 2016:08) bedömningen att det finns anledning att fokusera på vilka andra anknytningsmoment som bör kunna grunda jurisdiktion, snarare än själva lagringsplatsen. Detta gäller enligt utredningen särskilt vid s.k. ”loss of location”, dvs. situationer där man inte vet var elektronisk information är lagrad eller vilken stats regler som ska tillämpas på informationen. Tänkbara anknytningsmoment kan, angavs det, vara t.ex. var brottet begåtts, vilket land som har straffrättslig jurisdiktion och utreder det, var den misstänkte befinner sig och om åtgärden kan vidtas utan hjälp från något annat lands myndigheter. Utredningen hänvisade därefter till det arbete i syfte att nå en internationell konsensus på området som pågår och gjorde bedömningen att ett ställningstagande i frågan om ett svenskt synsätt inte lämpar sig för lagstiftning utan att de närmare förutsättningarna för jurisdiktion istället borde utmejslas i rättspraxis. (Se *Beslag och husrannsakan – ett regelverk för dagens behov* [SOU 2017:100] s. 362 f.)

I propositionen med förslag om nya regler om genomsökning på distans uttalade regeringen följande i frågan om exekutiv jurisdiktion (a. prop. s. 85 f.).

Den traditionella utgångspunkten i folkrätten är att det råder ett förbud för stater att vidta verkställighetsåtgärder inom andra staters territorier, till exempel att använda hemliga tvångsmedel där. Staters befogenhet att utöva åtgärder inom sitt territorium utgår från den s.k. territorialitetsprincipen. Principen uppfattas dock inte på samma sätt av alla stater i förhållande till vissa åtgärder.

Genomsökning på distans kan i vissa fall medföra att brottsbekämpande myndigheter påträffar handlingar som finns lagrade i utlandet eller på okänd plats. När det gäller inhämtande av elektroniska uppgifter är det inte sällan okänt var de finns lagrade fysiskt. Platsen kan ändras på bråkdelen av en sekund, och dessutom kan en och samma fil vara uppdelad och lagrad i olika länder. Utredningen anser, vilket Svea hovrätt och Ekobrottsmyndigheten instämmer i, att det därför finns anledning att ifrågasätta om just lagringsplatsen är den mest relevanta grunden för jurisdiktion när det gäller molnlagrad information och framhåller att det många gånger är slumpen som avgör var informationen lagras, liksom att användaren sällan har något inflytande över saken. Utredningen landar dock i slutsatsen att detta inte bör bli en fråga för lagstiftning utan något som får överlämnas till rättspraxis. Flera remissinstanser invänder dock mot utredningens bedömning och anser att frågan bör bli föremål för lagstiftning, däribland Hovrätten för Västra Sverige, Göteborgs tingsrätt, Åklagarmyndigheten, Ekobrottsmyndigheten och Skatteverket.

För en effektiv brottsbekämpning är det angeläget att reglerna om tillgång till elektronisk bevisning också kan tillämpas i praktiken, även när informationen finns utanför Sverige eller när det är okänt var den finns. Underlaget i det här lagstiftningsärendet ger dock inte möjlighet att närmare överväga frågan, men regeringen har nyligen tillsatt en utredning om datalagring vid brottsbekämpning som ska titta på bland annat frågan om exekutiv jurisdiktion, med utgångspunkt bland annat i de uttalanden som görs av Beslagsutredningen (dir. 2021:58). En del av utredningens uppdrag är att ta ställning till om det bör införas en särskild lagreglering för territorialitetsprincipen vid exekutiv jurisdiktion som också tar hänsyn till andra anknytningsfaktorer än var data lagras.

Förarbetena till lagen om hemlig dataavläsning

Utredningen om hemlig dataavläsning (Ju 2016:12) gjorde i sina överväganden om en ny lag om hemlig dataavläsning bedömningen att det finns starka skäl att nyansera den hittillsvarande svenska hållningen avseende vad territorialitetsprincipen vid exekutiv jurisdiktion innebär för elektroniskt lagrade uppgifter. Utredningen fann att frågan dock inte borde bli föremål för nationell lagstiftning utan borde prövas i rättstillämpningen. (Se *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet* [SOU 2017:89] s. 479 f.)

Utredningen utvecklade sin uppfattning enligt bl.a. följande.

När det särskilt gäller den s.k. loss of location-problematiken är det många gånger praktiskt möjligt för den brottsbekämpande myndigheten att ta del av uppgifter som lagras utanför det egna territoriet utan att befinna sig där uppgifterna finns. Så kan i de fallen ske utan den andra statens hjälp. En sådan möjlighet finns aldrig när det är fråga om annat än uppgifter som finns lagrade (eller kanske snarare manifesterade) på annat sätt än elektroniskt, t.ex. på papper. Eftersom det finns risk för att uppgifter av värde för en brottsutredning kan försvinna under den tid som det tar att utreda (om det alls är möjligt att utreda) var uppgifterna finns lagrade kan de beskrivna skillnaderna på mycket goda grunder utgöra en anledning att ifrågasätta om den

svenska hållningen avseende territorialitetsprincipen vid frågor om exekutiv jurisdiktion alltid har skäl för sig när det gäller utredningar som tangerar ”det digitala rummet”. Som framgått har flera andra stater valt att använda sig av ett annat synsätt när det gäller hur territorialitetsprincipen ska tillämpas under dessa förhållanden.
(…)

Såvitt avser de praktiska skälen för att förändra den svenska hållningen är det enligt vår mening starkaste argumentet att det, när en brottsutredning (eller ett underrättelseärende) pågår i Sverige och riktas mot en person som befinner sig här samt avser ett brott som begåtts (eller planeras) i riket, framstår som tämligen märkligt att svenska brottsbekämpande myndigheter inte ska kunna samla in elektroniskt lagrade uppgifter trots att de kan tillgängliggöras i Sverige utan att någon risk t.ex. för informationssäkerheten uppstår i den stat (eller i förekommande fall de stater) där uppgifterna lagras. Än mer märkligt blir detta med hänsyn till att lagringsplatsen i de allra flesta fall torde vara både irrelevant och okänd för den som äger eller disponerar informationen, och som alltså finns i Sverige, så länge hen kan få fram informationen på eget kommando. Med så många anknytningspunkter till en svensk utredning är det helt enkelt svårt att se varför lagringsplatsen i dessa fall ska avgöra den exekutiva jurisdiktionsfrågan. En jämförelse kan här göras med den danska högsta domstolens avgörande från 2012 där Højesteret nöjde sig med klart färre anknytningsfaktorer än de nu nämnda för att anse att dansk jurisdiktion förelåg.

Flera remissinstanser delade utredningens bedömning att den svenska hållningen borde ändras men ifrågasatte utredningens bedömning att frågan borde överlämnas till rättstillämpningen. I remissunderlaget framfördes synpunkten att uttalanden från utredningen om att det finns ett problem men inte någon föreslagen lösning kunde skapa osäkerhet om gällande rätt.

I propositionen med förslag till en ny lag om hemlig dataavläsning gjordes bedömningen att frågan om huruvida den svenska tolkningen av territorialitetsprincipen vid exekutiv jurisdiktion i förhållande till elektroniskt lagrade uppgifter borde ändras bäst skulle tas om hand inom ramen för det internationella samarbetet eller på annat lämpligt sätt och att den inte kunde tas om hand inom ramen för det lagstiftningsprojektet (prop. 2019/20:64 s. 201).

Datalagring vid brottsbekämpning – ytterligare åtgärder för en modern och ändamålsenlig reglering (dir. 2021:58)

Regeringen beslutade den 5 augusti 2021 att ge en särskild utredare i uppdrag att bl.a. analysera vissa frågor om jurisdiktion, inklusive folkrättsliga överväganden, i förhållande till elektronisk information som finns eller kan finnas utanför Sverige och ta ställning till om det bör införas en särskild lagreglering för exekutiv jurisdiktion. Uppdraget ska redovisas senast den 6 februari 2023.

I direktiven anges att någon lösning inom ramen för det internationella samarbetet ännu inte har kommit till stånd och att det hittills inte heller kommit någon vägledande praxis från de inhemska prejudikatinstanserna som löser jurisdiktionsfrågan för svensk del. För en effektiv brottsbekämpning är det, sägs det, viktigt att reglerna om tillgång till elektronisk kommunikation och annan elektronisk bevisning också kan tillämpas i praktiken, även när informationen finns utanför Sverige eller när det är okänt var den finns. Det finns därför enligt regeringen skäl att se över förutsättningarna, inklusive de folkrättsliga

aspekterna, för att införa en särskild lagreglering för territorialitetsprincipen vid exekutiv jurisdiktion i förhållande till elektronisk information som finns utanför Sverige.

Praxis

Genomsökning på distans

- **Svea hovrätt**, som instämde i tingsrättens bedömning, avslog i beslut den 18 augusti 2022 i mål Ö 10032-22 ett överklagande av tingsrättens beslut om tillstånd till genomsökning på distans. Stockholms tingsrätt hade den 17 augusti 2022 i mål B 5432-22 beslutat att tillåta genomsökning på distans trots invändningar om bristande jurisdiktion. Det var inte utrett i vilket land som informationen fanns lagrad. Åklagaren hade som anknytningsfaktorer gjort gällande att brottet hade begåtts och fått sin effekt i Sverige, att brottsutredningen pågick här med tillämpning av svensk lag, att den brottsmisstänkte hade hemvist och var medborgare i landet samt att informationen som eftersöktes kunde förväntas vara skriven på svenska**.**

- **Göta hovrätt,** som instämde i tingsrättens bedömning, fastställde i beslut den 10 juni 2022 i mål Ö 2216-22 tingsrättens beslut att tillåta genomsökning på distans efter att invändningar om bristande jurisdiktion hade förts fram. Det var inte känt var den lagrade informationen fanns lagrad. Tingsrätten hade i ett beslut den 7 juni 2022 i mål B 1846-22 funnit att exekutiv jurisdiktion fanns med hänvisning till att brottet hade begåtts i Sverige, det var här brottsutredningen pågick med tillämpning av svensk lag, den som kunde misstänkas för brottet hade hemvist här och var svensk medborgare, de avläsningsbara informationssystemen som kunde vara aktuella var tillgängliga från Sverige och annat hade inte framkommit än att avtal om tjänsten träffats från Sverige. Informationen kunde vidare hämtas från Sverige utan hjälp av utländska myndigheter och ett tvångsmedelsbeslut kunde verkställas på svenskt territorium.

- **Göta hovrätt**, som instämde i tingsrättens bedömning, fastställde i beslut den 14 juni 2022 i mål Ö 2268-22 tingsrättens beslut att tillåta genomsökning på distans efter invändningar om bristande jurisdiktion. Det var inte känt var informationen fanns lagrad. Tingsrätten hade den 7 juni 2022 i mål B 1497-22 beslutat om tillstånd till genomsökning på distans med hänvisning till att brottet hade begåtts i Sverige, det var här brottsutredningen pågick med tillämpning av svensk lag, den som kunde misstänkas för brottet hade hemvist här och var svensk medborgare, de avläsningsbara informationssystemen som kunde vara aktuella är tillgängliga från Sverige, annat hade inte framkommit än att avtal om tjänsten träffats från Sverige, informationen kunde hämtas från Sverige utan hjälp av utländska myndigheter och ett tvångsmedelsbeslut kunde verkställas på svenskt territorium. Högsta domstolen meddelade inte prövningstillstånd i målet (Högsta domstolens beslut den 15 juni 2022 i mål Ö 4022-22).

- **Attunda tingsrätt** beslutade den 10 juni 2022 i mål B 2799-22 att tillåta genomsökning på distans trots invändningar om bristande jurisdiktion. Tingsrätten anförde att om uppgifter lagras elektroniskt på annan plats än i Sverige eller om det är okänt var uppgifterna lagras så kan detta tala för att svenska brottsbekämpande myndigheter saknar jurisdiktion. Ju fler faktorer som innebär anknytning till Sverige och svenska intressen desto större anledning finns dock enligt tingsrätten för att hävda den motsatta ståndpunkten, nämligen att det finns svensk exekutiv jurisdiktion. De aktuella gärningarna påstods ha ägt rum i Sverige och den misstänkte påstods ha använt informationssystemet. Det fanns med hänsyn till detta och till de närmare omständigheterna i fallet enligt tingsrättens uppfattning svensk exekutiv jurisdiktion. Den begärda åtgärden bifölls därför.

- **Jönköpings tingsrätt** beslutade den 10 juni 2022 i mål B 2012-22 att tillåta genomsökning på distans trots invändningar om bristande jurisdiktion. Det var inte känt var informationen fanns lagrad. Tingsrätten konstaterade att gärningarna hade begåtts i Sverige och att det var här brottsutredningen pågick med tillämpning av svensk lag. Den som kunde misstänkas för brottet hade hemvist här och var svensk medborgare. De avläsningsbara informationssystemen som kunde vara aktuella var tillgängliga från Sverige. Den tjänst där den som kunde misstänkas hade sitt användarkonto var allmänt tillgängligt från Sverige. Avtal om tjänsten var träffat från Sverige, den information som eftersöktes kunde förväntas vara skriven på svenska och effekten av brottet hade inträffat i Sverige. Informationen kunde vidare hämtas från Sverige utan hjälp av utländska myndigheter.

Hemlig dataavläsning

Det finns, såvitt är känt, endast ett avgörande från hovrätterna som avser frågan om hur exekutiv jurisdiktion vid hemlig dataavläsning ska förstås (se nedan i första punkten). Det hovrättsavgörandet utgår från den traditionella tolkningen av territorialitetsprincipen, dvs. att lagringsstället avgör jurisdiktionen. När det gäller tingsrätterna finns det både ett antal beslut om att tillåta hemlig dataavläsning i sådana fall då det inte har kunnat klarläggas var informationen är lagrad och ett antal beslut om att inte ge tillstånd till hemlig dataavläsning i sådana situationer.

- I ett beslut om hemlig dataavläsning har en av landets hovrätter år 2021 instämt i den bedömning tingsrätten gjort att det i dagsläget saknas stöd för att göra avsteg från den hittillsvarande svenska hållningen vad gäller tolkningen av territorialitetsprincipen vid exekutiv jurisdiktion i förhållande till elektroniskt lagrade uppgifter. Ansökan, som avsåg information lagrad på en identifierad server utomlands, avslogs med hänvisning till bristande jurisdiktion.

- En av landets tingsrätter beslutade år 2020 att bevilja tillstånd till hemlig dataavläsning avseende ett iCloud-konto där det var okänt i vilket land som informationen fanns lagrad. Tingsrätten anförde i sina skäl för beslutet att det misstänkta brottet hade begåtts i Sverige, det enligt uppgift endast var svenska myndigheter som utredde brottet, den som var misstänkt för brottet hade gripits i Sverige och var häktad här samt mobiltelefonen hade funnits i Sverige och även hade fabriksåterställts här. Tingsrätten fann att det i det aktuella fallet inte var rimligt att falla tillbaka på Sveriges tidigare strikta hållning i fråga om territorialitetsprincipen och att ändamålet med lagstiftningen om hemlig dataavläsning i det aktuella fallet inte skulle kunna uppfyllas om inte den tidigare strikta hållningen luckrades upp något.

- En av landets tingsrätter avslog i ett beslut år 2021 en ansökan om tillstånd till hemlig dataavläsning. Det var okänt var informationen fanns lagrad. Tingsrätten ansåg att det fanns goda skäl att ifrågasätta om lagringsplatsen är relevant för att grunda jurisdiktion. Andra omständigheter borde enligt tingsrätten kunna påverka frågan om jurisdiktionen. Omständigheter som skulle kunna knyta det aktuella ärendet till Sverige var enligt tingsrätten om brottet har begåtts i Sverige, att det utreds endast av svenska myndigheter, att den elektroniska utrustningen finns i Sverige, att den misstänkte finns här i landet eller är medborgare här. I aktuellt fall var det enligt tingsrätten inte helt klart vilka omständigheter som kunde vara aktuella och under alla förhållanden framstod inte anknytningen till Sverige som helt tydlig eller övertygande. Mot denna bakgrund och då någon vägledning inte synes finnas från överrättspraxis i Sverige ansåg tingsrätten att ansökan skulle avslås.

- En ansökan om tillstånd till hemlig dataavläsning, som avsåg information där lagringsplatsen var okänd, avslogs av en tingsrätt år 2021 med motiveringen att den svenska utgångspunkten är att det enligt folkrätten inte är tillåtet för svenska myndigheter att med enbart tekniska hjälpmedel bereda sig tillgång till elektronisk information som är lagrad i andra länder och att en sådan här åtgärd alltså inte torde vara tillåten samt att frågan, såvitt känt, inte prövats i högre rätt. Därför fanns det enligt tingsrättens mening inte förutsättningar att bifalla ansökan i denna del.

- En av landets tingsrätter beviljade år 2021 en ansökan om hemlig dataavläsning som avsåg ett visst e-postkonto där det var känt i vilket land som informationen lagrades. Efter kontroll med det andra landets myndigheter konstaterades att e-posttjänsten var krypterad och det därför inte fanns någon möjlighet för dessa myndigheter att komma åt informationen genom husrannsakan. Det enda sättet att få tillgång till informationen var genom inloggning på det aktuella kontot med användarnamn och lösenord som utredningen hade tillgång till. I frågan om jurisdiktion ansåg tingsrätten att det inte var rimligt att falla tillbaka på Sveriges tidigare strikta hållning när det gäller elektroniskt lagrade uppgifter eftersom detta ställningstagande hade vuxit fram under en tid då information inte var rörlig på samma sätt som dagens elektroniska information är. Tingsrätten anförde att brottsutredningen bedrevs i Sverige, att brottet var begånget här, att den misstänkte var häktad här, att åklagaren hade möjlighet att bereda sig tillgång till informationen med hjälp av lösenord, att det under utredningens gång inte hade framkommit några internationella kopplingar beträffande brottsligheten och att anknytningspunkterna till den svenska utredningen därför var så många att det var svårt att se varför lagringsplatsen skulle avgöra den exekutiva jurisdiktionsfrågan.

- Ytterligare en av landets tingsrätter beviljade år 2020 en ansökan om hemlig dataavläsning där det var känt i vilket land som informationen lagrades (ett annat EU-land). Den misstänkte var vid tidpunkten häktad och belagd med restriktioner. Åklagaren gjorde gällande att det i och för sig skulle vara möjligt att få tillgång till informationen genom att utfärda en europeisk utredningsorder, men att det skulle ta väsentligt längre tid än att hämta in informationen genom ett beslut om hemlig dataavläsning. Tingsrätten beviljade ansökan, utan närmare motivering.

Högsta domstolen i Danmark och Norge

Danmarks Højesteret har i ett avgörande den 10 maj 2012 i sag 129/2011 tillåtit upprepade hemliga husrannsakningar avseende uppgifter på ett användarkonto (i det fallet en persons Facebook- och Messengerprofil till vilka den brottsbekämpande myndigheten hade lösenorden) trots att den elektroniska informationen som hämtades in vid husrannsakningarna var lagrad på servrar i utlandet. Polisen hade fått tillgång till den misstänktes lösenord genom hemlig telefonavlyssning och använde dessa för att logga in på hans användarkonto och bl.a. läsa inkomna och avsända meddelanden där. Højesteret hänvisade i skälen för sitt avgörande dels till andra anknytningspunkter än lagringsstället, dels till att åtgärderna kunde genomföras utan att utländska myndigheter involverades.

Norges Høyesterett har i ett avgörande den 28 mars 2019 HR 2019-619-A i sak nr 19-010640STR-HRET prövat frågan om det var tillåtet för polisen att från dataterminaler i ett företags lokaler i Oslo ladda ner elektroniskt material som företaget själv hade lagrat på en utländsk server eller om sådan tvångsmedelsanvändning faller utanför norska myndigheters jurisdiktion.

Högsta domstolen fann, med hänvisning till andra anknytningsfaktorer än lagringsställe, att det fanns norsk jurisdiktion för åtgärden och att tvångsåtgärden inte berörde en annan stat på ett sådant sätt att det innebar en kränkning av suveränitetsprincipen att verkställa den.

Min bedömning

Frågan om exekutiv jurisdiktion

Tvångsmedel kan bara verkställas inom svenska myndigheters jurisdiktion. För att vidta tvångsåtgärder i ett annat land krävs enligt folkrättsliga utgångspunkter det andra landets godkännande.

I svensk rätt har territorialitetsprincipen traditionellt tolkats så att brottsbekämpande myndigheter anses sakna exekutiv jurisdiktion om de vill verkställa åtgärder för att komma åt elektroniska uppgifter som finns lagrade i ett annat land eller beträffande vilka lagringsstället är okänt.

Denna tolkning har växt fram i den fysiska världen där det oftast är åtminstone teoretiskt möjligt att klarlägga var föremål förvaras och därför möjligt att vända sig till den stat som fysiskt förvarar föremålet.

I den digitala världen är det annorlunda. De tekniska lösningar för kommunikation och lagring av information som finns och hela tiden utvecklas innebär att elektroniska uppgifter kan finnas lagrade i flera stater samtidigt eller ständigt förflyttas mellan olika stater. Det är oftast omöjligt, även för exempelvis ett företag som tillhandahåller en kommunikationstjänst, att veta var informationen finns lagrad vid en given tidpunkt eftersom förändringar kan ske på bråkdelen av en sekund. Informationen kan också vara uppdelad i beståndsdelar och finnas på flera olika lagringsplatser samtidigt.

I de fall det är känt var de elektroniska uppgifterna finns lagrade kan svenska myndigheter ibland komma åt dem genom en framställan med begäran om internationell rättslig hjälp eller en europeisk utredningsorder ställd till det land där uppgifterna finns. Detta förutsätter att informationen finns stadigvarande tillgänglig på lagringsplatsen, vilket alltså mer sällan är fallet numera. Hanteringen av ärenden om rättslig hjälp medför en tidskrävande process. Risken är att värdet av att få tillgång till uppgifterna i ett visst skede av förundersökningen inte hinner uppfyllas i väntan på svaret på en rättslig hjälp. Vidare innebär nya krypteringslösningar att lagrad kommunikation i vissa fall inte finns tillgänglig i okrypterad version på lagringsstället. I sådana fall går det inte att komma åt kommunikationen i läsbar version via en begäran om rättslig hjälp. Däremot kan kommunikationen ofta läsas via ett användarkonto.

I de fall det inte kan klarläggas var uppgifterna finns lagrade, s.k. ”loss of location”, finns det inte någon stat att skicka en begäran om internationell rättslig

hjälp eller en europeisk utredningsorder till. Att det är okänt var informationen finns lagrad är, enligt min erfarenhet, en numera vanlig situation.

Frågan huruvida andra anknytningsmoment än lagringsstället kan utgöra grund för svensk jurisdiktion med stöd av territorialitetsprincipen när det gäller åtkomst till elektronisk information med tvångsåtgärder (exekutiv jurisdiktion) har därför ställts på sin spets genom de nya tvångsmedlen hemlig dataavläsning och genomsökning på distans.

Syftet med tvångsmedlet genomsökning på distans är att ge brottsbekämpande myndigheter effektivare verktyg eftersom de tidigare reglerna inte var anpassade efter samhällets, och brottslighetens, allt bredare digitalisering. Avsikten är alltså att ge förutsättningar för en mer effektiv brottsbekämpning.

Jag ansluter mig till den bedömning som flera avgöranden från underrätterna innehåller om att lagstiftarens avsikt rimligen måste anses ha varit att den nya lagstiftningen om genomsökning på distans ska kunna tillämpas även i fall där det inte gått att klarlägga var den lagrade informationen finns eftersom lagstiftningen annars skulle vara helt verkningslös.

Andra länder har inom ramen för sina rättsordningar gjort en tolkning av territorialitetsprincipen med utgångpunkt i alternativa anknytningsmoment. Av en kartläggning år 2012 av den s.k. Transbordergruppen inom Europarådet framgick, att de flesta stater inom EU redan åren 2009–2010 tillät sina brottsbekämpande myndigheter att bereda sig tillgång till elektroniska uppgifter för vilka lagringsplatsen är okänd från sina egna datorer om de brottsbekämpande myndigheterna hade fått tillgång till inloggningsuppgifter på ett lagligt sätt. Även i de fall då det står klart att uppgifterna lagras utanför den egna statens territorium tillät enligt kartläggningen ett flertal stater sina brottsbekämpande myndigheter att bereda sig tillgång till uppgifterna från de egna datorerna, om de hade laglig tillgång till inloggningsuppgifter för detta. (Se SOU 2017:89 s. 469 f.)

Sverige är inte bundet genom traktater eller folkrättslig sedvanerätt på ett sätt som hindrar en tolkning av territorialitetsprincipen med utgångspunkt i andra anknytningsfaktorer än elektroniska uppgifters lagringsställe. Det finns, enligt min uppfattning, därför inte något i den internationella rätten som förhindrar en tolkning med utgångspunkt i nya anknytningspunkter.

I förarbetena till de lagändringar som genomfördes med anledning av det svenska tillträdet till Europarådets konvention om it-relaterad brottslighet (ETS nr 185) klargjordes, när det gällde artikel 32 i konventionen, att en fördragsslutande stat utan tillstånd av en annan konventionsstat i vissa fall får bereda sig åtkomst till lagrade datorbehandlingsbara uppgifter som tekniskt sett finns på det egna territoriet. Det gäller bl.a. vid samtycke från den person som har laglig rätt att röja uppgifterna för staten via det datorsystemet. De situationer som avses i artikel 32 bedömdes vara sådana som alla parter var eniga om redan

är folkrättsligt tillåtna (se den förklarande rapporten p. 293) och några lagstiftningsåtgärder med anledning av artikelns innehåll bedömdes därför inte behövas. (Se prop. 2020/21:72 s. 63 och SOU 2013:39 s. 196.)

I det nu överklagade fallet är det inte känt var informationen finns lagrad (loss of location). Det finns därför inte någon stat att hämta in tillstånd från.

Brottet har begåtts på svenskt territorium och brottsmisstanken utreds av svenska myndigheter med tillämpning av svensk lag. Detta är omständigheter som har godtagits som jurisdiktionsgrundande anknytningspunkter i andra med Sverige jämförbara länder. Den brottsmisstänkte, som är den som disponerar över de mobiltelefoner och datorer som tagits i beslag från honom och därmed är informationsinnehavaren, har hemvist i Sverige och är svensk medborgare. Informationen kan göras tillgänglig från Sverige, dvs. utan bistånd av utländska myndigheter.

Det är min uppfattning att det i det aktuella fallet finns sådana anknytningspunkter till Sverige som utgör grund för exekutiv jurisdiktion för den begärda åtgärden. Det står dessutom klart att verkställigheten kan ske (informationen kan göras tillgänglig) utan bistånd från något annat land.

Eftersom svenska myndigheter enligt min bedömning har exekutiv jurisdiktion när det gäller den begärda åtgärden och förutsättningarna för genomsökning på distans i övrigt är uppfyllda i det här fallet bör hovrättens beslut stå fast.

Det är min uppfattning, i överensstämmelse med de bedömningar som Högsta domstolen i Danmark och Norge har gjort, att det även i de fall det är känt att information finns lagrad i ett land utanför Sverige kan finnas exekutiv jurisdiktion för svenska myndigheter om det finns andra anknytningspunkter till Sverige än lagringsstället och tvångsåtgärden kan verkställas utan att utländska myndigheter involveras, exempelvis genom inloggning på ett användarkonto med ett lösenord som kommits åt på ett lagligt sätt.

Frågan om inhibition

Beslut under rättegången enligt vilket rätten har utlåtit sig angående åtgärd, som avses i 25-28 kap. rättegångsbalken (tvångsmedel) ska genast gå i verkställighet (30 kap. 12 § första stycket 3 rättegångsbalken).

Om en hovrätt i ett brottmål har fastställt en tingsrätts beslut att bevilja en åtgärd som avses i 26–28 kap. rättegångsbalken (tvångsmedel) får Högsta domstolen i de fall domen har överklagats omedelbart besluta att hovrättens beslut tills vidare inte får verkställas (55 kap. 8 § andra stycket rättegångsbalken).

Någon motsvarande bestämmelse, eller hänvisning till bestämmelse, finns inte i reglerna i 56 kap. rättegångsbalken om överklagande av hovrättsbeslut.

Rättsläget i frågan om det måste finnas lagstöd för att högre rätt ska ha möjlighet att besluta om inhibition i ett mål om överklagade beslut (s.k. Ö-mål) när det gäller beslut som enligt föreskrift i lag ska verkställas utan hinder av att det inte vunnit laga kraft är inte helt klart.

Högsta domstolen har tidigare, när det gäller beslut som enligt föreskrift i lag ska verkställas utan hinder av att det inte har vunnit laga kraft, uttalat att sådana beslut som utgångspunkt får inhiberas endast då det finns lagstöd för detta. För att i rättstillämpningen avvika från den utgångspunkten med avseende på en viss kategori av omedelbart verkställbara avgöranden måste det enligt Högsta domstolen finnas alldeles speciella skäl. (Se NJA 2008 s. 1113 och NJA 2016 s. 140 p. 5.) Vad som avses med ”alldeles speciella skäl” utvecklas inte närmare.

I doktrinen finns stöd för att inhibition i brottmål kan ske utan lagstöd. Uppfattningen har där framförts att det i brottmål är av stor vikt att den tilltalade inte drabbas av en påföljd endast av det skälet att lagstiftaren har missat att införa inhibitionsmöjligheter i de fall sådana är behövliga. Här har heller inte ansetts finnas någon motpart som drabbas av inhibitionen. Det har därför gjorts gällande att det möter mindre betänkligheter med inhibition utan lagstöd i brottmål än i dispositiva tvistemål. (Hans Eklund, *Inhibition – om verkställighetsförbud m.m. i judiciell process, inom förvaltningsrätten och utsökningsförfarand*e, 1998, s. 29.)

Högsta domstolen beslutade den 16 juni 2015 i mål Ö 3074-15 att ett beslut om husrannsakan tills vidare inte fick verkställas efter att hovrättens beslut överklagats. Det tycks alltså i Högsta domstolens praxis finnas ett utrymme för inhibition i dessa situationer.

I det nu aktuella fallet har beslutet om genomsökning på distans redan verkställts. Med utgångspunkt i det och i min bedömning att hovrättens beslut bör stå fast saknas det skäl för ett beslut om inhibition av tingsrättens beslut.

Inhibitionsyrkandet bör mot bakgrund av det som sagts avslås.

Skälen för prövningstillstånd

Enligt 54 kap. 10 § första stycket 1 rättegångsbalken får prövningstillstånd meddelas om det är av vikt för ledning av rättstillämpningen att överklagandet prövas av Högsta domstolen (prejudikatdispens). För att bevilja prövning enligt denna punkt krävs alltså att målet med hänsyn till det allmänna intresset av tillgång till omfattande och vägledande prejudikatbildning bör prövas av Högsta domstolen (Peter Fitger m.fl., *Rättegångsbalken – en kommentar på internet*, kommentaren till 54 kap. 10 § rättegångsbalken).

Frågan om hur territorialitetsprincipen ska tolkas när det gäller åtkomst av elektronisk information genom tvångsåtgärder, t.ex. genomsökning på distans,

har inte prövats av Högsta domstolen. Den underrättspraxis som finns i frågan, inkluderande beslut om hemlig dataavläsning, är inte enhetlig.

Utredningen om hemlig dataavläsning och Beslagsutredningen har båda, på sätt som redovisats, argumenterat för att det i frågan om brottsutredande myndigheters åtkomst till elektronisk information finns skäl att låta andra anknytningsmoment än lagringsplatsen för informationen kunna grunda jurisdiktion. Båda utredningarna har gjort bedömningen att frågan inte lämpar sig för lagstiftning utan har hänvisat till att de närmare förutsättningarna för jurisdiktion bör utformas i rättspraxis.

När lagen om hemlig dataavläsning infördes gjorde regeringen bedömningen att frågan om hur territorialitetsprincipen vid exekutiv jurisdiktion bör tolkas bäst tas om hand inom ramen för det internationella samarbetet eller ”på annat lämpligt sätt”. Detta uppfattar jag som en hänvisning till rättsbildningen. I förarbetena till bestämmelsen om genomsökning på distans hänvisade i samma fråga regeringen till att det är angeläget att reglerna om tillgång till elektronisk bevisning också kan tillämpas i praktiken, även när informationen finns utanför Sverige eller när det är okänt var den finns, men att underlaget i det lagstiftningsarbetet inte gav möjlighet att närmare överväga frågan.

Eventuella resultat av det arbete som därefter har inletts i regeringskansliet och det som pågår inom ramen för det internationella samarbetet ligger i framtiden. Det går heller inte att utgå från att det pågående arbetet kommer leda till lagstiftning eller andra lösningar.

Frågan om hur territorialitetsprincipen bör tolkas vid tvångsåtgärder som avser åtkomst till elektronisk information är alltså inte löst av lagstiftaren, trots att frågan låg på lagstiftarens bord när reglerna om genomsökning på distans och hemlig dataavläsning arbetades fram.

Den närmare gränsdragningen för var gränserna för svensk jurisdiktion går måste göras utifrån folkrättsliga principer efter en bedömning av den begärda tvångsåtgärden i det konkreta fallet. Det finns enligt min bedömning därför inte något hinder med hänsyn till legalitetsprincipen mot att frågan avgörs genom rättsbildningen. En sådan rättsutveckling i praxis har skett i bl.a. Danmark och Norge.

Frågor om exekutiv jurisdiktion aktualiseras i varje ärende som rör tvångsåtgärder avseende elektronisk information. Hur territorialitetsprincipen ska tolkas i de här fallen har stor betydelse för både tänkta effektivitetsvinster med den svenska tvångsmedelslagstiftningen och för rättssäkerheten.

Det finns med hänsyn till det oklara rättsläget och mängden ärenden som frågan aktualiseras i ett brådskande behov av att Högsta domstolen ger vägledning om vilka anknytningsfaktorer som kan utgöra grund för svensk jurisdiktion med stöd

av territorialitetsprincipen när det gäller åtkomst till elektronisk information med tvångsåtgärder (exekutiv jurisdiktion).

Behovet av vägledning gäller både de fall då lagringsplatsen är okänd (loss of location) och de fall då det står klart att uppgifterna lagras utanför Sveriges territorium.

Mot den redovisade bakgrunden vore en prövning av målet i Högsta domstolen enligt min uppfattning av vikt för ledning av rättstillämpningen. Jag tillstyrker därför prövningstillstånd.

Bevisuppgift och handläggning

Ingen bevisning åberopas. Målet kan avgöras utan huvudförhandling.

Petra Lundh

Eva Bloch

Kopia till
Ekobrottskammaren i Linköping (EB-8296-20).
Kammaråklagaren Oscar Strömblad.
Utvecklingscentrum.
Ekobrottsmyndigheten (Överåklagarens kansli).