

Till:
Svea hovrätt

Stockholm den 26 juli 2021

Skickas endast per e-post

Mål B 2559-20 Åklagaren ./ Andreas Lookene m.fl.

I egenskap av ombud och offentlig försvarare för Andreas Lookene får jag härmed framställa följande yrkande.

Yrkande

1. Andreas Lookene yrkar att hovrätten ska avvisa åklagarens angivna och åberopade bevisning i aktbilaga 315 som benämns som ”Sammanställning av meddelanden i EncroChat”, i de delar som bevisningen åberopas mot Andreas Lookene.
2. Yrkandet grundar sig på följande omständigheter.

Kort sammanfattning av skälen för yrkandet

3. Enligt Andreas Lookenes uppfattning har det aktuella materialet inhämtats genom en åtgärd som är att likställa med hemlig dataavläsning enligt svensk lag. Den hemliga dataavläsningen har riktats mot, inte företaget EncroChatts server, utan mot de enskilda användarna av så kallade Encrotelefoner.
4. I det fall där den aktuella Encrotelefonen befunnit sig utanför Frankrikes territorium innebär den hemliga dataavläsningen att franska myndigheter utövat jurisdiktion i andra

stater. Folkkrätten innehåller ett principiellt förbud mot att utöva exekutiv jurisdiktion på andra staters territorium.

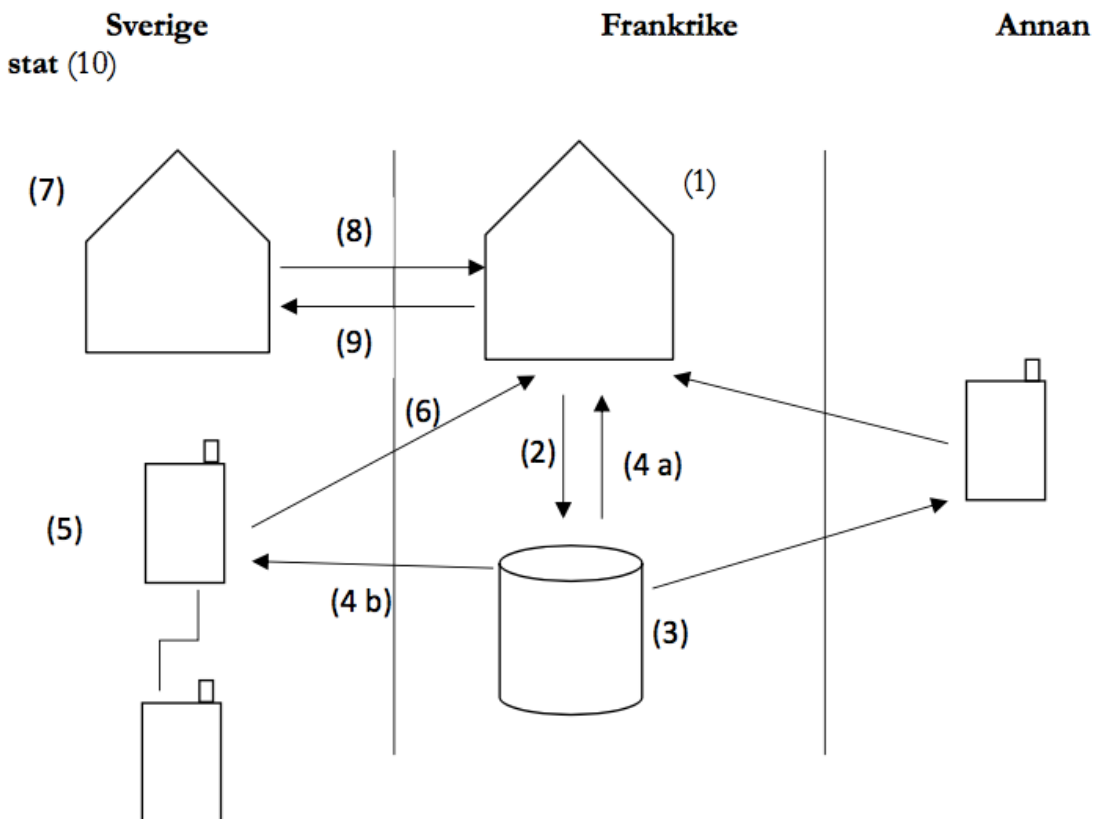
5. Något beslut från svenska myndigheter om att tillåta de franska myndigheterna att utöva exekutiv jurisdiktion på Sveriges territorium föreligger inte såvitt är känt. Frankrikes åtgärd är därför att anse som en allvarlig kränkning av Sveriges suveränitet.
6. Det är inte känt om den franska åtgärden är tillåten enligt fransk lag och inte heller hur den franska åtgärden utförts i alla sina praktiska detaljer, men det är uppenbart att åtgärden som sådan inte skulle varit tillåten enligt svensk lag. Det finns därför inte någon möjlighet för en svensk domstol eller annan myndighet att tillåta åtgärden på svenskt territorium.
7. Det sätt som de franska myndigheterna utfört den hemliga dataavläsningen på och hur de svenska myndigheterna inhämtat materialet genom en europeisk utredningsordet innebär allvarliga ingrepp i de drabbades rättigheter enligt art. 8 och art 6. i den Europeiska konventionen den 4 november 1950 om skydd för de mänskliga rättigheterna och de grundläggande friheter (EKMR). Agerandet från myndigheternas sida medför att det är praktiskt sett omöjligt att verifiera autenticiteten av det åberopade materialet och därför är även kränkningen av de drabbades rätt till en rättvis rättegång irreversibel.
8. Rättsföljden enligt svensk lag av att uppgifter läses av eller tas upp genom hemlig dataavläsning utan tillstånd är att materialet inte får åberopas mot den som drabbats eller på annat sätt berörs av åtgärden. Regeln utgör en inskränkning av principen om fri bevisprövning.
9. Även av praxis kring art. 6 EKMR framgår att bevisning som åtkommits genom hemliga tvångsmedel och som inte följer av nationell lag och om det visar sig att ingreppet i rättigheten är irreversibelt så får inte bevisningen användas i en senare brottmålsprocess.
10. Till utveckling av grunderna får följande anföras.

Bakgrund

11. Under mars 2020 lyckades franska myndigheter föra in en programkod i en server som befann sig i Lyon, Frankrike. Servern tillhörde det nederländska företaget EncroChart.

12. EncroChatt tillhandahöll sedan år 2015 ett operativsystem med krypterade applikationer för kommunikation. Vissa särskilt modifierade mobiltelefoner, s.k. Encrotelefoner försågs med det modifierade operativsystemet. Syftet med operativsystemet var att möjliggöra krypterad in- och utgående kommunikation via mobiltelefonerna genom en chattfunktion, även den kallad ”Encrochatt”.
13. Programkoden utförde två saker. Den speglade innehållet på servern och den skickade ut en uppdatering till de enskilda kommunikationsenheterna, d.v.s. telefonerna. När användaren av en sådan Encrotelefon accepterade uppdateringen överfördes programkoden till den enskilda kommunikationsenheten.
14. Programkoden var någon form av en så kallad key-log. Det innebär att så fort en kommunikationsenhet användes registrerades det och överfördes till de franska myndigheterna. Genom att läsa av och ta upp kommunikationen på den enskilda kommunikationsenheten kunde de franska myndigheterna kringgå själva krypteringstjänsten.
15. Det som framförallt kunde läsas av och tas upp av de franska myndigheterna var de så kallade Encrochattarna. Det förefaller däremot som om de franska myndigheterna inte kunnat avlyssna röstsamtal via Encrotelefonerna.
16. Följaktligen har de franska myndigheterna inte dekrypterat Encrochatt och inte heller läst av eller tagit upp en kommunikation via Servern i Lyon utan via en key-log läst av varje enskild kommunikationsenhet. Avläsningen har skett från den plats där kommunikationsenheten befunnit sig och innan alternativt parallellt med att meddelandena nått servern.
17. Enligt vad försvaret lyckats utröna från olika källor har avläsningen och upptagningen, och senare inhämtningen av upptagningarna, går till på följande sätt vilket schematiskt beskrivs i Skiss (1) nedan.

Skiss 1



- (1) En särskild brottsutredande enhet i Lille, Frankrike, har själva eller tillsammans med franska Gendarmeriet, ansökt om tillstånd hos antingen en domstol eller förundersökningsdomare om att få placera en programkod i en server placerad i Lyon.
- (2) Efter att tillstånd meddelats placerades programkoden i hemlighet på servern. Innehavaren och användarna av servern fick ingen underrättelse om åtgärden.
- (3) Servern tillhörde, i vart fall användes av, det holländska företaget EncroChatt. Via servern erbjöd EncroChatt sina kunder möjlighet att kommunicera med Encrotelefoner.
- (4) (a) Programkoden hade två funktioner, varav den första innebar att servern speglades och informationen översändes till de franska brottsutredande myndigheterna.

- (b) Den andra funktionen var att programkoden överfördes från servern till de enskilda kommunikationsenheterna, d.v.s. Encrotelefonerna.
- (5) När programkoden överförs till respektive Encrotelefon uppmanades användaren att uppdatera sin Encrotelefon/krypteringstjänst. Genom uppdateringen aktiverades den utsända programkoden i den enskilda Encrotelefonen.
- (6) I telefonen fungerade programkoden som en så kallad key-log, vilket innebar att varje användning av Encrotelefonernas tangentbord överfördes i realtid till de franska brottsutredande myndigheterna.
- (7) Avläsningen och upptagningen pågick under perioden från slutet av mars till den 13 juni 2020. Under den tid som åtgärden pågick deltog flera andra länder, däribland Sverige genom Nationella Operativ Avdelningen (NOA), i en samarbetsgrupp inom Eurojust som verkar ha tillåtit att sitta med och ta del av avläsningarna i realtid.
- (8) Sedan EncroChatt uppdagat intrånget i servern skickade företaget ut en varning till sina användare som uppmanades att göra sig av med telefonerna. För att få del av upptagningarna ställde svenska åklagare ut en europeisk utredningsorder till Frankrike med en begäran om att få del av upptagningar knutna till vissa angivna användarnamn.
- (9) Efter beslut av fransk domstol överlämnades upptagningarna till de svenska brottsutredande myndigheterna, som framgår i ett annat ärende, genom att gendarmeriet överlämnade en "CD-ROM".
- (10) I flertalet fall handlar det om enskilda Encrotelefoner som befunnit sig på svenskt territorium, men även Encrotelefoner i andra stater, såväl inom som utan EU, har blivit föremål för avläsning och upptagning.
18. De franska brottsutredande myndigheterna har genom det ovan beskrivna förfarandet läst av och tagit upp uppgifter från, i princip, alla kommunikationsenheter som använder Encrochatt. Avläsningarna och upptagningarna har skett direkt från kommunikationsenheterna, och inte från den server som var stationerad i Lyon och som var den enhet som först angreps med programkoden. Såvitt kan förstås var inga av de enskilda användarna av kommunikationsenheterna föremål för misstankar i den franska

förundersökning där åtgärden utfördes, utan det var företrädare för företaget EncroChatt som misstänktes för brott. Användarna av kommunikationsenheterna och kommunikationsenheterna själva befann sig i ett stort antal fall utanför Frankrikes territorium, däribland i Sverige, när avläsningen och upptagningen genomfördes och riktades mot personer som var medborgare i andra stater än Frankrike, däribland medborgare i den stat där såväl användare som kommunikationsenhet befann sig fysiskt.

19. Detta förfarande väcker ett flertal frågor av betydelse för nu aktuellt mål vad gäller användandet av Encrochattarna och andra uppgifter som lästs av och tagits upp som bevisning mot de tilltalade.

Gällande rätt

20. Utifrån ett folkrättsligt perspektiv skiljer man mellan legislativ, judiciell och exekutiv jurisdiktion. Med legislativ jurisdiktion avses lagstiftningens tillämpningsområde och med judiciell jurisdiktion avses de rättstillämpande organens tillämpning av nationell rätt. Med exekutiv jurisdiktion avses verkställigheten av beslutade åtgärder.
21. Av suveränitetsprincipen följer att varje stat har exklusiv jurisdiktion inom sitt eget territorium (SOU 2002:98 s. 73). En verkställighetsåtgärd eller annan maktutövning på en annan stans territorium utgör därför en klar suveränitetskränkning (Hilding Eek, Folkrätt (4:e uppl.) s. 405), såvida inte staten har en materiell kompetens, det vill säga kan lagstifta med bindande verkan för andra stater (Reinhold Reuterswärd, Lagstiftningsmaktens folkrättsliga gränser, SvJT 1977 s. 108 f.).
22. Detta bekräftades i det så kallade Lotus-fallet (S.S. Lotus (Fr. v. Turk), 1927 P.C.I.J., där det fastställs i p. 45 att;

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 exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by State outside its territory except by virtue of a permissive rule derived from international custom or from a convention. (min understrykning)

23. Stater har givits en möjlighet att bilateralt eller genom traktater tillåta en annan stat att utöva exklusiv jurisdiktion på den andra statens territorium. Lagen (2017:1000) om europeisk utredningsorder (LEUO) är en implementering av EU:s direktiv 2014/41 som

utgör sådant internationellt instrument som kan anses inskränka den folkrättsliga suveränitetsprincipen.

24. Det får anses uppenbart att den åtgärd som genomförts av de franska brottsutredande myndigheterna – d.v.s. att läsa av och ta upp uppgifter från kommunikationsenheter där såväl enheten som användaren befinner sig på en annan stats territorium, och inte är medborgare i Frankrike – innebär att de franska myndigheterna utövat exekutiv jurisdiktion utanför franskt territorium. Åtgärden förutsätter således stöd i traktat eller andra internationella instrument eller i den berörda statens nationella rätt, för att inte anses vara en kränkning av den andra statens suveränitet.

En europeisk utredningsorder

25. En europeisk utredningsorder (EUO) definieras, enligt 1 kap. 3 § LEUO, som ett beslut som innebär att en utredningsåtgärd ska vidtas i en annan medlemsstat i syfte att inhämta bevisning och som har meddelats av en åklagare eller domstol under en förundersökning eller rättegång i brottmål eller utanför en förundersökning.
26. En EUO ska avse tre olika förfaranden: i) att staten ska utföra åtgärden, ii) att staten ska bistå vid åtgärden eller iii) att staten ska tillåta åtgärden.
27. En EUO är ett beslut *sui generis* och det behöver inte finnas ett underliggande nationellt beslut avseende motsvarande åtgärd. Däremot får en EUO endast utfärdas om de förutsättningar som gäller för att vidta motsvarande utredningsåtgärd under en svensk förundersökning eller rättegång i brottmål är uppfyllda (2 kap. 3 § LEUO). Således kan en EUO inte utfärdas eller bifallas om utredningsåtgärden inte finns tillgänglig enligt svensk rätt eller de materiella förutsättningarna för åtgärden inte är uppfyllda enligt svensk rätt.
28. Med *inhämta bevis* avses såväl bevis som de behöriga myndigheterna har i sin besittning som bevis som behöver inhämtas genom att någon specifik utredningsåtgärd vidtas. Inhämtning av bevis som behöriga myndigheter har i sin besittning regleras i 1 kap. 4 § 11-12 pp. LEUO.
29. I 4 kap. 13-16 §§ LEUO regleras skyldigheten för en annan stat att underrätta Sverige om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation som utförs i Sverige utan bistånd av Sverige.

30. Av 13 § framgår att behörig myndighet i annan stat ska underrätta behörig åklagare om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation i Sverige. Motsvarande underrättelseskyldighet gäller även för hemlig dataavläsning (16 §).
31. Finner behörig åklagare att förutsättningarna för åtgärden är uppfyllda enligt svensk rätt ska ärendet överlämnas till domstol för beslut om tillstånd ska meddelas (14 §) En förutsättning för beviljande av tillstånd är att gärningen är straffbar enligt svensk rätt och förutsättningarna för motsvarande åtgärd enligt svensk rätt är tillämpliga.
32. Såvitt är känt för försvaret har behörig myndighet i Frankrike inte underrättat behörig åklagare i Sverige om den aktuella åtgärden och svensk domstol har inte heller gett sitt tillstånd till den.

Hemlig dataavläsning

33. Med hemlig dataavläsning (HDA) avses att uppgifter, som är avsedda för automatisk behandling, i hemlighet och med tekniskt hjälpmedel läses av eller tas upp i ett avläsningsbart informationssystem enligt 1 § lagen (2020:62) om hemlig dataavläsning, (LHDA).
34. Avläsningsbara informationssystem kan vara av fysisk karaktär, t.ex. datorer, mobiltelefoner och servrar, men även internetbaserade kommunikations- eller lagringstjänster och andra informationssystem som inte i sig utgör elektronisk kommunikationsutrustning innefattas. För det fall det avläsningsbara informationssystemet används av flera bör HDA endast få avse de relevanta uppgifter som är avgränsade till den enskilde användaren och de delar som denne har behörighet till.
35. De uppgifter som kan inhämtas med HDA är *kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter, platsuppgifter, kameraövervakningsuppgifter, rumsavlyssningsuppgifter* och *andra uppgifter* som finns i det avläsningsbara informationssystemet samt uppgifter som visar hur det används. HDA anses i stor utsträckning vara en form av verkställighet av redan befintliga hemliga tvångsmedel och förutsättningarna för att använda HDA följer därför i stor utsträckning bestämmelserna för de bakomliggande tvångsmedlen. De övriga uppgifter som inte svarar mot redan

befintliga uppgifter likställs med hemlig avlyssning av elektronisk kommunikation (HAK), se prop. 2019/20:64 s. 113 f.

36. HDA kan tillämpas under en förundersökning (4-6 §§ LHDA) och utanför en förundersökning (7-10 §§ LHDA). De senare reglerna bygger på föreskrifterna i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventionslagen), lagen (2012:78) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) och lagen (1991:572) om särskild utlänningskontroll, (LSU).
37. Vad gäller den som kan bli föremål för HDA under en förundersökning gäller att denne ska vara skäligen misstänkt (4 § LHDA), alternativt att HDA kan användas för att utreda vem som skäligen kan misstänkas (5 § LHDA).
38. Förutsättningar för HDA riktad mot den som skäligen kan misstänkas svarar, i princip, mot reglerna för HAK, med vissa särskilda regler när det kommer till kameraövervaknings- och rumsavlyssningsuppgifter.
39. När HDA använts för att utreda vem som skäligen kan misstänkas gäller ett antal inskränkningar. För det första gäller det bara kommunikationsövervaknings- och platsuppgifter och vad gäller kommunikationsövervakningsuppgifter får de endast avse förfluten tid. En ytterligare förutsättning är att det avläsningsbara informationssystemet använts vid ett brott eller i anslutning till en brottsplats eller som av någon annan anledning är av synnerligen vikt för utredningen.
40. HDA enligt 7 § LHDA är kopplade till en person och förutsätter att det föreligger en påtaglig risk för att personen antingen kommer att utöva sådan brottslig verksamhet som avses i 1 § preventivlagen eller medvetet kommer att främja att sådan brottslig verksamhet kommer att utövas inom en organisation eller grupp som personen tillhör eller verkar för. De avläsningsbara informationssystem som avses är sådana som personen använder eller som det finns särskild anledning att anta har använt eller kommer att använda eller, om det finns synnerlig anledning att anta, har kontaktat eller kommer att kontakta.
41. I de fall där avläsningen eller upptagningen riktar sig mot ett avläsningsbart informationssystem som t.ex. tillhandahåller kommunikations- eller lagringstjänster som erbjuder flera personer får HDA endast användas för att få tillgång till den del som den

misstänkta personen använder eller har behörighet att använda (prop. 2019/2020:64 s 104 f.)

42. HDA enligt 10 § LHDA är inte kopplad till person, utan avser de fall där det är av synnerlig vikt att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott enligt 2 § inhämtningsslagen. Vad som får läsas av eller tas upp är kommunikationsövervaknings- och platsuppgifter. Vad gäller kommunikationsövervakningsuppgifter får det endast avse uppgifter i förfluten tid.
43. Som framgått tidigare, och som kommer att utvecklas i det följande, har försvaret inte någon insyn i den franska förundersökning där den aktuella åtgärden genomförts, och inte heller tillgång till det franska domstolsbeslut eller liknande, enligt vilket tillstånd ges till åtgärden. Vad försvaret kunnat utröna om de bakomliggande förhållandena grundar sig på olika källor såsom pressmeddelanden, uttalanden i media, promemorior från andra förundersökningar, muntliga kontakter med kollegor i bl.a. Frankrike m.m.
44. Som försvaret förstår det handlar åtgärden om genomförandet av HDA med anledning av misstankar som riktats mot företrädare för det holländska företaget EncroChatt. Åtgärden riktar sig emellertid inte mot kommunikationsenheter som används eller kan komma att användas av de misstänkta eller enheter som de misstänkta kan kontakta eller kan komma att kontakta. Istället riktar sig åtgärden mot ett stort antal personer som inte kan misstänkas för det aktuella brottet och som inte heller på någon rimlig grund kan förväntas ha kontakt med de misstänkta.
45. Den åtgärd som de franska brottsutredande myndigheterna genomfört är närmast urskillningslös när det kommer till vem den drabbar. Enligt uppgift har åtgärden berört 60 000 – 70 000 användare av Encrochatt runt om i världen. Faktum är att det förefaller mycket sannolikt att de franska brottsutredande myndigheterna inte ens visste vem som skulle bli föremål för HDA när åtgärden vidtogs, utöver den omständigheten att vederbörande använde en Encrotelefon. Huruvida det sedan var en journalist, advokat, politiker eller präst förefaller varit helt likgiltigt.
46. Enligt försvarets uppfattning är det helt uppenbart att en liknande åtgärd inte kunnat tillåtas enligt LHDA och således inte varit möjlig att genomföra enligt svensk rätt.

Det franska beslutet

47. Såvitt är känt i föreliggande fall har en fransk domstol i Lille beslutat om att tillåta franska myndigheter att föra in en programkod i EncroChatts server som var placerad i Lyon. Den franska domstolens beslut är att likställa med ett beslut om HDA enligt svensk rätt. Vidare har inte behöriga franska myndigheter underrättat Sverige enligt 4 kap, 13-15 §§ LEUO om att kommunikationsenheter kopplade till EncroChatt är föremål för avläsning eller upptagning under tid som de befinner sig på svenskt territorium. Följaktligen har inte heller en svensk domstol meddelat tillstånd till en sådan utredningsåtgärd
48. Som det får förstås har den franska domstolen tagit beslutet under en förundersökning mot företrädare för företaget EncroChatt eller företaget EncroChatt. Misstanken ska ha varit att företrädare för företaget EncroChatt eller företaget EncroChatt tillhandahöll en tjänst som utnyttjades av, och endast av, kriminella personer.
49. Exakt vilka straffbestämmelser enligt fransk lag som låg till grund för beslutet är inte känt. Det är inte heller känt om det franska domstolsbeslutet avsåg att läsa av eller ta upp kommunikation på servern eller om det även innefattade en möjlighet att läsa av och ta upp uppgifter från enskilda kommunikationsenheter. Inte heller är det känt om beslutet innehöll en prövning av det förhållandet att en avläsning eller upptagning av uppgifter från enskilda kommunikationsenheter med nödvändighet skulle medföra att franska myndigheter utövade exekutiv jurisdiktion i andra stater.
50. Det är inte heller möjligt att utifrån föreliggande material bedöma om den teknik som de franska brottsutredande myndigheterna använt sig av, d.v.s. att översända en programkod till enskilda enheter via servern, och därefter läsa av och ta upp uppgifter direkt från de enskilda enheterna, svarar mot de uppgifter som den franska domstolens tillstånd avser. Försvaret och en svensk domstol har således inte ens möjlighet att ta ställning till om villkoren i 23 § HDA är uppfyllda eller om även den bestämmelsen skulle kunna utgöra en grund för svensk domstol att inte tillåta åtgärden.

Rättsliga förutsättningar för att meddela tillstånd enligt LEUO

51. Förutsättningarna för att meddela tillstånd enligt LEUO för franska brottsutredande myndigheter att genomföra HDA i Sverige utan bistånd av behörig svensk myndighet är att gärningen är straffbar enligt svensk rätt och förutsättningarna för motsvarande åtgärd enligt svensk rätt är tillämpliga (4 kap. 14 § LEUO).

52. Utan kännedom om den gärningsbeskrivning eller motsvarande beskrivning av brottet som ligger till grund för den franska domstolens beslut kan det inte med säkerhet fastställas att den aktuella gärningen ens är straffbar enligt svensk nationell rätt. Allmänt kan sägas att det enligt svensk rätt kan vara straffbart att tillhandahålla kommunikationsutrustning i avsikt att den ska användas för att utföra ett brott. Det torde då handla om någon form av medhjälp till en brottslig gärning.
53. Problemet är, som försvaret ser det, att den kommunikation som skedde medelst Encrotelefoner inte varit tillgänglig för de brottsutredande myndigheterna på grund av krypteringen. Grunden för misstanken förefaller ha varit att misstänkta kriminella personer använt Encrotelefoner, och att Encrotelefoner därför kan misstänkas användas i kriminella verksamheter, snarare än misstankar om mer eller mindre konkreta brottsliga gärningar.
54. Under sådana förhållanden finns två möjligheter enligt LHDA att ge tillstånd till HDA, nämligen för att utreda vem som skäligen kan misstänkas för brottet (5 § LHDA) eller för att förebygga, förhindra eller upptäcka brottslig verksamhet (10 § HDA). I båda fallen kan tillståndet endast avse kommunikationsövervakningsuppgifter i förfluten tid. Någon möjlighet enligt svensk rätt att ge tillstånd till att läsa av eller ta upp kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter i realtid finns inte.
55. Tillämpningen av LHDA för att läsa av eller ta upp kommunikationsavlyssningsuppgifter förutsätter även att åtgärden riktar sig mot sådana avläsningsbara informationssystem som den misstänkta personen använder eller kan komma att använda eller, om det föreligger synnerligen anledning, kan kontakta eller kommer att kontakta. För det fall HDA riktar sig mot en server som tillhandahåller kommunikations- eller lagringstjänster till ett stort antal personer får åtgärden endast avse de delar som den misstänkta personen använder eller har behörig åtkomst till.
56. Som framhållits ovan har den aktuella åtgärden inte riktats mot kommunikationsenheter som används eller kan komma att användas av de misstänkta eller kommunikationsenheter som de misstänkta kan kontakta eller komma att kontakta, utan istället riktats helt urskillningslöst mot ett mycket stort antal individer som inte är misstänkta för brott och som inte heller kan kopplas till företrädarna för EncroChatt på annat sätt än att de använder EncroChatts kommunikationssystem. Någon möjlighet enligt LHDA att besluta om HDA avseende ett avläsningsbart informationssystem som

används av ett stort antal personer, av vilka den övervägande majoriteten, om ens någon, inte är misstänkta för brott, och som inte heller kan antas stå i kontakt med de misstänkta eller komma att stå i kontakt med de misstänkta, existerar inte enligt svensk rätt .

Den franska åtgärden är otillåten

57. Således kan konstateras att det är oklart om den gärning som ligger till grund för den franska domstolens beslut är straffbar enligt svensk rätt, och att den åtgärd som de franska myndigheterna använt sig av, d.v.s. att rikta HDA för att läsa av eller ta upp kommunikationsavlyssningsuppgifter mot personer som inte misstänks för brott, inte heller finns tillgänglig enligt svensk rätt. Det får därför anses uteslutet att en svensk domstol skulle tillåta utredningsåtgärden även om den blivit underrättad om den enligt 4 kap. 13 § LEUO.
58. De franska myndigheternas åtgärd att läsa av och ta upp uppgifter från avläsningsbara informationssystem som befunnit sig på svenskt territorium, och där användaren är många gånger svensk medborgare, har därför skett utan stöd i svensk lag eller traktat eller andra internationella instrument som reglerar frågan om exekutiv jurisdiktion mellan Sverige och Frankrike och innebär således en kränkning av den svenska suveräniteten.
59. Kränkningen är av synnerligen allvarlig karaktär, eftersom den varit urskillningslös och riktats mot ett stort antal individer utan hänsyn till svenska nationella intressen, som t.ex. yttrandefrihet, grundläggande fri- och rättigheter och säkerhet.

Rättsliga konsekvenser av den olovliga åtgärden

60. Varken LEUO eller LHDA innehåller uttryckliga bestämmelser om vad som gäller i ett fall där en annan stat läst av eller tagit upp uppgifter från en enhet som befinner sig på svenskt territorium utan att underrättelse skett och rätten gett tillstånd till åtgärden.
61. I 17 § HDA framgår att om uppgifter lästs av eller tagits upp av en svensk myndighet utan tillstånd från rätten och det inte i efterhand anses föreligga skäl att ge tillstånd till åtgärden får uppgifterna inte användas i en brottsutredning till nackdel för den som omfattas av åtgärden eller för någon annan som uppgifterna avser. Med det senare uttrycket avses t.ex. personer som omtalas i en kommunikation mellan två andra personer (prop. 2019/2020:34 s. 230 ff.)

62. En motsvarande bestämmelse finns intagen i 27 kap, 21 a § rättegångsbalken avseende hemlig avlyssning av elektronisk kommunikation. I förarbetena till den bestämmelsen uttalades att (prop. 2013/2014:237 s. 143 ff.):

”Regeringen anser därför att en begränsningsregel av det nu aktuella slaget är nödvändig för att säkerställa att ett förslag om utökade möjligheter till intermistiska beslut inte får negativa konsekvenser för enskildas rättssäkerhet. En sådan regel är således en förutsättning för att förslaget om interimistiska beslut ska kunna genomföras. Under sådana omständigheter anser regeringen att det får accepteras att begränsningsregeln i viss mån innebär en avvikelse från vad som normalt gäller i fråga om bevisrätten i brottmål. Det kan också påpekas att begränsningar i möjligheterna att använda information gäller även beträffande överskottsinformation från hemliga tvångsmedel”.

63. Uttalandet har relevans vid tillämpningen av motsvarande bestämmelser i LHDA, särskilt mot bakgrund av att lagstiftaren framhållit att HDA ska uppfattas som en verkställighetsåtgärd av det bakomliggande tvångsmedlet, i detta fall HAK, och att det HDA allmänt sett bör likställas med HAK (se t.ex. prop. 2019/20:64 s. 112 ff.)
64. Enligt försvarets uppfattning ska 17 § HDA tillämpas analogt i ett fall som detta där en annan stat har ägnat sig åt HDA utan tillstånd. De skäl som ligger bakom 17 § HDA gör sig lika starkt, om inte starkare, gällande i ett sådant fall. Inte minst de krav på dubbel straffbarhet och övriga förutsättningar för åtgärden som svensk lag enligt 14 § LEUO föreskriver understryker vikten av en domstolsprövning för att kunna upprätthålla de rättssäkerhetsgarantier som ska omgärda ett så pass ingripande tvångsmedel som HDA.
65. Som framhållits ovan har de franska brottsutredande myndigheterna genomfört åtgärden helt urskillningslöst, inte bara när det kommer till misstänkta och inte misstänkta, utan även till vilka kategorier av personer som avlyssnats (se 17 § LHDA) och vilka uppgifter som lästs av eller tagits upp (se 11 och 23 §§ LHDA) . Det finns således en påtaglig risk för att åtgärden utan tillstånd från svensk domstol har kommit att rikta mot sig mot ett mycket stort antal personer och verksamheter som det är förbjudet att använda åtgärden mot.
66. Här kan även tilläggas att det, allmänt sett, vore synnerligen olämpligt om en annan stat, utan tillstånd, skulle kunna använda sig av HDA mot t.ex. en svensk tidningsredaktion som befinner sig på svenskt territorium, och det materialet sedan, med kringgående av de

svenska bestämmelserna om källskydd och frågeförbud, skulle kunna åberopas av svenska åklagare i en brottmålsprocess.

67. Detta talar med styrka för att material som härrör från HDA som genomförts utan rättens tillstånd inte får användas i en brottmålsprocess, och det även i de fall där det är en utländsk myndighet som genomfört åtgärden och sedan lämnat över materialet till en svensk myndighet. Till det kommer även att åtgärden utgör en allvarlig kränkning av den svenska suveräniteten och har skett i direkt strid med gällande lag och de bakomliggande EU-rättsliga direktiven.

68. På de skäl som redovisas ovan ska även 17 § LHDA anses utgöra en lagstadgad inskränkning av principen om fri bevisföring och tillämpas analogt på fall där behöriga myndigheter i annan stat olovligen ägnat sig åt HDA på svenskt territorium utan tillstånd från svensk domstol. Sådana uppgifter som lästs av eller tagits upp utan tillstånd från rätten får inte användas i en brottsutredning och således inte heller åberopas som bevis i en rättegång mot den som omfattas av åtgärden eller för någon annan som uppgifterna avser.

69. Den aktuella bevisningen ska därför avvisas.

Kränkning av EKMR

70. Sedan 1994 är EKMR en del av svensk rätt och den har en särskild ställning i förhållande till övriga lagar och förordningar. Således ska tidigare lagar tolkas föredragskonformt och senare lagstiftning får inte stå i strid med EKMR.

71. Enligt artikel 8, 1 st. i EKMR äger svenska invånare rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Den Europeiska domstolen har fastslagit att hemlig avläsning av meddelanden på individers mobiltelefoner utgör ett ingrepp i nämnda rättigheter. Ett sådant ingrepp är endast godtagbar om den är förenlig med lag (artikel 8, 2 st. EKMR).

72. Den franska domstolens beslut som möjliggjort avläsningen är grundad på fransk lag. Som framhållits ovan är såväl fransk lag i denna del som innehållet i det franska domstolsbeslutet okänt för försvaret. Det går därför inte att ta ställning till om den åtgärd som faktiskt utfördes av de franska brottsutredande myndigheten är förenlig med fransk lag.

73. Som framhållits ovan är den åtgärd som de franska brottsutredande myndigheterna genomfört att likställa med sådana åtgärder som i svensk rätt regleras i LHDA. Vidare har tidigare framhållits att för det fall HDA genomförs avseende enheter eller uppgifter som befinner sig i Sverige av en annan stat, utan bistånd av den svenska staten, ska Sverige underrättas om åtgärden och en svensk domstol ge sitt tillstånd till den. I avsaknad av ett sådant tillstånd kan inte åtgärden under några förhållanden anses förenlig med svensk lag.
74. Således utgör den franska polisens avläsning och upptagning av meddelande från Encrotelefonerna en uppenbar kränkning av artikel 8 EKMR.
75. En kränkning av art 8 EKMR utgör i sig inte en grund för avvísning av bevisning, men kränkningen kan, tillsammans med övriga omständigheter, komma att anses utgöra även en kränkning av art 6 EKMR. Enligt den Europeiska domstolen ska i så fall den nationella rättsordningen erbjuda möjlighet till prövning om tillåtligheten av bevisning åtkommen i strid med artikel 8 (se p. 39, Case of Khan v. The United Kingdom, application no. 35394/97 (nedan "Khanmålet") och p. 79, case of P.G. and J.H. v. the United Kingdom, application no. 44787/98 (nedan "P.G-målet")).
76. I målet Schenk v. Switzerland, application no 0001}862/84 uttalade den Europeiska domstolen att:
- "While Article 6 of the Convention guarantees the right to a fair trial, it does not lay down any rules on the admissibility of evidence as such, which is therefore primarily a matter for regulation under national law.*
- The Court therefore cannot exclude as a matter of principle and in the abstract that unlawfully obtained evidence of the present kind may be admissible. It has only to ascertain whether Mr. Schenks trial as a whole was fair."* (p. 46).
77. Utifrån ett rättighetsperspektiv ska således inte bevisning tillåtas om den medför att rätten till en rättvis rättegång inte kan uppfyllas. Domstolen konstaterade sedan att i föreliggande fall hade inte art. 6 EKMR kränkts, eftersom följande kriterier (de s.k. Schenk-kriterierna) var uppfyllda.

(1) Schenk hade givits möjlighet att ifrågasätta äktheten (authenticity) av ljudinspelningen (p. 47)

(2) Schenk hade givits möjlighet att förhöra Pauty, som var den som genomförde avlyssningen (p. 47)

(3) Schenk hade avstått från att kalla polisinspektör Messerli som vittne, trots att denne ledde förundersökningen och var ansvarig för insamlandet av bevis (p. 47)

(4) Det faktum att ljudinspelningen inte utgjorde det enda beviset som domen grundade sig på och att det av domskälen framgår att domen även grundade sig på andra bevis än ljudinspelningen (p. 48)

78. Vad gäller *det första kriteriet* kan, som konstaterats ovan, försvaret inte ens fastställa om den utförda HDA:n varit förenlig med fransk rätt. Ännu mindre kan det i någon detalj fastställas hur åtgärden vidtagits, hur det avlästa och upptagna materialet har hanterats eller lagrats, inte heller vilka säkerhetsåtgärder som var på plats för att garantera en korrekt upptagning går att kontrollera. Försvaret kan inte heller kontrollera hur materialet hanterats i samband med att det överfördes till Sverige och vilka säkerhetsåtgärder som vidtogs för att säkerställa en korrekt överföring.
79. Vad gäller *det andra och tredje kriteriet* är det helt okänt för försvaret vem som läste av eller tog upp de aktuella uppgifterna, eftersom dessa åtgärder vidtogs av personal hos de franska brottsmyndigheterna och försvaret ges inte tillgång till de underliggande besluten m.m. som eventuellt skulle kunna fastställa deras identitet. Försvaret har överhuvudtaget någon insyn i den franska förundersökningen eller rätt till sådan insyn.
80. Vad gäller *det tredje kriteriet* så grundar sig bevisningen i föreliggande fall i allt väsentligt på de uppgifter som lästs av och tagits upp från de enskilda kommunikationsenheterna.
81. Enligt försvarets uppfattning är det uppenbart att de brister som föreligger inte går att avhjälpa under rättegången, eftersom försvaret inte kan få tillgång till det material som krävs för att kunna kontrollera och pröva den nu aktuella bevisningen.
82. Högsta domstolen har konstaterat att olovligen åtkommen bevisning inte måste leda till att den avvisas, utan istället kan effekten bli att den fränkänns värde (NJA 2007 s 1037). Det ska noteras att Högsta domstolen inte utesluter att sådan bevisning i vissa fall kan komma att avvisas.
83. Med hänvisning till att HDA är ett synnerligen ingripande och integritetskränkande hemligt tvångsmedel och det i LHDA föreskrivs i 17 § och 23 § att uppgifter som lästs

ADVOKATFIRMAN
JOHAN RAINER

av eller tagits upp utan tillstånd och/eller riktats mot förbjudna kategorier av personer är att anse som otillåten bevisning, vilket inskränker den fria bevisföringen, menar försvaret att om åtgärden även medför en kränkning av art. 6 EKMR, så ska den avvisas även på den grunden.

Stockholm som ovan,

Johan Rainer e.u. Ersin Aziman