Användning av hemlig dataavläsning i ett tvångsmedelsärende vid Åklagarkammaren i Linköping

Sammanfattning

Säkerhets- och integritetsskyddsnämnden har granskat användningen av hemlig dataavläsning i ett tvångsmedelsärende vid Åklagarkammaren i Linköping.

Vid granskningen har nämnden framför allt uppmärksammat att åklagarens ansökningar om hemlig dataavläsning inte varit tillräckligt specificerade. Ansökningarna har bl.a. omfattat sociala medier och andra internetbaserade tjänster. Något användarkonto eller någon på motsvarande sätt avgränsad del av tjänsterna har dock inte angetts. Det medför att delar av den prövning som ska göras av rätten i praktiken förskjuts till åklagaren eller den verkställande myndigheten. Det innebär också en förväxlingsrisk. Därmed bedömer nämnden att ansökningarna inte har utformats på ett sätt som är förenligt med lagen om hemlig dataavläsning.

Nämnden uttalar sig också gällande urvalet av de avläsningsbara informationssystem som omfattas av åklagarens ansökningar.

Postadress
Box 22523, 104 22 Stockholm

Telefon
08-617 98 00

E-post
sakint@sakint.se

Organisationsnummer
202100-5703

Besöksadress
Norr Mälarstrand 6, Stockholm

Telefax
08-617 98 88

Webbplats
www.sakint.se

Bankgiro
782-4329

1. Bakgrund

Säkerhets- och integritetsskyddsnämnden (nämnden) har underrättats om beslut om hemlig dataavläsning under en förundersökning. Nämnden beslutade att granska tvångsmedelsärendet såvitt avser hemlig dataavläsning för att kontrollera om det handlagts i enlighet med lag eller annan författning. Nämnden har endast granskat ansökningar och tillstånd som fanns i ärendet vid tiden för granskningens inledande.

2. Rättsliga utgångspunkter

Hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel läses av eller tas upp i ett avläsningsbart informationssystem. Med avläsningsbart informationssystem avses antingen en elektronisk kommunikationsutrustning (t.ex. en mobiltelefon eller en dator) eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst (1 § lagen [2020:62] om hemlig dataavläsning). De två typerna av avläsningsbara informationssystem benämns i vissa sammanhang fysiska respektive immateriella informationssystem.[1]

Ett tillstånd till hemlig dataavläsning får beviljas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse (3 § lagen om hemlig dataavläsning). En annan förutsättning för att hemlig dataavläsning ska tillåtas under en förundersökning är att åtgärden är av synnerlig vikt för utredningen (4 § första stycket lagen om hemlig dataavläsning).

Under en förundersökning får ett tillstånd till hemlig dataavläsning, med vissa undantag,[2] endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av någon som är skäligen misstänkt för det brott som ligger till grund för tvångsmedelsanvändningen (4 § andra stycket lagen om hemlig dataavläsning). Det avläsningsbara informationssystem som åtgärden avser ska anges i tillståndet (18 § första stycket 2 lagen om hemlig dataavläsning).

[1] Jfr prop. 2019/20:64 s. 57 och ”Hemliga tvångsmedel – hanteringen i vissa avseenden”, Åklagarmyndighetens rättsliga vägledning 2022:25, publicerad i augusti 2022, s. 55.

[2] Ett tillstånd får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta (4 § tredje stycket lagen om hemlig dataavläsning). Vidare får hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas endast avse ett avläsningsbart informationssystem som har använts vid ett brott eller i anslutning till en brottsplats vid brottstidpunkten eller som av någon annan anledning är av synnerlig vikt för utredningen (5 § andra stycket lagen om hemlig dataavläsning).

Enligt förarbetena betyder det att det i tillståndet måste anges vilket specifikt informationssystem tillståndet gäller för. När tillståndet gäller immateriella informationssystem anges lämpligen det användarkonto eller andra avgränsade delar av tjänsterna som åtgärden ska vidtas i. Det kan vara exempelvis en e-postadress eller ett användarnamn till ett konto på sociala medier eller annan internetbaserad tjänst. Uppgifterna måste i vart fall vara så specificerade att det går att verkställa åtgärden och att det är möjligt att bedöma kopplingen mellan informationssystemet och den som åtgärden avser, när sådan prövning krävs, för att förhindra förväxlingsrisk med andra informationssystem.[3]

3. Utredningen

3.1. Tvångsmedelsärendet

Av handlingarna i tvångsmedelsärendet framgår såvitt nu är av intresse följande. Ett antal misstänkta har varit föremål för hemlig dataavläsning inom ramen för en förundersökning gällande ett allvarligt brott. I åklagarens ansökningar och rättens tillstånd har de avläsningsbara informationssystemen kategoriserats som antingen fysiska eller immateriella informationssystem. Varje ansökan om och tillstånd till hemlig dataavläsning har omfattat ett fysiskt informationssystem och flera immateriella informationssystem. De fysiska informationssystemen har avsett mobiltelefoner som specificerats genom angivande av IMEI-nummer. De immateriella informationssystemen har angetts med namn på internetbaserade tjänster, bl.a. olika sociala medier, och inte genom att ett användarnamn eller liknande specificerats. Samtliga ansökningar och tillstånd har förenats med villkoret att avläsningen ska ske på sådant sätt att det innebär minsta möjliga integritetsintrång för den enskilde.

3.2. Remissfrågor och remissvar m.m.

Nämnden har i remiss till den ansvariga åklagaren ställt frågor om vilka delar av de angivna internetbaserade tjänsterna som omfattas av tvångsmedelsåtgärden och hur utformningen av ansökningarna förhåller sig till förarbetsuttalandena om att det avläsningsbara informationssystemet ska vara så speci-

[3] Prop. 2019/20:64 s. 232–233. Det krävs inte någon koppling mellan informationssystemet och den som åtgärden avser när hemlig dataavläsning används i syfte att utreda vem som skäligen kan misstänkas eller att förebygga, förhindra eller upptäcka brottslig verksamhet (5 § andra stycket respektive 10 § första stycket lagen om hemlig dataavläsning).

ficerat att det är möjligt att verkställa åtgärden och förhindra förväxlingsrisk. Åklagaren har sammanfattningsvis svarat följande.

> Ansökningarna har gjorts avseende en viss person, en viss fysisk enhet och vissa avläsningsbara informationssystem. Varje ansökan avser endast konton knutna till den aktuella personen kopplade till just den aktuella enheten. Information från andra fysiska enheter eller konton knutna till andra personer ger inte tillståndet rätt att få ut. Det föreligger därför inte någon förväxlingsrisk. Eftersom molntjänsterna är kopplade till ett specifikt IMEI-nummer är det endast de molntjänster som tillhör personen som kan hämtas in, d.v.s. rent tekniskt går det inte att hämta in någon annan persons data. Avläsningen är därför avgränsad till målpersonen, vilket är det som lagstiftaren varit noga med och det som är ändamålet bakom regleringen.

Vidare har nämnden frågat varför åklagaren valt ut de ifrågavarande immateriella informationssystemen. I den delen har åklagaren anfört att ansökningarna utformats på grundval av vad Polismyndigheten bedömt att det funnits förutsättningar att avläsa i de enskilda fallen. Åtgärden har enligt åklagarens bedömning varit proportionerlig i förhållande till brottets allvar.

Utöver det anförda har åklagaren besvarat frågor om bl.a. differentiering av de uppgiftstyper som ansökningarna omfattat och överväganden gällande användningen av villkor.[4]

Nämnden har med bistånd av Polismyndigheten kontrollerat verkställigheten av den hemliga dataavläsningen i ärendet. Nämnden har även anmodat Polismyndigheten att besvara skriftliga frågor i den delen.

4. Nämndens bedömning

4.1. Specificering av immateriella informationssystem

Vid rättens tillståndsprövning tecknas vanligtvis beslutet om tillstånd till ett hemligt tvångsmedel på åklagarens ansökningshandling. Ansökan får därmed betydelse för hur tillståndet utformas. Även om rätten[5] har det yttersta ansvaret för ett beslut om tillstånd anser nämnden att det åligger åklagaren att utforma ansökan så att den både uppfyller de formella kraven på vad ett tillstånd ska innehålla och ger korrekta förutsättningar för prövningen.[6]

---

[4] Differentiering står i fokus för nämndens granskning i ett pågående initiativärende (dnr 161-2022) och berörs därför inte närmare i detta uttalande.
[5] Nämndens tillsyn omfattar inte domstolarnas verksamhet.
[6] Se bl.a. nämndens uttalande den 21 juni 2021 ”Hanteringen av hemliga tvångsmedel vid åklagarkammaren i Eskilstuna” (dnr 136-2019).

I det aktuella ärendet har varje ansökan om hemlig dataavläsning utformats så att den avser en elektronisk kommunikationsutrustning i form av en mobiltelefon och ett antal internetbaserade tjänster. Något användarkonto eller någon på annat sätt avgränsad del av tjänsterna har inte angetts i ansökningarna. Utifrån ansökningarnas underlag (d.v.s. promemorior som upprättats av tjänstemän vid Polismyndigheten) är det möjligt att dra slutsatsen att de har avsett användarkonton som tillhör respektive misstänkt på de internetbaserade tjänsterna och som används genom den mobiltelefon som omfattas av respektive ansökan,[7] vilket överensstämmer med vad åklagaren har uppgett i remissvaret till nämnden.

Enligt nämndens mening innebär bestämmelsen i 18 § första stycket 2 lagen om hemlig dataavläsning att det avläsningsbara informationssystemet inte ska anges på ett sätt som förutsätter tillgång till underliggande handlingar och som möjliggör olika tolkningar. Det är därför problematiskt att åtgärdens omfattning inte uttryckligen framgår av ansökningar och tillstånd.

En annan fråga är om det är godtagbart att utforma en ansökan på det sätt som åklagaren har hävdat i remissvaret. I den delen gör nämnden följande bedömning.

Det är vanligtvis möjligt att på samma elektroniska kommunikationsutrustning använda flera olika användarkonton till en internetbaserad tjänst. Därmed uppstår en risk för förväxling när ett tillstånd avser en internetbaserad tjänst i den del den används med hjälp av en viss elektronisk kommunikationsutrustning. Om en misstänkt t.ex. tillfälligt lånar ut en av tillståndet omfattad dator till en annan person för att låta denne logga in och kontrollera sina meddelanden på en i tillståndet angiven internetbaserad tjänst, får det till följd att den andra personens konto på tjänsten utgör ett avläsningsbart informationssystem som omfattas av beslutet om hemlig dataavläsning. Enligt nämnden är en ansökan som möjliggör en sådan verkställighet inte förenlig med de ovan återgivna förarbetsuttalandena. I ljuset av det anförda framstår åklagarens svar om att det rent tekniskt inte är möjligt att hämta in någon annan persons data som en missuppfattning.

En tydlig brist med en ansökan som avser ett till den misstänkte hörande, men inte med användarnamn eller liknande specificerat, konto som finns på en internetbaserad tjänst och som används genom en viss elektronisk kommunikationsutrustning, är att delar av den prövning som ska tillkomma rätten i

[7] Enligt vad nämnden har kunnat iaktta inom ramen för andra granskningar finns det flera fall där åklagare utformat ansökningar om hemlig dataavläsning på detta sätt.

praktiken överlämnas till åklagaren eller den verkställande myndigheten. Rätten tar visserligen ställning till om det finns särskild anledning att anta att den elektroniska kommunikationsutrustningen har använts eller kommer att användas av den misstänkte. Rätten prövar emellertid inte huruvida det finns en tillräcklig koppling mellan den misstänkte och de immateriella informationssystem som används eller har använts genom den elektroniska kommunikationsutrustningen. Konsekvensen blir att det är åklagaren eller den verkställande myndigheten som prövar den kopplingen och avgör om åtgärden ska tillåtas i det enskilda fallet. Det kan argumenteras för att förväxlingsrisken är en aspekt som innefattas i rättens proportionalitetsbedömning enligt 3 § lagen om hemlig dataavläsning och att frågan om koppling mellan den misstänkte och de immateriella informationssystemen därmed omfattas av rättens prövning. I det sammanhanget måste det dock beaktas att rättens möjlighet att ta ställning till frågan om proportionalitet är begränsad när åtgärdens omfattning inte anges i ansökan. Eftersom det inte kan förutses vilka eller ens hur många immateriella informationssystem som tillståndet kommer att omfatta urholkas rättens möjligheter att göra en reell prövning.[8]

Sammantaget anser nämnden att det inte är förenligt med lagen om hemlig dataavläsning att ansökan och tillstånd utformas så att tvångsåtgärden avser ett till den misstänkte hörande, men inte med användarnamn eller liknande specificerat, konto som finns på en internetbaserad tjänst. Att tjänsten används med hjälp av en viss elektronisk kommunikationsutrustning är således inte tillräckligt.

4.2. Urval av avläsningsbara informationssystem

Ansökningarna om och tillstånden till hemlig dataavläsning har avsett flera olika internetbaserade tjänster. Remissvaret till nämnden kan uppfattas som att åklagarens urval av immateriella informationssystem i första hand har styrts av vilka tjänster som det varit tekniskt möjligt att få tillgång till genom åtgärden och inte av behovet av uppgifter från de olika tjänsterna i förhållande till utredningen av brottet.

Nämnden har på befintligt underlag inte anledning att ifrågasätta åklagarens bedömning gällande urvalet av de avläsningsbara informationssystem som omfattas av ansökningarna. Det finns dock skäl att framhålla vikten av att en

[8] Liknande resonemang har ansetts tala emot en ordning där tillstånd till hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan knytas enbart till den person som åtgärden avser, i stället för till ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning, se SOU 2018:30 s. 53–59 och prop. 2019/20:145 s. 9–14.

ansökan om hemlig dataavläsning utformas så att den inte avser fler informationssystem än vad det finns behov av med hänsyn till omständigheterna i det enskilda fallet. Om syftet med en ansökan om hemlig dataavläsning är att ta del av uppgifter från en av flera internetbaserade tjänster som kan tillgås bör inte ansökan avse användarkonton till samtliga tjänster, såvida inte åtgärden i alla delar är av synnerlig vikt för utredningen.

4.3. Övriga frågor

Användningen av villkor vid ansökan om hemlig dataavläsning granskas av nämnden i ett pågående initiativärende[9] och berörs därför inte närmare i detta sammanhang. Det kan dock framhållas att det i ärendet aktuella villkoret saknar betydelse för den bedömning som nämnden gör i avsnitt 4.1 och 4.2.

Nämndens bedömning i detta uttalande förändras inte heller av eventuella verkställighetstekniska aspekter. Som nämnden framhållit tidigare ska tekniska förutsättningar eller begränsningar i systemen inte vara avgörande för hur en ansökan om ett hemligt tvångsmedel utformas.[10]

Utöver det som anförts ovan har nämnden gjort vissa iakttagelser och ställt frågor gällande omständigheter som med hänsyn till vad som framkommit i ärendet och på grund av sekretesskäl inte återges i uttalandet.

5. Beslut

Med detta uttalande avslutas ärendet.

På Säkerhets- och integritetsskyddsnämndens vägnar

Gunnel Lindberg

I avgörandet har deltagit: Gunnel Lindberg (ordförande), Barbro Thorblad, Anti Avsan, Charlotta Bjälkebring Carlsson, Matheus Enholm, Elisabeth Falkhaven, Eva Flyborg, Christina Linderholm och Björn von Sydow (enhälligt).

Föredragande: Viktor Wallén

[9] Dnr 80-2022.
[10] Nämndens uttalande den 15 december 2021 ”Granskning av ärenden vid Åklagarmyndigheten i vilka hemlig dataavläsning använts” (dnr 92-2020).

Expedition till:
Åklagarkammaren i Linköping
Polismyndigheten, rättsavdelningen (dnr HD5900-24/2023)

För kännedom till:
Åklagarmyndigheten, tillsynsavdelningen
Linköpings tingsrätt