Användning av hemlig dataavläsning i ett tvångsmedelsärende vid Åklagarkammaren i Falun

Sammanfattning

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

Vid granskningen har nämnden uppmärksammat att åklagarens ansökningar om hemlig dataavläsning varit bristfälligt utformade. I ansökningarna har det inte angetts vilka internetbaserade tjänster som omfattas av tillståndet, utan endast att det är ”molntjänster” som avses. En sådan utformning medför svårigheter för rätten att göra en proportionalitetsbedömning och uppfyller inte kraven i 18 § lagen om hemlig dataavläsning.

Nämnden uttalar sig även om vikten av att åklagare har viss kunskap om verkställighet av hemlig dataavläsning inför en ansökan.

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 när granskningen inleddes.

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 bl.a. följande. Ett antal misstänkta har varit föremål för hemlig dataavläsning inom ramen för en förundersökning gällande allvarliga brott. Samtliga ansökningar om och tillstånd till hemlig dataavläsning har omfattat både fysiska och immateriella informationssystem. De fysiska informationssystemen anges med IMEI-nummer och de immateriella informationssystemen anges som molntjänster knutna till de aktuella IMEI-numren. Ansökningarna och tillstånden innefattar avläsning av uppgifter från tiden innan beslutsdagen och s.k. realtidsuppgifter. Samtliga tillstånd avser uppgiftstyperna i 2 § punkterna 1–3 och 6–7 lagen om hemlig dataavläsning. I alla tillstånd finns villkor med innebörden att särskild försiktighet ska iakttas beträffande överskottsinformation.

3.2. Remissfrågor och remissvar m.m.

Nämnden har i remiss till den ansvariga åklagaren bl.a. ställt frågor om överväganden kring vilka informationssystem som ansökningarna omfattat och hur de har specificerats. Även frågor om differentiering[4] av uppgiftstyper och överväganden gällande villkor för att begränsa integritetsintrånget har ställts. Åklagaren har sammanfattningsvis anfört följande.

[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).
[4] Differentiering enligt 2 § lagen om hemlig dataavläsning står i fokus för nämndens granskning i ett pågående initiativärende (dnr 161-2022) och berörs därför inte närmare i detta uttalande.

Det uppmärksammades i ärendet att de misstänkta använde applikationer för att kommunicera men det kunde inte klargöras vilka applikationer som användes. Innebörden av begreppet molntjänster diskuterades inte på sammanträdet. Det var omöjligt att på förhand få information om de tekniska förutsättningarna för verkställighet. Därför ansöktes om tillgång till fysiska och immateriella informationssystem. Även när besluten verkställdes lämnades ingen teknisk information om på vilket sätt verkställighet skedde. Det var inte praktiskt möjligt att mer detaljerat specificera informationssystemen i ansökningarna. Ansökningarna var proportionerliga och åtgärden av synnerlig vikt för utredningen. Villkorens innebörd och effekt kan jag inte uttala mig om då jag inte fick kunskap om vilken tillgänglig information som fanns och vad som inte inhämtades på grund av villkoren.

Nämnden har med bistånd av Polismyndigheten kontrollerat verkställigheten av tillstånden.

4. Nämndens bedömning

4.1. Immateriella informationssystem ska specificeras i ansökan

I det nu granskade ärendet har ansökningarna om hemlig dataavläsning avsett en mobiltelefon och inte närmare angivna internetbaserade tjänster (som i ansökan och tillstånd benämnts molntjänster). Vilka internetbaserade tjänster som skulle vara föremål för hemlig dataavläsning i enlighet med tillstånden har inte angivits.

Nämnden konstaterar att ansökningarna och tillstånden till hemlig dataavläsning inte är utformade på det sätt som lagen kräver, d.v.s. med angivande av det eller de immateriella avläsningsbara informationssystem som åtgärden avser (18 § första stycket 2 lagen om hemlig dataavläsning). Att det i ansökan framgår att tillståndet ska avse molntjänster, ett begrepp som inte definierades eller tydliggjordes vid sammanträdet, är således otillräckligt. Om det inte i ansökan specificeras vilka molntjänster eller internetbaserade tjänster som omfattas av ett tillstånd innebär det – förutom bristande lagenlighet – en ofullständighet och svårigheter för rätten att göra en korrekt proportionalitetsbedömning.

Utöver att det i tillstånden inte närmare anges vilka internetbaserade tjänster som omfattas av ansökningarna har inte heller något användarkonto eller på motsvarande sätt avgränsade delar av tjänsterna specificerats, varken i ansökningarna eller tillstånden. Nämnden har tidigare uttalat att även en sådan specificering är nödvändig, bl.a. för att möjliggöra en korrekt proportionalitets-

bedömning och utesluta förväxlingsrisk.[5] En hantering som innebär att det är otydligt vad som faktiskt omfattas av en ansökan och därmed också tillståndet till hemlig dataavläsning är inte godtagbar.

4.2. Åklagare behöver ha viss kunskap om verkställigheten

Åklagaren har gett uttryck för att, så som det får förstås, avsaknaden av information och kunskap om de tekniska möjligheterna för verkställighet av hemlig dataavläsning har påverkat utformningen av ansökan. På motsvarande sätt har åklagaren uttryckt att hon inte kunnat uttala sig om villkorens innebörd och effekt eftersom hon inte haft tillräcklig information.

Nämnden vill understryka att åklagaren har ansvar för de rättsliga överväganden och avvägningar som ska göras inför en ansökan om hemlig dataavläsning. Nämnden har tidigare uttalat att eftersom åklagaren är den som bäst känner ärendet är det angeläget att denne i samband med en ansökan om ett hemligt tvångsmedel noga överväger de närmare förutsättningarna för verkställighet.[6] Nämnden har förståelse för att hemlig dataavläsning kan vara tekniskt komplex men anser att en åklagare behöver ha viss kunskap om verkställigheten för att säkerställa en rättssäker tillämpning. Att på grund av otillräcklig kunskap eller information ansöka om ett mer omfattande tillstånd än nödvändigt är inte godtagbart. Det åligger också åklagaren att i varje enskilt fall överväga om och hur integritetsintrånget kan begränsas i samband med en ansökan om hemlig dataavläsning. Även det förutsätter enligt nämnden att åklagaren har kunskap om verkställigheten så att syftet med och effekten av ett av rätten fastställt villkor blir ändamålsenligt.[7]

5. Beslut

Med detta uttalande avslutas ärendet.

På Säkerhets- och integritetsskyddsnämndens vägnar

Gunnel Lindberg

---

[5] Se nämndens uttalande den 29 mars 2023 ”Användning av hemlig dataavläsning i ett tvångsmedelsärende vid Åklagarkammaren i Linköping” (dnr 43-2022).
[6] Se nämndens uttalanden den 21 juni 2021 ”Hanteringen av hemliga tvångsmedel vid åklagarkammaren i Eskilstuna” (dnr 136-2019) och den 15 december 2021 ”Granskning av ärenden vid Åklagarmyndigheten i vilka hemlig dataavläsning använts” (dnr 92-2020).
[7] Se även nämndens uttalande den 20 juni 2023 ”Användningen av villkor vid ansökan om hemlig dataavläsning” (dnr 80-2022).

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

Föredragande: Johanna Herder Toll

Expedition till:
Åklagarkammaren i Falun

För kännedom till:
Åklagarmyndigheten, tillsynsavdelningen
Polismyndigheten, rättsavdelningen
Falu tingsrätt