Otillåten tilläggsinformation och differentiering vid användning av hemlig dataavläsning

Sammanfattning

Säkerhets- och integritetsskyddsnämnden har granskat otillåten tilläggsinformation och differentiering av uppgiftstyper enligt lagen om hemlig dataavläsning. Nämnden har ställt frågor till Polismyndighetens rättsavdelning och Åklagarmyndigheten. Nämnden har även granskat ett urval av ansökningar och tillstånd till hemlig dataavläsning och ställt frågor till enskilda åklagare.

Nämnden har ingen erinran mot myndigheternas rutiner på området. Eftersom det, såvitt känt, hittills inte hänt att otillåten tilläggsinformation avlästs eller tagits upp går det dock inte att uttala sig om hur rutinerna gällande hantering av otillåten tilläggsinformation skulle fungera i praktiken.

Nämnden menar att det finns en otydlighet i lagstiftningen angående vilka uppgifter som omfattas av respektive uppgiftstyp i 2 § lagen om hemlig dataavläsning. Vissa uppgifter i ärendet talar vidare för att bestämmelsen om otillåten tilläggsinformation i 23 § lagen om hemlig dataavläsning påverkar hur ansökningar om hemlig dataavläsning utformas. Eftersom differentiering av uppgifter ingår som ett viktigt led i den proportionalitetsbedömning som alltid ska göras är det problematiskt.

Nämnden uttalar vidare att bestämmelsen om skyldighet att underrätta nämnden om otillåten tilläggsinformation i 23 § lagen om hemlig dataavläsning är en viktig rättssäkerhetsgaranti, trots att den hittills inte tillämpats.

Avslutningsvis konstaterar nämnden att enskilda åklagare lämnat svar som visar på bristande kunskap om hemlig dataavläsning. Nämnden förutsätter att det på kammarnivå säkerställs att rätt kunskap sprids i organisationen.

Innehåll

1. Bakgrund

Säkerhets- och integritetsskyddsnämnden (nämnden) har noterat att flertalet av ansökningarna om och tillstånden till hemlig dataavläsning utformas så att de omfattar alla uppgiftstyper i 2 § lagen (2020:62) om hemlig dataavläsning, med undantag för kameraövervaknings- och rumsavlyssningsuppgifter. Nämnden har tidigare uttalat att ansökningarnas utformning väcker frågan om behovet av uppgifter i varje enskilt fall varit styrande på det sätt som lagstiftaren avsett.[1]

I 23 § lagen om hemlig dataavläsning föreskrivs att nämnden ska underrättas i de fall där otillåten tilläggsinformation har lästs av eller tagits upp. Begreppet otillåten tilläggsinformation förekommer endast i förhållande till hemlig dataavläsning och det finns ingen motsvarighet i reglerna avseende de andra hemliga tvångsmedlen. Nämnden har inte vid något tillfälle hittills underrättats om otillåten tilläggsinformation.

2. Granskningen

Den 16 november 2022 beslutade nämnden att kontrollera om hanteringen av otillåten tilläggsinformation överensstämmer med lag eller annan författning samt om Polismyndigheten och Åklagarmyndigheten har ändamålsenliga rutiner på området. Nämnden beslutade att även kontrollera hur differentiering av uppgiftstyper i ansökningar om tillstånd till hemlig dataavläsning hanteras i förhållande till regleringen om otillåten tilläggsinformation.

Nämnden har ställt frågor till Polismyndighetens rättsavdelning och till Åklagarmyndigheten. Nämnden har även, utifrån sin fortlöpande granskning av de underrättelser om beslut enligt 21 § lagen om hemlig dataavläsning som kommit in under år 2022, valt ut 19 ansökningar och tillstånd till hemlig dataavläsning för granskning. Med beaktande av geografisk spridning har nämnden då valt ut dels ett antal ansökningar och tillstånd som omfattar alla uppgiftstyper i 2 § lagen om hemlig dataavläsning med undantag för kameraövervaknings- och rumsavlyssningsuppgifter, dels ett antal ansökningar och tillstånd som gett intryck av att åklagaren gjort en specifik differentiering utifrån behovet av uppgifter. Kopior av relevanta handlingar i ärendena har begärts in till nämndens kansli. Ansvariga åklagare, eller i förekommande fall, kammarledningen, har skriftligen besvarat frågor.

[1] Se nämndens uttalande den 15 december 2021 ”Granskning av ärenden vid Åklagarmyndigheten i vilka hemlig dataavläsning använts” (dnr 92-2020).

Frågor om verkställighet av hemlig dataavläsning har ställts till de enskilda åklagarna. Nämnden har dock inte, inom ramen för denna granskning, kontrollerat verkställigheten av tillstånden hos verkställande myndighet.

3. Rättsliga utgångspunkter

Hemlig dataavläsning innebär att de brottsbekämpande myndigheterna med hjälp av någon form av tekniskt hjälpmedel i hemlighet bereder sig tillgång till en teknisk utrustning som kan användas för elektronisk kommunikation och därigenom får besked om hur utrustningen används eller har använts och vilken information som finns i den (1 § lagen om hemlig dataavläsning).

Det är i normalfallet en åklagare som ansöker om tillstånd till hemlig dataavläsning och rätten som beslutar om tillstånd till tvångsmedelsanvändning (14–15 §§ lagen om hemlig dataavläsning).

I 2 § lagen om hemlig dataavläsning anges vilka typer av uppgifter som får läsas av eller tas upp. I ett tillstånd till hemlig dataavläsning ska det enligt 18 § första stycket 3 lagen om hemlig dataavläsning anges vilken typ av uppgift som enligt 2 § första stycket får läsas av eller tas upp.

Kommunikationsavlyssningsuppgifter (punkt 1) är uppgifter om innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon annan adress. Uppgifterna motsvarar de som får hämtas in genom hemlig avlyssning av elektronisk kommunikation (27 kap. 18 § RB).

Kommunikationsövervakningsuppgifter (punkt 2) är uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon annan adress. Dessa uppgifter motsvarar de uppgifter som får hämtas in genom bl.a. hemlig övervakning av elektronisk kommunikation (27 kap. 19 § första stycket 1 RB).

Platsuppgifter (punkt 3) avser uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits. Uppgifterna är till sin typ sådana som får hämtas in genom bl.a. hemlig övervakning av elektronisk kommunikation (27 kap. 19 § första stycket 3 RB).

Med kameraövervakningsuppgifter (punkt 4) avses uppgifter som framkommer genom optisk personövervakning. Det motsvarar sådana uppgifter som får hämtas in genom hemlig kameraövervakning (27 kap. 20 a § RB).

Rumsavlyssningsuppgifter (punkt 5) är uppgifter som avser tal i enrum, samtal mellan andra, eller förhandlingar vid sammanträden eller andra samman-

komster som allmänheten inte har tillträde till. Uppgifterna motsvarar de som får hämtas in genom hemlig rumsavlyssning (27 kap. 20 d § RB).

Lagrade uppgifter (punkt 6) är uppgifter som finns lagrade i ett avläsningsbart informationssystem men som inte avses i punkterna 1–5. Lagringstjänster kan t.ex. vara sådana tjänster som möjliggör lagring av data på annan plats än i den egna elektroniska kommunikationsutrustningen, s.k. molntjänster. Lagrade uppgifter enligt punkten 6 kan exempelvis handla om kontaktuppgifter i telefonboken, fotografier, inloggningsuppgifter, utkast till meddelanden och program- eller systemfiler.

Uppgifter enligt punkten 7 är uppgifter som visar hur den tekniska utrustningen används men som inte avses i punkterna 1–6. Det kan exempelvis handla om användning som inte leder till att information lagras, t.ex. vilka program och applikationer i en mobiltelefon som körs, anteckningar som görs och utkast till meddelanden som inte sparas.[2]

Vid all tvångsmedelsanvändning gäller ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. Proportionalitetsprincipen innebär att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden. I lagen om hemlig dataavläsning regleras proportionalitetsprincipen i 3 §. I förarbetena anges att principen kan få särskild betydelse när en ansökan om hemlig dataavläsning avser flera uppgiftstyper eftersom integritetsriskerna då blir större för den enskilde.[3] Behovet av uppgifter i varje enskilt fall bör enligt förarbetena vara styrande för vad hemlig dataavläsning får användas för. Detta benämns att åtgärden ska differentieras. Det anges vidare att det endast undantagsvis och bara i de allra allvarligaste fallen, t.ex. vid terroristbrottslighet eller annan mycket allvarlig brottslighet, bör vara möjligt att få tillstånd till avläsning eller upptagning av samtliga uppgiftstyper samtidigt.[4]

Enligt 23 § första stycket lagen om hemlig dataavläsning ska den teknik som används i samband med hemlig dataavläsning anpassas efter det tillstånd som beviljats. Tekniken får inte göra det möjligt att läsa av eller ta upp någon annan typ av uppgift än vad som anges i tillståndet, s.k. otillåten tilläggsinformation.[5] Det innebär t.ex. att om ett tillstånd endast tillåter hemlig dataavläsning för kommunikationsavlyssningsuppgifter ska det inte vara möjligt att läsa av eller

[2] Prop. 2019/20:64 s. 214.
[3] Prop. 2019/20:64 s. 110.
[4] Prop. 2019/20:64 s. 110.
[5] Prop. 2019/20:64 s. 237.

ta upp kameraövervakningsuppgifter.[6] Om ett tekniskt hjälpmedel är konstruerat på så sätt att det i och för sig är möjligt att använda det för att läsa av eller ta upp olika uppgiftstyper krävs att hjälpmedlet är inställt på ett sådant sätt att det inte är möjligt att utan ändringar av inställningarna i hjälpmedlet komma åt andra uppgiftstyper än de som tillståndet avser.[7] I 23 § första stycket anges vidare att om otillåten tilläggsinformation lästs av eller tagits upp ska upptagningar och uppteckningar av dessa uppgifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas.

I 2 § förordningen (2020:172) om hemlig dataavläsning föreskrivs att verkställande myndighet skyndsamt ska underrätta åklagaren om otillåten tilläggsinformation har lästs av eller tagits upp. Åklagaren ska därefter skyndsamt underrätta nämnden.

4. Nämndens iakttagelser och bedömning

4.1. Myndigheternas riktlinjer och rutiner

4.1.1 Riktlinjer och rutiner om differentiering och otillåten tilläggsinformation

En del i nämndens granskning har varit att kontrollera om Polismyndigheten och Åklagarmyndigheten har riktlinjer eller rutindokument som rör differentiering av uppgiftstyper respektive hantering av otillåten tilläggsinformation.

Åklagarmyndigheten har redogjort för att myndigheten på sitt intranät publicerat vägledande styrdokument som berör såväl rättslig som praktisk tillämpning samt där även publicerat vägledande lagkommentarer till lagen om hemlig dataavläsning. Nämnden har inom ramen för denna granskning inte tagit del av Åklagarmyndighetens styrdokument.

Polismyndigheten har angett att myndigheten har dokumenterade rutiner för hur hemlig dataavläsning ska verkställas som bl.a. syftar till att förhindra att otillåten tilläggsinformation läses av. Polismyndigheten har bifogat ett tillfälligt rutindokument beträffande vissa arbetsmoment. Myndigheten har vidare upplyst om att det, såvitt känt, aldrig har hänt att otillåten tilläggsinformation har avlästs eller tagits upp. När det gäller differentiering av uppgiftstyper har Polismyndigheten anfört att sådan främst är hänförlig till frågan om hur ett tillstånd till hemlig dataavläsning bör utformas, samt att detta är ett ansvar som i första hand åligger åklagaren och rätten och att

[6] Prop. 2019/20:64 s. 236.
[7] Prop. 2019/20:64 s. 236 f.

myndigheten därför inte har upprättat något rutindokument gällande det. Myndigheten har tillagt att inför en ansökan om hemlig dataavläsning förs en dialog mellan polis och åklagare, varvid utformningen av tillståndet kan komma att diskuteras.

Nämnden har, utifrån de svar som Polismyndigheten och Åklagarmyndigheten lämnat, ingen invändning mot myndigheternas rutiner på området. Eftersom det såvitt känt hittills inte har hänt att otillåten tilläggsinformation avlästs eller tagits upp, går det emellertid inte att uttala sig om hur rutinerna gällande hantering av otillåten tilläggsinformation skulle fungera i praktiken. Nämnden anser att det är godtagbart att Polismyndigheten saknar skriftliga riktlinjer angående differentiering av uppgiftstyper. Det är dock viktigt att Polismyndigheten har den kompetens som krävs för att förmedla till enskilda åklagare vilken information som kan läsas av eller tas upp vid verkställighet av de olika uppgiftstyperna.

4.1.2 Polismyndighetens rutiner kring teknikanpassning

Nämnden har, mot bakgrund av bestämmelsen i 23 § första stycket lagen om hemlig dataavläsning, ställt frågor till Polismyndigheten om myndighetens rutiner kring teknikanpassning. Polismyndigheten har redogjort för på vilket sätt den uppfyller lagens krav på teknikanpassning.

Nämnden har ingen erinran mot Polismyndighetens svar i denna del. Det kan tilläggas att nämndens granskning inte har innefattat praktiska eller rent tekniska aspekter av verkställigheten. Nämnden saknar därför underlag för att uttala sig om själva teknikanpassningen.

4.2. Differentiering av uppgiftstyper

4.2.1 Det finns en viss otydlighet i lagstiftningen

Polismyndigheten har i sitt remissvar till nämnden anfört att myndigheten anser att det finns en otydlighet angående vilka uppgifter som omfattas av respektive uppgiftstyp i 2 § lagen om hemlig dataavläsning. Som exempel har myndigheten angett att det finns svårigheter att bedöma vilka uppgifter som ska hänföras till lagrade uppgifter (punkt 6) respektive användningsuppgifter (punkt 7). Myndigheten har hänvisat till förarbetsuttalandet om att användningsuppgifter (punkt 7) kan innefatta vilka program eller appar som körs, anteckningar som görs och utkast till meddelanden som inte sparas.[8] Enligt tekniskspecialister inom Polismyndigheten lagras emellertid de i

[8] Prop. 2019/20:64 s. 214.

förarbetena exemplifierade uppgifterna, om än tillfälligt (genom t.ex. internminnet eller processorn), vilket innebär att uppgifterna även bör rymmas under punkt 6. Myndigheten har uppgett att förhållandet kompliceras eftersom uppgifter enligt punkt 6 och 7 även innehåller metadata i form av övervaknings- och platsuppgifter (punkt 2 och 3). Polismyndigheten har anfört att detta innebär att även sådana uppgifter behöver omfattas av ett tillstånd till hemlig dataavläsning, eftersom lagrade uppgifter och användningsuppgifter (punkt 6 och 7) är sekundära till de övriga uppgifterna. Myndigheten har som ytterligare exempel på gränsdragningsproblem angett att brottsbekämpande myndigheter diskuterat om t.ex. meddelanden och e-post som inte är under befordran ska anses utgöra lagrade uppgifter (punkt 6) eller kommunikationsavlyssningsuppgifter (punkt 1). Enligt Polismyndigheten har lagstiftaren inte i tillräcklig utsträckning insett i vilken omfattning uppgiftstyperna överlappar varandra och de svårigheter detta medför när det gäller att upprätthålla krav på differentiering.

Även Åklagarmyndigheten har uttryckt att det finns viss oklarhet angående vilka uppgifter som omfattas av respektive uppgiftstyp i 2 § lagen om hemlig dataavläsning. Särskilt har myndigheten angett att det inte är helt klart om en uppgift ska anses vara en kommunikationsavlyssningsuppgift (punkt 1) eller en lagrad uppgift (punkt 6) när användaren har bearbetat eller vidtagit någon åtgärd med ett mottaget meddelande. Som exempel har Åklagarmyndigheten nämnt att ett inkommet meddelande i en e-postserver är en kommunikationsavlyssningsuppgift (punkt 1) men att det, om ett sådant meddelande sparas ned i en mapp på datorn, är oklart om det alltjämt är en kommunikationsavlyssningsuppgift eller om det blivit en lagrad uppgift (punkt 6).

De flesta av de enskilda åklagarna har i sina remissvar angett att de inte har stött på några problem vid valet av uppgiftstyper enligt 2 § lagen om hemlig dataavläsning. Endast två av 15 åklagare har svarat att de anser att det finns otydligheter. Den ena av dessa åklagare har uttryckt att det inte är alldeles enkelt att få grepp om vad som avses med formuleringen i punkt 6 om lagrade uppgifter och att han därför kontaktar handläggare vid Polismyndigheten för att vinna mer klarhet i vilken information det går att få fram och vad som undantas vid respektive uppgiftstyp.[9] Den andra har uppgett att användningsuppgifter (punkt 7) är svåra att skilja från övriga uppgiftstyper bl.a. eftersom sådana uppgifter också kan tänkas förekomma som kommunikationsavlyssnings- eller övervakningsuppgifter (punkt 1 och 2).[10]

[9] Ärendet har handlagts vid åklagarkammaren i Gävle.
[10] Ärendet har handlagts vid åklagarkammare i Malmö.

Gemensamt för svaren från åklagarna är att de har uttryckt att behovet av information styr vilka uppgifter de anger i en ansökan om hemlig dataavläsning. Ingen åklagare har anfört att valet av uppgiftstyper i de granskade ärendena berott på otydlighet i uppdelningen av uppgiftstyper. En åklagare, som låtit ansökan om hemlig dataavläsning omfatta punkterna 1–3 och 6–7, har framhållit att det är svårt att på förhand veta vilken information som kan vara relevant för brottet och att det påverkar utformningen av ansökan i fråga om val av uppgiftstyper.[11]

Uppgifterna till nämnden från Polismyndigheten och Åklagarmyndigheten visar att regleringen om uppgiftstyperna i 2 § lagen om hemlig dataavläsning i viss mån uppfattas som otydlig. Att de flesta av de tillfrågade åklagarna uppgett att de inte haft problem vid valet av uppgiftstyper torde delvis kunna förklaras av att ansökningar om hemlig dataavläsning i regel omfattar flera av uppgiftstyperna och att åklagarna därför inte behövt ställas inför gränsdragningsproblem. Det kan dock inte vara hela förklaringen och det är givetvis positivt att flertalet av de tillfrågade åklagarna inte upplever några problem vid valet av uppgiftstyper. Nämnden anser vidare att det är en god ordning att åklagare kontaktar verkställande myndighet för att reda ut eventuella oklarheter.

Differentiering av uppgifter ingår som ett viktigt led i den proportionalitets-bedömning som alltid ska göras. Det är mot den bakgrunden problematiskt att regleringen om uppgiftstyper uppfattas som otydlig. En särskild utredare har för närvarande i uppdrag att utvärdera lagen om hemlig dataavläsning och ta ställning till om den bör permanentas och om den i så fall bör ändras i något avseende.[12] Polismyndigheten har uppgett att den påtalat problem kring bl.a. gränsdragningar och differentiering för utredningen.

4.2.2 Det finns inte problem att verkställa endast få uppgiftstyper

Polismyndigheten och Åklagarmyndigheten har på fråga från nämnden uppgett att det inte finns några problem med att verkställa tillstånd som endast innefattar en eller ett fåtal uppgiftstyper. Polismyndigheten har framhållit att de uppgifter som det vanligen finns ett behov av emellertid innebär att tillståndet behöver omfatta flera uppgiftstyper för att den hemliga dataavläsningen ska ge den effekt som brottsutredningarna behöver. Åklagarmyndigheten har angett att gällande rutin är att inför en ansökan om hemlig dataavläsning kontakta verkställande myndighet för att undersöka om

[11] Ärendet har handlagts vid åklagarkammaren i Gävle.
[12] Utredningen om utvärdering av hemlig dataavläsning (Ju 2022:07).

verkställighet är möjlig. Åklagarmyndigheten har även anfört att om beslutet endast går att verkställa på ett sätt som innebär att information utöver de uppgiftstyper som ansökan ska omfatta kommer att hämtas in, och det inte motiveras av utredningsskäl, bör åklagaren överväga att avstå från ansökan.

Av de tillfrågade åklagarna har tre uppgett att de inte kan uttala sig om huruvida det finns problem vid verkställighet av tillstånd som endast innefattar en eller ett fåtal uppgiftstyper då de saknar erfarenhet av eller inte har någon uppfattning i frågan.[13] Fyra åklagare har svarat att det finns problem men lämnat svar som inte direkt handlar om svårighet att verkställa tillstånd med få uppgiftstyper. En av dessa åklagare har angett att det finns behov av att avläsa lagrad information så snart som möjligt, eftersom sådan information kan komma att ändras eller raderas och därigenom bli oåtkomlig.[14] En annan har konstaterat att det, trots att verkställigheten är lyckad, generellt kan vara svårt att få fram all information som eventuellt finns på grund av tekniska aspekter av verkställighet av hemlig dataavläsning.[15] Två åklagare har gett uttryck för att det finns tekniska svårigheter att vid verkställigheten begränsa tillgång till viss information.[16]

Nämnden konstaterar att svaren från de enskilda åklagarna talar för att det finns vissa svårigheter vid verkställighet av hemlig dataavläsning. Svaren talar dock inte för att det finns svårigheter att verkställa endast få uppgiftstyper i 2 § lagen om hemlig dataavläsning. Enligt nämndens mening saknas det anledning att ifrågasätta de uppgifter som lämnats av Polismyndigheten, dvs. den verkställande myndigheten. Nämnden utgår således från att det inte finns problem att verkställa endast få uppgiftstyper, vilket också stämmer överens med vad som angetts av Åklagarmyndigheten och flertalet av de tillfrågade åklagarna. Detta är givetvis positivt.

Nämnden konstaterar emellertid att den omständigheten att vissa åklagare inte kunnat svara på nämndens fråga visar på okunskap om verkställighet av hemlig dataavläsning. Som nämnden tidigare uttalat har nämnden 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.[17] En förutsättning för en rättssäker tillämpning är

[13] Ärendena har handlagts vid åklagarkammaren i Östersund, Söderorts åklagarkammare och åklagarkammaren i Örebro.
[14] Ärendet har handlagts vid åklagarkammaren i Malmö.
[15] Ärendet har handlagts vid åklagarkammaren i Gävle.
[16] Ärendena har handlagts vid Norrorts åklagarkammare.
[17] Nämndens uttalande den 20 juni 2023 ”Användning av hemlig dataavläsning i ett tvångsmedelsärende vid Åklagarkammaren i Falun” (dnr 44-2022).

vidare att det finns en tydlig kommunikation kring frågor om verkställighet mellan ansökande åklagare och verkställande myndighet.

4.3. Otillåten tilläggsinformation

4.3.1 Innebörden av otillåten tilläggsinformation är tydlig

Nämnden har ställt frågor till Polismyndigheten och Åklagarmyndigheten om innebörden av otillåten tilläggsinformation i 23 § lagen om hemlig dataavläsning. Båda myndigheterna har svarat att begreppet otillåten tilläggsinformation är begränsat till de olika uppgiftstyperna i 2 § lagen om hemlig dataavläsning. Enligt myndigheterna rör bestämmelsen om otillåten tilläggsinformation alltså uteslutande vilka typer av uppgifter som får läsas av eller tas upp genom en hemlig dataavläsning, inte t.ex. avläsning eller upptagning utöver angivna tidsperioder eller villkor. Nämnden delar myndigheternas bedömning som får stöd av såväl ordalydelsen i 23 § lagen om hemlig dataavläsning som förarbetena till bestämmelsen.[18]

4.3.2 Frågan om bestämmelsen om otillåten tilläggsinformation påverkar utformningen av en ansökan

Nämnden har frågat Polismyndigheten, Åklagarmyndigheten och åklagarna i de enskilda ärendena om de är av uppfattningen att bestämmelsen om otillåten tilläggsinformation i 23 § lagen om hemlig dataavläsning påverkar hur en ansökan om hemlig dataavläsning kan utformas.

Polismyndigheten har angett att det finns vissa svårigheter att förhålla sig till förarbetsuttalandena om att ett tillstånd till hemlig dataavläsning ska differentieras i varje enskilt fall utan att samtidigt riskera att avläsa otillåten tilläggsinformation. Myndigheten har betonat att detta inte beror på att den saknar möjlighet att anpassa tekniken utan på de otydligheter som finns beträffande innebörden av uppgiftstyperna i 2 § lagen om hemlig dataavläsning och överlappningarna av respektive uppgiftstyp. Problemen med gränsdragningar och överlappningar har enligt Polismyndigheten medfört att flertalet av tillstånden till hemlig dataavläsning utformats likformigt och att differentiering av tillstånd i viss mån har fått stå tillbaka i förhållande till vikten av att verkställigheten ska vara lagenlig.

Åklagarmyndigheten har å sin sida framhållit att bestämmelsen om otillåten tilläggsinformation varken ska påverka eller påverkar hur en ansökan om tillstånd till hemlig dataavläsning utformas i fråga om behovet av de olika

[18] Prop. 2019/20:64 s. 236 f.

uppgiftstyperna. Att flera ansökningar omfattar flertalet uppgiftstyper, undantaget kameraövervakningsuppgifter och rumsavlyssningsuppgifter, beror enligt Åklagarmyndigheten på att det oftast är av väsentlig betydelse för utredningen att ta del av fler än en uppgiftstyp.

Även svaren från de enskilda åklagarna går isär. Flertalet av åklagarna har framhållit att bestämmelsen om otillåten tilläggsinformation inte påverkat utformningen av ansökan om hemlig dataavläsning i de granskade ärendena. Två åklagare har, som det får förstås, angett att bestämmelsen om otillåten tilläggsinformation kan påverka hur ansökan om hemlig dataavläsning utformas och därtill resonerat kring verkställande myndigheters tekniska möjligheter att begränsa tillgången till information i vissa fall och dragit slutsatsen att det bl.a. är viktigt att tillstånden omfattats av villkor.[19] En åklagare har uppgett att hon beaktat bestämmelsen om otillåten tilläggsinformation vid ansökan om tillstånd men att hon rätteligen skulle ha utformat ansökan tydligare.[20] En annan åklagare har framfört att risken för otillåten tilläggsinformation i det granskade ärendet var försumbar eftersom ansökan endast avsåg förfluten tid och beslagtagna telefoner.[21]

Nämnden har inte funnit någon tydlig förklaring till varför myndigheterna uttryckt så olika uppfattning i frågan. Polismyndighetens svar talar för att bestämmelsen om otillåten tilläggsinformation i viss mån kan vara en bidragande orsak till att flertalet av ansökningarna utformas så att de omfattar alla uppgiftstyper i 2 § lagen om hemlig dataavläsning, med undantag för kameraövervaknings- och rumsavlyssningsuppgifter. Eftersom Åklagarmyndigheten uttryckt motsatt uppfattning och inte heller svaren från de enskilda åklagarna ger en tydlig bild, är det dock inte klarlagt om bestämmelsen om otillåten tilläggsinformation faktiskt påverkar valet av uppgiftstyper.

De redovisade svaren från enskilda åklagare visar däremot att det finns viss okunskap gällande vad som utgör otillåten tilläggsinformation. Som konstateras ovan är begreppet otillåten tilläggsinformation endast kopplat till valet av uppgiftstyper, vilket innebär att frågan om uppgifter är i realtid eller om telefoner är tagna i beslag saknar betydelse i sammanhanget. Vidare bör ett villkor inte direkt kunna hindra förekomsten av otillåten tilläggsinformation. Slutligen behandlar 23 § lagen om hemlig dataavläsning i huvudsak förhållanden som verkställande myndighet ansvarar för, varför det

[19] Ärendena har handlagts vid Norrorts åklagarkammare.
[20] Ärendet har handlagts vid åklagarkammaren i Östersund.
[21] Ärendet har handlagts vid åklagarkammaren i Malmö.

inte är något som åklagaren särskilt ska beakta i ansökan. Det är Polismyndigheten som i praktiken identifierar otillåten tilläggsinformation. Nämnden anser dock att det är av stor vikt att åklagaren har kunskap om begreppet, särskilt med beaktande av att det är åklagaren som ska anmäla till nämnden om otillåten tilläggsinformation lästs av eller tagits upp (2 § förordningen [2020:172] om hemlig dataavläsning).

5. Avslutande synpunkter

Nämnden har hittills inte underrättats om otillåten tilläggsinformation och Polismyndigheten har uppgett att sådan information aldrig avlästs eller tagits upp. Att det, såvitt känt, inte hänt att otillåten tilläggsinformation avlästs eller tagits upp är givetvis i sig mycket positivt och kan bero på faktorer som Polismyndighetens verkställighetsmetod och de brottsbekämpande myndigheternas rutiner. Av granskningen har det inte framkommit något som talar för att Polismyndighetens eller enskilda åklagares hantering varit bristfällig i detta avseende. Trots att bestämmelsen om underrättelseskyldighet i 23 § lagen om hemlig dataavläsning således hittills inte har tillämpats anser nämnden att den utgör en viktig rättssäkerhetsgaranti.

Nämndens granskning visar att en förklaring till att flertalet av ansökningarna om och tillstånden till hemlig dataavläsning utformas så att de omfattar alla uppgiftstyper i 2 § lagen om hemlig dataavläsning med undantag för kameraövervaknings- och rumsavlyssningsuppgifter kan vara att det är otydligt vad som omfattas av vissa uppgiftstyper. Att det, såvitt känt, aldrig hänt att otillåten tilläggsinformation avlästs eller tagits upp sedan lagen trädde i kraft kan också tala för att osäkerhet i val av uppgiftstyper gått ut över differentieringen. Vidare har Polismyndigheten gett uttryck för att bestämmelsen om otillåten tilläggsinformation i viss mån påverkar differentieringen. Eftersom differentieringen är en del av den proportionalitetsbedömning som alltid ska göras anser nämnden att det är problematiskt. Som framgår av detta uttalande har Polismyndigheten påtalat problem med gränsdragningar, differentieringar och otillåten tilläggsinformation för Utredningen om utvärdering av hemlig dataavläsning.

Avslutningsvis bör några i granskningen gjorda särskilda iakttagelser belysas. Vissa åklagare har uttryckligen uppgett att de inte kan svara på nämndens frågor, eftersom att de saknar kunskap på området. Andra åklagare har lämnat svar som visar på bristande kunskap om hemlig dataavläsning, vilket särskilt har uppmärksammats vid nämndens frågor om verkställighet. Enligt nämnden är detta anmärkningsvärt. Som nämnden tidigare uttalat måste en åklagare ha viss kunskap om verkställighet av hemlig dataavläsning för att

säkerställa en rättssäker tillämpning.[22] Vid granskningen har det vidare framkommit felaktigheter i enskilda åklagares hantering av hemlig dataavläsning. Till exempel har åklagaren i ett fall, av förbiseende, kryssat i kameraövervakningsuppgifter (punkt 4) i stället för platsuppgifter (punkt 3) i ansökan, vilken sedan beviljats av rätten.[23] I ett annat fall har ett tillstånd felaktigt, på grund av ansökans utformning, kommit att omfatta punkterna 6 och 7 trots begränsningen i nuvarande 4 a § andra stycket lagen om hemlig dataavläsning.[24] Nämnden har förståelse för att ansökan om hemlig dataavläsning ofta ges in skyndsamt men vill framhålla vikten av noggrannhet och att ansökan blir korrekt eftersom beslutet fattas på samma handling. Trots att de ovan nämnda besluten enligt åklagarna aldrig kom att verkställas ser nämnden allvarligt på det inträffade. Nämnden förutsätter att det på kammarnivå säkerställs att rätt kunskap om hemlig dataavläsning sprids i organisationen.

6. 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, Christina Linderholm och Olle Sandahl (enhälligt).

Föredragande: Johanna Herder Toll

Expedition till:
Malmö åklagarkammare
Norrorts åklagarkammare
Riksenheten mot internationell och organiserad brottslighet
Södra åklagarkammaren i Stockholm

[22] Se nämndens uttalande den 20 juni 2023 ”Användning av hemlig dataavläsning i ett tvångsmedelsärende vid Åklagarkammaren i Falun” (dnr 44-2022).
[23] Ärendet har handlagts vid Södertörns åklagarkammare.
[24] Ärendet har handlagts vid åklagarkammaren i Skövde. Enligt 4 a § andra stycket (4 § tredje stycket innan den 1 oktober 2023) lagen om hemlig dataavläsning får ett tillstånd som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter (punkt 1, 2 och 3) 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.

Västerorts åklagarkammare
Åklagarkammaren i Gävle
Åklagarkammaren i Skövde
Åklagarkammaren i Västerås
Åklagarkammaren i Örebro
Åklagarkammaren i Östersund
Åklagarmyndigheten, utvecklingscentrum
Polismyndigheten, rättsavdelningen
Åklagarmyndigheten, tillsynsavdelningen