SÄKERHETS- OCH INTEGRITETSSKYDDSNÄMNDEN

Uttalande med beslut

2021-12-15 Dnr 92-2020

Granskning av ärenden vid Åklagarmyndigheten i vilka hemlig dataavläsning använts

1. SAMMANFATTNING

Hemlig dataavläsning är ett nytt hemligt tvångsmedel som innebär att brottsbekämpande myndigheter i hemlighet bereder sig tillgång till en dator, mobil eller annan teknisk kommunikationsutrustning och därigenom får besked om hur utrustningen används eller har använts och vilken information som finns i den.

Säkerhets- och integritetsskyddsnämnden har granskat användningen av hemlig dataavläsning i ett antal tvångsmedelsärenden som handlagts vid olika åklagarkammare. Granskningen visar bl.a. att ansökningarna om och tillstånden till hemlig dataavläsning i flera fall innefattat anmärkningsvärt långa tidsperioder. Nämnden har inte funnit tillräckliga skäl att ifrågasätta de bedömningar som gjorts i de granskade ärendena, men framhåller vikten av att åklagaren i varje enskilt fall gör en noggrann prövning av nödvändigheten och att restriktivitet iakttas när det gäller tiden för tvångsmedelsanvändningen.

Nämnden framhåller också flera omständigheter som har betydelse för bedömningen av om användningen av hemlig dataavläsning är proportionerlig. Utöver tillståndstidens längd bör bl.a. den samlade användningen av hemliga tvångsmedel, antalet uppgiftstyper enligt 2 § lagen om hemlig dataavläsning och förekomsten av villkor som begränsar integritetsintrånget beaktas. Enligt nämnden innebär 18 § lagen om hemlig dataavläsning att det är obligatoriskt att ange villkor för att tillgodose intresset av att enskildas integritet inte kränks i onödan. Det är därför problematiskt att flertalet tillstånd saknat sådana villkor.

Granskningen visar sammantaget att det finns anledning för nämnden att återkomma till flera av de iakttagelser som gjorts.

Avslutningsvis uttalar sig nämnden om under hur lång tid nya verkställighetsförsök bör kunna göras.

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

Innehåll

2. BAKGRUND

Lagen (2020:62) om hemlig dataavläsning trädde ikraft den 1 april 2020. Regleringen är komplex och användningen av hemlig dataavläsning innebär ett långtgående integritetsintrång för den som utsätts. Tvångsmedlet utgör ett av Säkerhets- och integritetsskyddsnämnden (nämnden) beslutat fokusområde.

Enligt 21 § lagen om hemlig dataavläsning ska nämnden underrättas när rätten beslutat i frågor om hemlig dataavläsning. Med utgångspunkt i underrättelserna kan nämnden inom ramen för ett särskilt initiativärende,[1] utöver en löpande kontroll, fördjupa granskningen genom att begära tillgång till handlingar i utvalda tvångsmedelsärenden hos de brottsbekämpande myndigheterna. Nämndens tillsyn omfattar inte domstolarnas verksamhet.

3. GRANSKNINGEN

Nämnden begärde i juni 2020 in samtliga vid den tidpunkten befintliga handlingar gällande hemlig dataavläsning i ett antal tvångsmedelsärenden. Urvalet av ärenden gjordes dels utifrån uppgifter som angetts i ovan nämnda underrättelser, dels geografisk spridning.[2] Granskningen har syftat till att kontrollera om användningen av hemlig dataavläsning varit i överensstämmelse med lag eller annan författning.

Nämnden har särskilt granskat

- om grundläggande rättsliga förutsättningar för hemlig dataavläsning funnits,
- hur ansökan om och tillstånd till hemlig dataavläsning utformats,
- vilka överväganden som gjorts vid tillämpningen av proportionalitetsprincipen,
- om verkställigheten av tillståndsbesluten har legat inom de tillåtna tidsperioderna och omfattat de tillåtna uppgiftstyperna, och
- om vidtagna åtgärder dokumenterats på ett tillfredsställande sätt.

Med anledning av de iakttagelser som gjorts har ansvariga åklagare skriftligen besvarat frågor. Av åklagarnas svar framgick att samtliga förundersökningar var pågående vid tiden för nämndens frågor. Därför har varken förstöring av

[1] Se nämndens beslut den 20 maj 2020 ”Granskning av underrättelser om beslut i fråga om hemlig dataavläsning” (dnr 77-2020).
[2] De granskade ärendena har handlagts vid åklagarkammaren i Norrköping, Västerorts åklagarkammare i Stockholm, Malmö åklagarkammare, City åklagarkammare i Stockholm, Göteborgs åklagarkammare och nationella åklagaravdelningen, riksenheten mot internationell och organiserad brottslighet.

material från hemlig dataavläsning eller underrättelse till enskild aktualiserats i granskningen.

Polismyndigheten har upprättat skriftliga riktlinjer för hemlig dataavläsning.[3] Dessa har innefattats i granskningen. Åklagarmyndigheten har enligt vad som uppgetts inte några riktlinjer eller andra stöddokument som specifikt avser hemlig dataavläsning.

4. RÄTTSLIGA UTGÅNGSPUNKTER

4.1 Vad är hemlig dataavläsning?

Hemlig dataavläsning innebär att de brottsbekämpande myndigheterna med hjälp av någon form av tekniskt hjälpmedel i hemlighet bereder sig tillgång till en dator, mobil eller annan 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. Det skiljer sig från vad som är fallet vid hemlig avlyssning av elektronisk kommunikation (hemlig avlyssning) och hemlig övervakning av elektronisk kommunikation (hemlig övervakning) enligt rättegångsbalken (RB), där uppgifterna hämtas in på väg till eller från någons tekniska utrustning. Det skiljer sig också från hemlig rumsavlyssning och hemlig kameraövervakning enligt RB, där uppgifterna hämtas in genom utrustning som tillhör och monteras av de brottsbekämpande myndigheterna.[4]

I 2 § lagen om hemlig dataavläsning anges vilka typer av uppgifter som får läsas av eller tas upp genom hemlig dataavläsning.

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 (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 (27 kap. 19 § första stycket 1 RB).

---

[3] PM 2020:16 Polismyndigheten riktlinjer för hemlig dataavläsning, beslutade den 1 april 2020.
[4] Prop. 2019/20:64 s. 55.

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 (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 sammankomster 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. Med avläsningsbart informationssystem avses en elektronisk kommunikationsutrustning eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst.[5] Lagringstjänster kan till exempel 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, till exempel vilka program och applikationer i en mobiltelefon som körs, anteckningar som görs och utkast till meddelanden som inte sparas.[6]

Redan innan lagen om hemlig dataavläsning trädde i kraft kunde de brottsbekämpande myndigheterna få tillstånd att hämta in många av de uppgifter som kan hämtas in genom hemlig dataavläsning. I många fall motsvarades emellertid inte rätten av att hämta in uppgifterna av en faktisk möjlighet att göra så, vilket till stor del berodde på att internetbaserad kommunikation allt oftare har krypterat innehåll.

[5] Prop. 2019/20:64 s. 103 f.
[6] Prop. 2019/20:64 s. 214.

4.2 Förutsättningar för hemlig dataavläsning

4.2.1 Tillstånd till hemlig dataavläsning m.m.

Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagare (14 § lagen om hemlig dataavläsning). Som huvudregel får hemlig dataavläsning, utom vad gäller rumsavlyssningsuppgifter, användas vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år (4 § första stycket 1). Tillståndet får som huvudregel endast avse ett avläsningsbart informationssystem som används, eller om det finns särskild anledning att anta har använts eller kommer att användas, av någon som är skäligen misstänkt för brottet (4 § andra stycket). Det krävs att åtgärden är av synnerlig vikt för utredningen (4 § första stycket). Enligt förarbetena innebär det att metoden för uppgiftsinhämtningen ska ges en särskilt framträdande roll och att riskerna för informationssäkerheten talar för att åtgärden endast bör få användas när andra metoder inte är tillräckliga, är svårare att genomföra än hemlig dataavläsning eller förväntas leda till större integritetsintrång.[7]

Tiden för ett tillstånd till hemlig dataavläsning får inte bestämmas längre än nödvändigt. Vid bestämmandet av vad som är en nödvändig tidsram får hänsyn tas till den tid som kan behövas för att installation eller motsvarande ska kunna utföras och att åtgärden ska bli användbar. När det gäller tid som infaller efter beslutet (hemlig dataavläsning i realtid) får tiden inte överstiga en månad från dagen för beslutet (18 § tredje stycket lagen om hemlig dataavläsning). Tidsbegränsningen tar inte sikte på tid som ligger före beslutet. Det innebär att det inte finns någon lagstadgad bortre tidsgräns för historiska uppgifter. Detta kan få betydelse vid upptagning eller avläsning av lagrade uppgifter eller exempelvis historiska meddelanden.

I tillståndet ska det anges villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan (18 § första stycket 4 lagen om hemlig dataavläsning). I förarbetena anges att det villkor som ska föreskrivas kan vara av teknisk karaktär, t.ex. en föreskrift om att den brottsbekämpande myndigheten som ska verkställa en åtgärd på en viss utpekad plats (kameraövervaknings- eller rumsavlyssningsuppgifter) måste göra det tekniskt omöjligt att genomföra hemlig dataavläsning på annan plats än den som tillståndet avser. Vidare anges att villkoren också kan vara av annan karaktär, exempelvis att tillståndet endast får avse inkommande samtal eller samtal där den misstänkte deltar eller att endast lagrade uppgifter av viss filtyp, viss karaktär eller med viss beteckning omfattas.[8]

---

[7] Prop. 2019/20:64 s. 118.
[8] Prop. 2019/20:64 s. 233.

4.2.2 Särskilt om proportionalitetsprincipen och s.k. differentiering

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.[9] Behovet av uppgifter i varje enskilt fall bör vara styrande för vad hemlig dataavläsning får användas för. I förarbetena benämns detta som att åtgärden bör differentieras. Om en brottsbekämpande myndighet t.ex. behöver komma åt uppgifter från en krypterad kommunikation i en mobiltelefon bör åtgärden inte också per automatik ge tillgång till alla bilder, filer och lösenord som finns sparade i telefonen.[10] Vid tillståndsprövningen måste rätten, utöver att beakta samtliga omständigheter som åberopas i det enskilda fallet, också ställa sig frågan om det är proportionerligt att tillåta avläsning eller upptagning av flera olika uppgiftstyper. Det bör endast undantagsvis och endast i de allra allvarligaste fallen, t.ex. vid terroristbrottslighet eller annan mycket allvarlig brottslighet, vara möjligt att få tillstånd till avläsning eller upptagning av samtliga uppgiftstyper samtidigt.[11]

5. NÄMNDENS IAKTTAGELSER OCH BEDÖMNING

5.1 Inledning

Genom hemlig dataavläsning kan betydande mängder uppgifter från olika informationssystem göras tillgängliga för brottsbekämpande myndigheter. Bland dessa uppgifter finns typiskt sett mycket integritetskänslig information, exempelvis privata bilder och dagboksanteckningar, som helt saknar betydelse för utredning av brottet. I de fall där en ansökan om tillstånd till hemlig dataavläsning avser flera uppgiftstyper och dessutom långa tillståndsperioder blir integritetsintrånget än större. En utgångspunkt är därför att utformningen av en ansökan och frågan om hur tvångsåtgärden ska verkställas måste övervägas noggrant.

I en majoritet av de granskade ärendena har ansökningarna och tillstånden omfattat samtliga de uppgiftstyper, med undantag för kameraövervakningsuppgifter och rumsavlyssningsuppgifter, som anges i 2 § lagen om hemlig dataavläsning. I flera ärenden har åklagarna ansökt om och beviljats tillstånd till att läsa av eller ta upp de aktuella uppgiftstyperna under tidsperioder som i vissa

[9] Prop. 2019/20:64 s. 110.
[10] Prop. 2019/20:64 s. 93.
[11] Prop. 2019/20:64 s. 110.

fall uppgått till flera år. Granskningen har också visat att det är vanligt förekommande att andra hemliga tvångsmedel antingen har använts eller används parallellt med hemlig dataavläsning.

Nämnden har mot denna bakgrund ställt frågor om bl.a. vilka överväganden som föregått ansökningarna när det gäller de olika uppgiftstyperna och den sökta tidsperioden för tvångsmedelsanvändningen. Åklagarna har också anmodats att redogöra för vilka överväganden som gjorts med avseende på åtgärdens proportionalitet, både utifrån användningen av hemlig dataavläsning som tvångsåtgärd i sig och i förhållande till den sammanlagda användningen av hemliga tvångsmedel. Frågor som har att göra med bestämmelsen om att ett tillstånd till hemlig dataavläsning ska förenas med villkor för att värna den enskildes integritet har ställts i samtliga ärenden.

5.2 Grundläggande förutsättningar för hemlig dataavläsning

En del i nämndens granskning har varit att kontrollera att de grundläggande förutsättningarna för tvångsmedelsanvändningen varit uppfyllda. Det har bl.a. innefattat att nämnden granskat omständigheterna i det enskilda fallet i förhållande till det tillståndsgrundande brottet, att brottets straffskala kan ligga till grund för ansökan och tillstånd, att det funnits ett behov av tvångsåtgärden och att den kan anses ha varit av synnerlig vikt för utredningen. Som framgått i avsnitt 4.2.1 ges rekvisitet synnerlig vikt för utredningen en delvis annan innebörd vid hemlig dataavläsning i jämförelse med hemliga tvångsmedel enligt rättegångsbalken. Eftersom det är fråga om ett nytt hemligt tvångsmedel har förutsättningarna för tvångsmedelsanvändningen utgjort en central del av granskningen.

Nämnden konstaterar att hemlig dataavläsning i samtliga fall har använts i förundersökningar om mycket allvarlig brottslighet, såsom mord eller grov allmänfarlig ödeläggelse. Det har i flera fall funnits kopplingar till organiserad brottslighet. Nämndens bedömning är att det med ett undantag har framgått tydligt av handlingarna i tvångsmedelsärendena att det funnits behov av hemlig dataavläsning och att möjligheterna att använda andra tvångsmedelsåtgärder har varit uttömda. Det har exempelvis angetts i promemorian till ansökan att den misstänktes kommunikation inte varit möjlig att ta del av eftersom den varit krypterad. I ett annat ärende har det redogjorts för varför det inte varit möjligt att använda hemlig kameraövervakning på viss plats och på vilket sätt hemlig dataavläsning i den situationen utgjort ett alternativ för att kunna ta del av uppgifter om den misstänkta verksamheten. I ärendet där underlaget varit bristfälligt har åklagaren på nämndens begäran utvecklat sina överväganden och de omständigheter som legat till grund för ansökan. Efter det svar som lämnats anser nämnden att det funnits grund för att använda tvångsmedlet.

Nämnden har sammantaget inga synpunkter på hanteringen i denna del.

5.3 Utformning av ansökan m.m.

5.3.1 Tillståndstidens längd

I några ärenden har tillstånden till hemlig dataavläsning innefattat historiska uppgifter under tidsperioder på från tre till som längst sju år. I ett ärende har åklagaren uppgett att det varit fråga om omfattande brottslighet i näringsverksamhet som pågått under lång tid. Åklagaren har vidare uppgett att hemlig dataavläsning behövdes under så lång tid som sju år eftersom det fanns underrättelseinformation om den brottsliga verksamheten från denna tidpunkt. Det bedömdes nödvändigt att få uppgifter om den misstänktes nätverk för att kunna kartlägga verksamheten och förstå brottsupplägget över tid.

I ett annat ärende har åklagaren lämnat en mer praktisk förklaring till den sökta tidsperioden, som i det fallet uppgick till drygt tre år.

Av åklagarens svar framgår bl.a. följande.

Ansökan avsåg en spegling av innehållet i telefonen. Anledningen till tillståndstidens startdatum var att den misstänkte innehaft den aktuella teleadressen sedan dess. Enligt information från polisen var det inte tekniskt möjligt att i tid avgränsa speglingen utifrån ett senare datum. Tillståndet hade för att begränsa integritetsintrånget förenats med ett villkor om att information som lagrats i telefonen innan ett visst datum inte fick läsas.

Nämnden konstaterar att det har varit anmärkningsvärt långa tillståndstider i vissa ärenden. Detta inger betänkligheter, särskilt mot bakgrund av att det är fråga om ett nytt och särskilt integritetskränkande hemligt tvångsmedel. Det finns inga övergångsbestämmelser i lagen om hemlig dataavläsning som innebär en begränsning i det här avseendet. Det finns inte heller någon lagstadgad bortre gräns för tid som ligger innan tillståndet meddelades. Som framgått i avsnitt 4.2.1 ligger begränsningen, i likhet med vad som gäller vid andra hemliga tvångsmedel, i att tiden aldrig får bestämmas längre än nödvändigt.

Nämnden har sammantaget inte funnit tillräckliga skäl att i de granskade ärendena ifrågasätta de bedömningar som gjorts gällande tillståndstidens längd. Det finns dock anledning att framhålla vikten av att åklagaren gör en noggrann prövning av nödvändigheten i varje enskilt fall. Hemlig dataavläsning under lång tid ger stora mängder information om den person som utsätts för tvångsåtgärden, vilket innebär ett omfattande integritetsintrång. Enligt nämnden bör därför en restriktiv hållning alltid intas eftersom tidsperioden vid användning av ett

hemligt tvångsmedel har stor betydelse för den slutliga bedömningen av om åtgärden är proportionerlig eller inte (se vidare om proportionalitet i avsnitt 5.3.3).

Den förklaring som lämnats i det fall där behovet av en lång tillståndstid närmast tycks motiveras utifrån ett praktiskt perspektiv torde bero på en missuppfattning. De verkställighetskontroller som nämnden utfört och den information som lämnats i anslutning till det har gett en annan bild (se vidare om verkställighet i avsnitt 5.4). Nämnden noterar att den aktuella ansökan gjordes kort tid efter att lagen om hemlig dataavläsning trädde i kraft, vilket kan förklara att det fanns olika uppfattningar om vad som var tekniskt möjligt. Nämnden vill dock understryka att tekniska förutsättningar eller eventuella begränsningar i systemen inte ska vara avgörande för hur en ansökan om ett hemligt tvångsmedel utformas.

5.3.2 Särskilt om uppgifter enligt 2 § 7 lagen om hemlig dataavläsning

I ett ärende har åklagaren ansökt om och beviljats tillstånd till hemlig dataavläsning avseende historiska uppgifter enligt, såvitt nu är av intresse, 2 § 7 lagen om hemlig dataavläsning. I bestämmelsen anges att tillstånd till hemlig dataavläsning får beviljas för att läsa av eller ta upp uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i punkterna 1–6. Iakttagelsen, som nämnden noterat inte bara i detta ärende utan också i underrättelser som kommit in under året, väcker frågan om hur en ansökan enligt 2 § 7 ska utformas när det gäller tiden.

Nämnden konstaterar att bestämmelsens ordalydelse talar för att det bör vara fråga om att läsa av eller ta upp uppgifter i realtid. I bestämmelsen om hemlig övervakning i rättegångsbalken används de olika tempusformerna *finns* eller *har funnits* för att visa att åtgärden är tillåten både i realtid och historiskt (27 kap. 18 § 3 RB). I förarbetena till lagen om hemlig dataavläsning framgår inte klart vad avsikten varit enligt 2 § punkten 7, men exemplen som anges tyder enligt nämnden också på att det är uppgifter i realtid som varit utgångspunkten. Domstolar tycks emellertid bevilja tillstånd både historiskt och i realtid. Som nämnts inledningsvis omfattar inte nämndens tillsyn domstolarnas verksamhet och det saknas inom ramen för denna granskning förutsättningar för nämnden att utreda frågan vidare.

5.3.3 Proportionalitetsprincipen och differentiering

Granskningen visar att det utöver användningen av hemlig dataavläsning har varit vanligt att andra hemliga tvångsmedel har använts eller används mot den misstänkte parallellt med hemlig dataavläsning. Det har framför allt varit fråga om hemlig avlyssning och hemlig kameraövervakning. I ett ärende i en förundersökning om grov allmänfarlig ödeläggelse har hemlig avlyssning, hemlig

kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning använts samtidigt mot den misstänkte. Åklagaren har på nämndens fråga uppgett att tvångsmedelsanvändningen bedömdes proportionerlig med hänsyn till att det var fråga om en brottslighet med livstids fängelse i straffskalan som drabbat en mycket omfattande personkrets. I ett annat ärende har åklagaren angående proportionaliteten framhållit att den information som behövde säkras varit huvudsakligen affärsrelaterad eller av teknisk karaktär och att tvångsmedlet inte har riktats mot de misstänktas privata sfär. Hemlig dataavläsning har inte i något fall riktats mot annan person än den skäligen misstänkte.

Enligt nämnden bör bedömningen av om användningen av hemlig dataavläsning är proportionerlig göras utifrån den sammanlagda tvångsmedelsanvändningen. Andra viktiga omständigheter som ska beaktas är bl.a. tillståndstidens längd, vem som omfattas av åtgärden och förekomsten av villkor som begränsar integritetsintrånget. Som redan konstaterats har samtliga förundersökningar handlat om mycket allvarlig brottslighet och när det gäller användningen av hemlig dataavläsning har andra metoder bedömts vara otillräckliga. Sammantaget har nämnden inte funnit tillräckliga skäl att ifrågasätta att tvångsåtgärden i de granskade ärendena varit proportionerlig (se dock nedan och avsnitt 5.3.4 om villkor).

I sammanhanget finns det anledning att särskilt uppmärksamma att majoriteten av de granskade tillstånden har utformats likadant, det vill säga omfattat alla uppgiftstyper med undantag för kameraövervaknings- och rumsavlyssningsuppgifter. Nämnden har gjort motsvarande iakttagelse i de underrättelser som kommit in under året. I förarbetena framhålls att de brottsbekämpande myndigheterna kommer att behöva anpassa verkställighetstekniken efter tillståndet.[12] Som redogjorts för i avsnitt 5.3.1 har det i granskningen framkommit exempel på när tillståndsperioden anpassats utifrån de tekniska förutsättningarna och inte tvärtom. Ansökningarnas utformning avseende uppgiftstyperna väcker frågan om behovet av uppgifter i varje enskilt fall har varit styrande på det sätt som lagstiftaren avsett. Det finns anledning för nämnden att återkomma till denna frågeställning i kommande granskningar.

5.3.4 Villkor

Med några undantag har tillstånden till hemlig dataavläsning saknat villkor för tvångsmedelsanvändningen. Åklagarna har anmodats att redogöra för vilka överväganden som gjorts i samband med ansökan när det gäller villkor eller begränsningar av åtgärden för att värna den enskildes integritet. Nämnden har också ställt frågor om de närmare förutsättningarna för att använda tvångsmedlet, om verkställigheten av tvångsmedlet och om ett eventuellt villkor

[12] Prop. 2019/20:64 s.155.

diskuterades vid rättens sammanträde. I de ärenden där villkor har angetts har dessa exempelvis föreskrivit att information som lagrats i telefonen i tiden före ett visst datum inte får läsas eller att åtgärden ska genomföras så att minsta möjliga överskottsinformation samlas in.

Sammanfattningsvis har följande framkommit av remissvaren.

Vid rättens sammanträden har frågor om villkor, verkställighet och den misstänktes integritet diskuterats. I de fall där villkor inte har angetts i tillståndet har uppfattningen varit att ansökan utformats på sådant sätt att den misstänktes personliga integritet inte kränks i onödan. Att därutöver uppställa villkor ”endast för villkorets skull” är överflödigt. I något fall har ansvarig tekniker från polisen varit med på sammanträdet och redogjort för hur åtgärden skulle verkställas, vilket varit anledningen till att något villkor inte angetts.

Nämnden anser att det i och för sig är positivt att frågor kring verkställighet och integritet har diskuterats vid rättens sammanträden. Avsaknaden av villkor i tillstånden innebär dock att det inte är möjligt att i efterhand kontrollera att en hantering som uppges ha diskuterats i samband med tillståndsprövningen efterlevs. Som framgått av avsnitt 4.2.1 *ska* det i ett tillstånd till hemlig dataavläsning anges villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Bestämmelsen skiljer sig enligt ordalydelsen från vad som gäller för tvångsmedelsregleringen i rättegångsbalken. Där anges att i ett beslut att tillåta åtgärder ska det, när det finns skäl till detta, också i övrigt anges villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan (27 kap. 21 § sjätte stycket RB). Enligt nämnden ska 18 § i lagen om hemlig dataavläsning läsas som att det är obligatoriskt att ange villkor för användningen.[13] Det förhållandet att flertalet tillstånd, även de som inte innefattats i granskningen, saknar villkor är således problematiskt.

Utifrån den rättsliga regleringen är frågan om villkor ytterst rättens ansvar och inte åklagarens. Nämnden har tidigare uttalat att eftersom åklagaren är den som bäst känner ärendet är det angeläget att denne i samband med en ansökan till ett hemligt tvångsmedel noga överväger de närmare förutsättningarna för verkställighet, och i de fall det är lämpligt anger hur integritetsintrånget kan begränsas genom ett villkor.[14] Detta gäller även vid användningen av hemlig dataavläsning. Enligt vad nämnden erfar har verkställigheten i vissa fall inte gått att genomföra på grund av det villkor som föreskrivits. Att det råder osäkerhet kring hur ett villkor bör anges kan vara en anledning till att det saknas i tillstånden.

---

[13] Prop. 2019/20:64 s. 233. Se även Lindberg, Lag (2020:62) om hemlig dataavläsning 18 § 4, Karnov 2021-11-25, (JUNO)

[14] Se nämndens beslut den 21 juni 2021 ”Hanteringen av hemliga tvångsmedel vid åklagarkammaren i Eskilstuna” (dnr 136-2019).

Nämnden avser att återkomma i frågan. Det är viktigt att användningen av villkor i praktiken utgör den rättssäkerhetsgaranti som varit lagstiftarens avsikt.

5.4 Verkställighet

5.4.1 Kontroll av verkställighet

Hemlig dataavläsning är till sin natur teknisk komplicerad. Såväl vid tillämpning som vid tillsyn i efterhand aktualiseras svåra och i sammanhanget nya frågor som har att göra med gränsdragningen mellan teknik och juridik.[15]

Nämnden har i delar kontrollerat verkställigheten av de tillstånd som innefattats i granskningen. Flera tillstånd har aldrig verkställts. I de fall tillstånden har verkställts har användningen, såvitt kunnat utläsas i Polismyndighetens system, legat inom ramen för tillståndstiden. Verkställighetskontrollen har också innefattat säkerställande av att endast de uppgiftstyper som tillståndet avsett varit inlagda i systemet. I ett fall har den sistnämnda kontrollen inte varit möjlig trots att tillståndet verkställts. Tillståndet avsåg upptagning och avläsning av uppgifter i vissa närmare angivna molntjänster. Det finns utifrån de iakttagelser som gjorts anledning för nämnden att återkomma till frågor som gäller verkställigheten. Bedömningen är att dessa frågor bäst hanteras i en granskning med ett särskilt fokus på det.

5.4.2 Under hur lång tid kan nya verkställighetsförsök göras?

I ett ärende har åklagaren ansökt om och fått tillstånd till hemlig dataavläsning avseende både historiska uppgifter och uppgifter i realtid. Efter att verkställigheten misslyckats ansökte åklagaren om förlängning av tillståndet varvid även den historiska tidsperioden upptogs på nytt. I motsvarande situation i ett annat ärende har åklagaren vid ansökan om förlängning avseende uppgifter i realtid inte inkluderat den tidigare beviljade historiska tidsperioden. På fråga från nämnden har åklagaren i det sistnämnda ärendet uppgett att hon utgått från att det ”tidigare beslutet täckt åtgärden bakåt i tiden och att det nya tillståndet täckt åtgärden framåt i tiden.”

Nämnden konstaterar att tekniska problem eller andra omständigheter som de brottsbekämpande myndigheterna inte råder över ibland leder till att verkställigheten inte kan genomföras. På grund av att tvångsmedlet är beroende av vissa tekniska funktioner torde verkställighetsproblem göra sig gällande i större utsträckning vid hemlig dataavläsning jämfört med verkställighet av övriga hemliga tvångsmedel. Såvitt nämnden förstår förekommer det att ett tillstånd inte kan verkställas vid ett första försök men väl senare. Detta tillsammans med

[15] Sedan oktober 2020 finns en teknisk rådgivare på nämndens kansli.

åklagarnas till synes olika förhållningssätt aktualiserar frågan om under hur lång tid som nya verkställighetsförsök kan göras.

Enligt 20 § lagen om hemlig dataavläsning får ett beslut i frågor om hemlig dataavläsning verkställas omedelbart. En utgångspunkt tycks vara att det inte finns något hinder mot att avläsning äger rum flera gånger under tillståndstiden och att uppgifter som lagrats under den tiden läses av.[16] Någon reglering eller på annat sätt uttalad tidpunkt för när ett tillstånd *senast* bör verkställas finns inte. Enligt den princip som gäller för tvångsmedelsanvändning i allmänhet bör dock ett tvångsmedelsbeslut alltid verkställas i så nära anslutning till beslutet som möjligt.[17]

Nämnden anser att det ligger nära till hands att applicera motsvarande synsätt vid verkställighet av ett tillstånd till hemlig dataavläsning. Det skulle i så fall innebära att ett nytt tillstånd behövs för möjligheten till fortsatta verkställighetsförsök när viss tid förflutit. I de fall ansökan och tillstånd innefattar hemlig dataavläsning även i realtid framstår det som lämpligt att låta den i lag angivna tidsbegränsningen på en månad utgöra den bortre gränsen också för möjligheten till fortsatta verkställighetsförsök avseende historiska uppgifter. Nämndens uppfattning i denna del överensstämmer således med hur frågan har hanterats i ett av ärendena ovan.

5.4.3 Territorialitetsprincipen

Några ansökningar och tillstånd har avsett avläsningsbara informationssystem av immateriell karaktär, exempelvis applikationer i mobiltelefoner och molntjänster. I dessa fall har det inte framgått av tvångsmedelsärendena, eller på annat sätt, var de uppgifter som omfattas av ansökan är lagrade. Den svenska hållningen har hittills varit att om uppgifter lagras elektroniskt på annan plats än i Sverige, eller om det är okänt var uppgifterna lagras, så saknar svenska brottsbekämpande myndigheter jurisdiktion. Detta baseras på en tolkning av den s.k. territorialitetsprincipen. Under utredningsarbetet till lagen om hemlig dataavläsning framfördes att det finns skäl att ändra den svenska hållningen, men frågan hänvisades till rättstillämpningen. Nämnden uttalade i sitt remissyttrande att hanteringen inte var godtagbar och efterfrågade en fortsatt analys.[18] Regeringen bedömde att frågan om hur territorialitetsprincipen vid exekutiv jurisdiktion bör tolkas bäst tas om hand inom ramen för det internationella samarbetet eller på annat lämpligt sätt.[19]

---

[16] Se Lindberg, Lag (2020:62) om hemlig dataavläsning 2 § 6, Karnov 2021-11-24, (JUNO)
[17] JO 1997/98 s. 165.
[18] Se nämndens yttrande över ”Hemlig dataavläsning - ett viktigt verktyg i kampen mot allvarlig brottslighet” (SOU 2017:89) (dnr 193-2017).
[19] Prop. 2019/20:64 s. 202 f.

Ur ett verkställighetsperspektiv är frågan om var uppgifterna lagras i förhållande till tolkningen av territorialitetsprincipen mycket viktig. Mot bakgrund av att regeringen nyligen har beslutat att tillsätta en utredning om datalagring vid brottsbekämpning[20] med uppdrag bl.a. att göra en översyn av territorialitetsprincipen saknas skäl att i nuläget utreda frågan vidare.

5.5 Avslutande synpunkter

Det har överlag varit god ordning i den granskade tvångsmedelshanteringen. Nämndens frågor, också i delar som inte redovisats i uttalandet, har i huvudsak besvarats utförligt och noggrant. De granskade ärendena innehåller några av de allra första ansökningarna om hemlig dataavläsning. De brottsbekämpande myndigheterna, och enskilda åklagare i synnerhet, hade förmodligen inte fullt ut orienterat sig i den nya lagstiftningen. Det är därför sannolikt att någon fråga skulle ha besvarats annorlunda om den ställts när lagen varit i kraft en tid.

I samband med kontroll av verkställigheten vid Polismyndigheten framkom bl.a. att arbetet med att effektivisera verksamheten kring hemlig dataavläsning har föranlett vissa interna förändringar. Nämnden har förståelse för att det pågår ett utvecklingsarbete men vill samtidigt betona vikten av att interna riktlinjer är heltäckande och hålls uppdaterade. Nämnden anser att det vore önskvärt att även Åklagarmyndigheten tar fram riktlinjer eller annan vägledning som syftar till att ge åklagarna stöd och främja en enhetlig och rättssäker hantering av hemlig dataavläsning.

Flera iakttagelser i granskningen har antingen väckt frågor eller visat på oklarheter angående hur lagen om hemlig dataavläsning ska tillämpas. Som framgått finns det anledning för nämnden att återkomma i flera delar. Lagen om hemlig dataavläsning är tidsbegränsad. Det är därför angeläget att nämnden under denna tid både kan identifiera var riskerna för felaktig tillämpning av lagen finns och får en ökad förståelse för vilka konsekvenser det nya hemliga tvångsmedlet har för den personliga integriteten. För att kunna utöva en effektiv tillsyn behöver nämnden mer kunskap om hur hemlig dataavläsning används och verkställs.

Vad som i övrigt framkommit vid granskningen ger inte anledning till något uttalande från nämndens sida.

[20] Datalagring vid brottsbekämpning – ytterligare åtgärder för en modern och ändamålsenlig reglering dir. 2021:58.

6. BESLUT

Med dessa synpunkter avslutas ärendet.

På Säkerhets- och integritetsskyddsnämndens vägnar

Gunnel Lindberg

I avgörandet har deltagit: Gunnel Lindberg (ordförande), Barbro Thorblad, Charlotta Bjälkebring Carlsson, Matheus Enholm, Elisabeth Falkhaven och Christina Linderholm (enhälligt).

Föredragande: Maria Gylder och Johanna Rådberg

Expedition till:
Åklagarkammaren i Norrköping
Västerorts åklagarkammare i Stockholm
Malmö åklagarkammare
City åklagarkammare i Stockholm
Göteborgs åklagarkammare
Nationella åklagaravdelningen, riksenheten mot internationell och organiserad brottslighet

Polismyndigheten, nationella operativa avdelningen

Kopia för kännedom till:
Åklagarmyndigheten (huvudkontoret, tillsynsavdelningen)
Ekobrottsmyndigheten (rättsenheten)
Polismyndigheten (rättsavdelningen)
Domstolsverket (rättsavdelningen)