

## Datainspektionens skriftliga synpunkter efter hearing över betänkandet SOU 2009:66 Signalspaning för polisiära behov

Datainspektionen har granskat promemorian och lämnar sina synpunkter främst utifrån sin uppgift att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter.

- A) Datainspektionen anser att valet av en befogenhetslösning innebär att fler personuppgifter kommer att tillföras FRA än vad som hade blivit fallet med en delgivningslösning; detta eftersom det ges ytterligare en möjlighet (för polisiära behov) att inhämta signaler.
- B) Det behöver undersökas hur mycket trafik som det i realiteten blir fråga om som FRA får tillgång till. För ett rån av normalgraden som kan bedömas ha ett straffvärde på två år eller därutöver är signalspaning i tråd möjlig. Minsta omfattning på inhämtningen är signalerna i en signalbärare; det finns anledning att anta att det för utredning av ett visst brott inte alltid räcker med en signalbärare. Med utredningens resonemang (sid. 133) om antalet signalbärare skulle en signalbärare motsvara 0,2 – 0,4 promille av all gränsöverskridande trafik. Man kan ifrågasätta om det är proportionerligt att myndigheterna får tillgång till så mycket personuppgifter för utredning av ett enda brott. Det sagda talar i sig emot att tillåta signalspaning, i vart fall i kabel, inom ramen för en förundersökning.
- C) Det finns enligt Datainspektionen anledning att noggrannare än vad utredaren har gjort undersöka vilka konsekvenser det får för personuppgiftsbehandlingen att olika lagar kommer att bli tillämpliga på de behandlingar som kan komma att utföras med det inhämtade materialet; inhämtningen regleras av inhämtningslagen, för den vidare behandlingen gäller vid FRA FRA-PuL och vid polisen polisdatlagen eller tillstånd som

Datainspektionen har meddelat med stöd av den numera upphävda datalagen. Vad får exvis. avsaknaden av en bestämmelse likt den i 1 kap 13 § FRA-PuL för betydelse när råmaterial överlämnas från FRA till polisen? Kommer den lagring av råmaterialet som sker hos polisen omedelbart efter inhämtning, samt språklig översättning och kryptoforcering m.m. i den mån detta sker hos polisen att innebära att behandlingen riskerar att bli olaglig om förstöringspliktig information finns i det överlämnade materialet? Vad får det för konsekvenser att uppgifter som överlämnas från FRA och som ska gallras eller förstöras (kolliderande bestämmelser), men där det ändå finns möjlighet att behandla personuppgifter i polisiära register? Jfr exvis. den politiska överenskommelsen från 2008 (FRA:s signalspaning i försvarsunderrättelseverksamhet) om att inget råmaterial ska sparas mer än ett år. Kan det bli fråga om långa/längre lagringstider i den polisiära registermiljön; frister som inte hade varit möjliga hos FRA (efter införandet av bestämmelser som kodifierar den aktuella delen av den politiska överenskommelsen)? Kan skillnader i sökmöjligheter hos FRA och polisen innebära att FRA kan göra sökningar i material som ska överlämnas till polisen och där sökningarna inte hade varit möjliga för polisen (eftersom de inte hade varit tillåtna hos polisen men är det hos FRA)?

D) Skrivningarna om överskottsinformation ger upphov till en viss osäkerhet när det gäller kontrollen av flödet av personuppgifter totalt sett. Såsom Datainspektionen tolkar utredningen ska det finnas möjligheter för uppgifter att flöda mellan de två disciplinerna (försvarsunderrättelseverksamhet och polisiär verksamhet). Även om vissa av frågeställningarna i det följande inte är nya i den meningen att de har varit föremål för diskussion och överväganden i den praktiska tillämpningen även i tiden före FRA:s möjligheter att bedriva signalspaning i tråd, kan frågorna vara av värde att besvara i ljuset av de förändrade förhållanden som kommer att gälla för informationsinhämtning genom signalspaning. Hur säkerställs det att t.ex. personuppgifter som talar till en misstänkts fördel och som har inhämtats inom ramen för en förundersökning verkligen tillförs utredningen? Vad händer om FRA beträffande sådan information anser att ett röjande skulle avslöja myndighetens metod och förmåga? FRA verkar vara den myndighet som ska medge offentliggörande i samband med överlämnande. Hur förhåller sig FRA:s möjlighet att påverka den överlämnade informationen till sitt innehåll och framtida offentliggörande till innehållet i domstolens tillstånd och rättegångsbalkens regler om partsinsyn och förundersökning m.m.? Hur ska hörande av FRA-personal i rättegångar kunna

säkerställas? Att analogivis tillämpa 27:23 a RB; får det några konsekvenser att det är fråga om underrättelser som har inhämtats genom signalspaning jämfört med hemlig teleavlyssning; det finns all anledning att anta att signalspaning innebär en mycket större mängd inhämtade signaler jämfört med det precisa tvångsmedlet hemlig teleavlyssning vilket i sin tur innebär att riskerna för otillbörliga integritetsintrång blir större när överskottsinformationen från signalspaning används. Det verkar sammanfattningsvis finnas flera funktioner och mekanismer (bl.a. FRA, domstolen och förundersökningsledare) som kan styra flödet av personuppgifter, oklart hur det kommer att se ut i praktiken.

- E) Kan man se det som ett integritetsskydd att FRA, som är en försvarsunderrättelsemyndighet, ska fungera som ett filter för att tillse att bara vissa uppgifter överlämnas till polisen?
- F) Ska en förundersökningsledare kunna förhindra att information som inhämtats genom signalspaning för polisen lämnas till regeringen, Regeringskansliet och Försvarsmakten inom ramen för försvarsunderrättelseverksamheten? Innebär det att förundersökningsledaren får insyn i försvarsunderrättelseverksamhetens behov och inriktningar (för att kunna göra sin bedömning)?
- G) Vad är det för ”nya situationer” eller motsvarande som motiverar att Säkerhets- och integritetsskyddsnämnden (SIN) ska kunna avbryta inhämtning som sker med stöd av domstolstillstånd? Vilka är motiven till att ge SIN större befogenheter än Kontrollmyndigheten vid signalspaning i försvarsunderrättelseverksamheten? Kan det finnas en risk för att obalansen i kontrollorganens befogenheter leder till att förtroendet för domstolens tillstånd i polisfallen sänks och att det kan bli problem/osäkerhet nästa gång ett liknande tillstånd söks (avseende liknande förhållande som SIN har upphävt)? Är det domstolens praxis eller SIN:s praxis som kommer att bli vägledande för polisens signalspaning? Även om utredaren motiverar sitt ställningstagande med, som det får förstås, integritetsskäl, finns det anledning att rikta principiella invändningar mot förslaget i denna del.
- H) Blandad trafik förekommer, dvs. trafik som går i såväl kabel som i etern. Förslaget är inte teknikneutralt i denna del. Hur ska man hantera inhämtning som går i både tråd och eter? Kan detta ställa till problem för domstolen eller andra aktörer?