Datainspektionen

Beslut
2016-10-24

Diarienr
2331-2015

Ert diarienr
KH20 400:6041/16

Försvarets radioanstalt (FRA)
Box 301
161 26 Bromma

Tillsyn över behandlingen av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet

Datainspektionens beslut

Datainspektionen konstaterar att Försvarets radioanstalt (FRA) behandlar personuppgifter i strid med 3 kap. 2 § första stycket lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (FRA-PuL) genom att inte genomföra regelbundna logguppföljningar i försvarsunderrättelseverksamheten.

Datainspektionen förutsätter att FRA inför den centrala logganalysfunktion som myndigheten har redogjort för i ärendet. FRA föreläggs att till Datainspektionen senast den 1 maj 2017 lämna en skriftlig redogörelse för de åtgärder som myndigheten har vidtagit och avser att vidta i fråga om den centrala logganalysfunktionen.

Utöver vad som framgår ovan lämnar Datainspektionen, med anledning av den fråga som Statens inspektion för försvarsunderrättelseverksamheten (SIUN) har anmält till Datainspektionen, sin tolkning av 1 kap. 13 § FRA-PuL, se s. 15.

Ärendet avslutas.

Redogörelse för tillsynsärendet

Datainspektionen har granskat delar av den personuppgiftsbehandling som Försvarets radioanstalt (FRA) genomför enligt lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (FRA-PuL) med anslutande förordning (2007:261) (FRA-PuF). Detta innefattar också den personuppgiftsbehandling som sker vid FRA i samband med inhämtning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (LSF).

Tillsynen inleddes genom att Datainspektionen begärde att FRA skriftligen skulle besvara ett antal frågor kring den personuppgiftsbehandling som sker. Datainspektionen har därefter genomfört inspektion på plats hos FRA vid fyra tillfällen och då dels fått en genomgång av den personuppgiftsbehandling som sker, dels granskat personuppgiftsbehandlingen i två av Datainspektionen utvalda projekt hos FRA. Granskningen av de två projekten har gått till så att Datainspektionen först fått en teoretisk genomgång av respektive projekt. Därefter har inspektionen förevisats det praktiska arbete som utförs av enskilda analytiker med hjälp av uppgifter från olika gemensamt tillgängliga uppgiftssamlingar i respektive projekt. Personal på FRA har genomfört sökningar på begäran av Datainspektionen och i övrigt förevisat systemen i enlighet med inspektionens anvisningar.

Tillsynen har dels skett som ett led i Datainspektionens planerade tillsynsverksamhet, dels som en uppföljning av den granskning som inspektionen genomförde under 2010 enligt regeringsuppdraget Fö2009/355/SUND. Därutöver har tillsynen omfattat en rättslig fråga som Statens inspektion för försvarsunderrättelseverksamhet (SIUN) anmält i enlighet med 15 § andra stycket i förordningen (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamhet. Frågan gäller tolkningen av 1 kap. 13 § FRA-PuL, se Datainspektionens ärende med dnr 580-2015.

De frågor som Datainspektionen har ställt till FRA har bland annat rört de förändrade förutsättningarna för personuppgiftsbehandling till följd av möjligheterna att inhämta signaler i tråd, kraven på nödvändighet och anknytning till en preciserad inriktning, behandlingen av känsliga personuppgifter, förstöringsplikt, gallring och loggning.

FRA har gett in skriftligt svar på de av Datainspektionen ställda frågorna. Datainspektionen har därutöver tagit del av FRA:s interna föreskrifter och annan relevant dokumentation. FRA har redogjort för den verksamhet som bedrivs samt för de rutiner och arbetssätt som tillämpas avseende behandling av personuppgifter enligt FRA-PuL och LSF. Den verksamhet som FRA bedriver är sådan att den i stor utsträckning omfattas av kvalificerad sekretess. Mot den bakgrunden återges vad som har framkommit i ärendet endast i begränsad omfattning.

FRA har försett inspektionen med de uppgifter som behövts för ärendets handläggning.

Skäl för beslutet

Beskrivning av FRA:s verksamhet och rättsliga utgångspunkter

Försvarsunderrättelseverksamhet ska enligt lagen (2000:130) om försvarsunderrättelseverksamhet bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för att kartlägga yttre hot mot landet. Verksamheten ska fullgöras genom inhämtning, bearbetning, analys av information samt rapportering. Teknisk inhämtning av information kan ske genom signalspaning vilket regleras i LSF. I 1 § andra stycket LSF anges uttömmande de syften för vilka signalspaning i försvarsunderrättelseverksamhet får ske.

Försvarsunderrättelseverksamhet bedrivs av Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut. Det är regeringen som bestämmer försvarsunderrättelseverksamhetens inriktning. Signalspaning handlar om att inhämta signaler, bearbeta och analysera dessa samt att rapportera underrättelser. Inhämtade signaler kan ge information om innehållet i ett meddelande men också information om meddelandet och dess förmedling, s.k. trafikdata. Inhämtning av signaler kan ske till exempel via satellit eller tråd (om signalspaning se prop. 2006/07:63, s. 22 f). Medan LSF framför allt tar sikte på inhämtningen av signaler, omfattar FRA-PuL hanteringen av de personuppgifter som inhämtats och är under fortsatt behandling.

Signalspaning bedrivs av FRA på inriktande myndigheters uppdrag och enligt LSF. Inriktning av signalspaning i försvarsunderrättelseverksamhet får anges endast av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen vid Polismyndigheten. Inriktningen får inte avse endast en viss fysisk person. Inom ramen för denna närmare inriktning tas årligen ett beslut om preciserad inriktning av FRA:s generaldirektör.

Vid signalspaning via tråd begränsas inhämtningen till de signalbärare för vilka FRA erhållit tillstånd av Försvarsunderrättelsedomstolen. Den faktiska tillgången till de tillståndsgivna signalbärarna ges därefter av SIUN. Operatörers skyldighet att överföra signaler för att möjliggöra inhämtning regleras i lagen (2003:389) om elektronisk kommunikation. I det tillstånd som lämnas av Försvarsunderrättelsedomstolen anges vilket inhämtningsuppdrag tillståndet avser, vilka signalbärare som FRA ska få tillgång till, vilka sökbegrepp eller kategorier av sökbegrepp som får användas vid inhämtningen, den tid som tillståndet avser och de villkor i övrigt som behövs för att begränsa integritetsintrånget. Den trafik som inte väljs ut försvinner utan att kunna återskapas.

Den information som inhämtas är ofta krypterad eller formulerad på ett främmande språk. För att FRA ska kunna framställa rapporter med underrättelser måste informationen bearbetas och analyseras. Under bearbetningsfasen tydliggörs de inhämtade signalernas innehåll och materialet struktureras.

I och med att LSF trädde ikraft 2009 gavs FRA möjlighet att bedriva signalspaning i tråd och inte, som tidigare, enbart i etern. På samma sätt som tidigare får dock signalspaning endast riktas mot yttre hot och inhemsk kommunikation får inte inhämtas. Utvidgningen av signalspaning till signaler i tråd innebär emellertid en mer omfattande inhämtning via det globala nätet jämfört med tidigare då endast satellitburna delar av det globala nätet inhämtades. Merparten av trafiken i det globala nätet saknar betydelse för försvarsunderrättelseuppdraget. FRA:s förmåga att avgränsa inhämtningen till den för försvarsunderrättelseuppdraget relevanta trafiken är därför central för integritetsskyddet, men även för verksamhetens behov av effektivitet.

Datainspektionen är tillsynsmyndighet enligt FRA-PuL för den behandling av personuppgifter som sker i FRA:s försvarsunderrättelse- och

utvecklingsverksamhet. Därutöver har SIUN ett särskilt uppdrag att granska den behandling av uppgifter som sker enligt FRA-PuL. SIUN är också kontrollmyndighet enligt LSF och har särskilda uppgifter enligt den lagen.

Konsekvenserna av LSF:s ikraftträdande och möjligheterna att inhämta signaler i elektronisk form

Vad FRA har anfört

Utbyggnaden av FRA:s kabelaccess har skett successivt sedan skyldigheten för trådägande operatörer att överlämna signaler trädde ikraft. Åtkomsten till signalbärare har sedan Datainspektionens granskning 2010 utökats genom inrättande av fler samverkanspunkter. Inhämtningen i de tillståndsgivna signalbärarna har också utökats genom anskaffning av ytterligare inhämtningssystem. Kabelaccessen har varit fullständigt avgörande för en framgångsrik rapportering på ett flertal underrättelseområden som i regeringens årliga inriktning av försvarsunderrättelseverksamheten getts den högsta prioritetsnivån. Den utökade åtkomsten till signalbärare gör att de informationsmängder som blir föremål för manuell granskning kan väljas ut ur ett mer omfattande underlag, vilket i slutändan förbättrar kvaliteten i underrättelseproduktionen.

När manuell granskning blir aktuell sker denna granskning alltid med dokumenterad anknytning till en preciserad inriktning eller med anknytning till ett ändamål i utvecklingsverksamheten. Inhämtningen avgränsas genom domstolstillstånd samt regler om förbud mot inhämtning av signaler mellan en avsändare och mottagare i Sverige. Endast sådana typer av trafikdata som har relevans för försvarsunderrättelse- och utvecklingsverksamheten inhämtas. Vidare finns ett krav på anknytning till en preciserad inriktning och en absolut gallringsfrist för uppgiftssamlingar för råmaterial. För att kunna producera underrättelser avseende oförutsedda händelser ligger det i sakens natur att inhämtningen av trafikdata inte låter sig begränsas till trafikdata som endast avser på förhand kända aktörer och företeelser. Endast en mycket liten bråkdel av inhämtade trafikdata blir dock föremål för manuell granskning. Att i efterhand kunna söka i brett inhämtade trafikdata är helt vitalt för verksamheten, t.ex. för möjligheterna att i efterhand kartlägga plötsliga oförutsedda skeenden eller att snabbt ta sig an ett nytt underrättelseområde där aktörerna är nya och okända. Inhämtningen sker endast på de våglängder och satellitfrekvenser som bedöms innehålla de mest relevanta trafikflödena. Inhämtningen av trafikdata sker endast på en delmängd av den för FRA tillgängliga signalmiljön.

Datainspektionens bedömning

Datainspektionen kan konstatera att inhämtningen av signaler i tråd har ökat successivt sedan LSF trädde ikraft och att den bedömning som inspektionen gjorde i sin rapport från 2010 – att det fanns en relativt hög sannolikhet för att personer som kommunicerar i signalbärare som FRA bedriver inhämtning mot kommer att få uppgifter om sin kommunikation sparade hos FRA i form av trafikdata – var korrekt. Genom införandet av LSF fick FRA möjlighet till en ny form av inhämtning, nämligen inhämtning av signaler i elektronisk kommunikation via tråd eller kabel. I förarbetena till lagen konstaterades att möjligheten att signalspana inte skulle begränsas av det faktum att kommunikationen till stor del förflyttas från eter till tråd (prop. 2006/07:63, s. 69). Även om tekniken och sättet att kommunicera i och för sig har förändrats ytterligare sedan lagen infördes, bedömer Datainspektionen att lagstiftaren redan då förslaget lades fram måste ha varit medveten om den ökade mängden inhämtade uppgifter som signalspaningen i tråd skulle medföra.

För att motverka de integritetsrisker som signalspaningen i tråd skulle kunna innebära för enskilda infördes bestämmelser i LSF i syfte att begränsa inhämtningen, till exempel krav på domstolstillstånd, förbud mot inhämtning av inhemsk trafik, förstöringsplikt, underrättelseskyldighet och SIUN:s utredningsskyldighet. Dessutom finns bestämmelser i FRA-PuL som reglerar förutsättningarna för FRA att behandla personuppgifter. Regeringen uttalade i samband med införandet av kompletterande bestämmelser i LSF att det var väsentligt att i sammanhanget beakta all den lagstiftning som reglerar verksamheten och hänvisade särskilt till FRA-PuL, vars syfte är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter i FRA:s försvarsunderrättelse- och utvecklingsverksamhet (prop. 2008/09:201, s. 83). En uttrycklig hänvisning till FRA-PuL finns därför i 12 a §.

Utöver den yttre ram som uppställs i lag styrs den signalspaning som bedrivs vid FRA av de inriktningar som regeringen och andra uppdragsgivare lämnar. Den verksamhet som FRA bedriver utgår således inte från myndighetens egna behov utan är helt styrd av uppdragsgivarnas aktuella underrättelsebehov. Dessa behov kommer till exempel till uttryck i av uppdragsgivarna prioriterade geografiska områden eller företeelser vilka förändras i takt med omvärlden. De givna inriktningarna omsätts sedan av FRA i så kallade projekt.

FRA har anfört att den ökade mängden inhämtade uppgifter inte har påverkat möjligheterna att tillämpa bestämmelserna i FRA-PuL och LSF. Utöver den särskilda frågan kring tolkning av 1 kap. 13 § FRA-PuL (se s. 15 ff nedan), bedömer också Datainspektionen att FRA, såvitt framkommit i ärendet, tillämpar bestämmelserna om inhämtning och annan behandling av personuppgifter i enlighet med gällande lagstiftning och att frågorna om personlig integritet tas på stort allvar. FRA har tagit fram detaljerade föreskrifter och infört rutiner för att säkerställa en hög medvetandenivå inom organisationens alla delar ifråga om vilka regler som gäller för personuppgiftsbehandling och integritetsskydd. Enligt inspektionens bedömning fyller dessa rutiner och föreskrifter en viktig funktion för den enskilde medarbetaren när denne har att tillämpa regelverket om behandling av personuppgifter i den operativa verksamheten.

Krav på nödvändighet och anknytning till en preciserad inriktning

I 1 kap. 8 § FRA-PuL anges att personuppgifter endast får behandlas om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet. Uppgifter om en person får endast behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja inriktningen.

Vad FRA har anfört

Kravet på nödvändighet och anknytning till en preciserad inriktning säkerställs genom den preciserade inriktningen som är ett årligt beslut av generaldirektören. Denna inriktning utgör produktionsplan för försvarsunderrättelseverksamheten vid FRA och innehåller de närmare förutsättningarna för behandling av personuppgifter. Utifrån produktionsplanen görs ansökningar till Försvarsunderrättelsedomstolen om inhämtningstillstånd som är anpassade för att kunna fullfölja inriktningen. Huruvida behandling av en viss personuppgift är nödvändig för att fullfölja den preciserade inriktningen måste därutöver bedömas löpande. Den bedömningen kan endast göras av medarbetare som besitter sakämneskunskap inom respektive underrättelseområde. Det föreligger ofta ett stort mått av vaghet och osäkerhet i allt underrättelsearbete då det baseras på hypoteser och antaganden. Rapportmottagaren har ofta bättre förutsättningar att bedöma en enstaka uppgifts relevans eller betydelse för ett händelseförlopp eller utvecklingen av en företeelse.

Det sker en löpande utvärdering av de källor som FRA inriktar signalspaningen mot i syfte att fastställa relevansen för fortsatt inhämtning m.m. Denna utvärdering sker med stöd av den återkoppling om rapporteringens relevans som erhålls från rapportmottagarna.

Det finns interna föreskrifter som säkerställer att särskilt utpekade funktioner ansvarar för att aktiverade sökbegrepp ligger inom ramen för gällande tillstånd och att rapportering som innehåller personuppgifter endast får ske om det finns stöd i den preciserade inriktningen och behandlingen är nödvändig för att fullfölja inriktningen. Överskottsinformation får inte rapporteras.

Datainspektionens bedömning

Bestämmelsen i 1 kap. 8 § FRA-PuL är central och utgör en begränsning av vilka personuppgifter som får behandlas i försvarsunderrättelseverksamheten. Kravet på nödvändighet och anknytning till en preciserad inriktning säkerställs i första hand genom att den preciserade inriktningen ligger till grund för konkreta underrättelseuppdrag. I förarbetena till bestämmelsen uttalades att graden av anknytning med hänsyn till verksamhetens speciella karaktär måste avgöras från fall till fall. Det anfördes vidare att det alltid måste finnas en sådan koppling mellan en person och den företeelse som verksamheten syftar till att kartlägga, att man i efterhand kan hänföra personuppgiftsbehandlingen till en viss preciserad inriktning (prop. 2006/07:46, s. 67).

I all underrättelseverksamhet måste det finnas utrymme för att behandla uppgifter på ett tidigt stadium utan att man vid den tidpunkten med säkerhet kan slå fast uppgifternas relevans. Datainspektionen vill dock understryka vikten av att det i verksamheten kontinuerligt görs en bedömning av om behandlingen är förenlig med 1 kap. 8 § FRA-PuL. Det sätt på vilket FRA har beskrivit att bestämmelsen tillämpas visar att det finns väl utarbetade rutiner och funktioner för att säkerställa att kravet på nödvändighet och anknytning till preciserad inriktning upprätthålls. Datainspektionen har inte heller gjort några iakttagelser som visat på att uppgifter behandlas i strid med 1 kap. 8 §.

Känsliga personuppgifter

I 1 kap. 11 § FRA-PuL regleras behandlingen av känsliga personuppgifter. Sådana uppgifter får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter när det är absolut nödvändigt för syftet med behandlingen.

Vad FRA har anfört

Genom att FRA inriktas mot utländska förhållanden som i hög grad avser konflikter inom och mellan länder samt hot mot Sverige och svenska intressen är det t.ex. inom flertalet inriktningsområden absolut nödvändigt att behandla uppgifter som avser ras, etniskt ursprung, politiska åsikter samt religiös eller filosofisk övertygelse. Detta för att kunna förstå och beskriva aktörers bevekelsegrunder och agerande samt deras relevans i sammanhanget. Behandling av känsliga personuppgifter kan även vara nödvändig för att FRA:s uppdragsgivare ska kunna bedöma såväl potentiella som reella källors lämplighet och tillförlitlighet.

Enligt FRA:s interna föreskrifter ska behandling av känsliga personuppgifter föregås av ett skriftligt beslut i vilket förutsättningarna för behandling anges. Av beslutet ska framgå varför det anses absolut nödvändigt att behandla de känsliga personuppgifterna och vilka typer av känsliga personuppgifter inom respektive underrättelseområde beslutet avser. Beslut om behandling av känsliga personuppgifter fattas en gång per år. Därefter gör analytiker inom ramen för beslutet en bedömning i varje enskilt fall. Om en analytiker känner osäkerhet i hur en enskild bedömning ska göras lyfter denne frågan vidare. Det finns inte någon teknisk funktion som säkerställer att den nödvändighetsbedömning som ska göras dokumenteras i FRA:s IT-system.

Datainspektionens bedömning

FRA har i många sammanhang ett behov av att registrera och behandla känsliga personuppgifter. Samtidigt måste även i denna verksamhet restriktivitet iakttas i fråga om att behandla sådana uppgifter vilket följer av kravet på absolut i nödvändighet i 1 kap. 11 § FRA-PuL. Datainspektionen förordade i sin rapport från 2010 en teknisk funktion för att säkerställa att den avvägning som gjorts när det gäller nödvändighetsbedömning dokumenteras i systemen. Någon sådan funktion har inte införts. Mot bakgrund av de rutiner och föreskrifter som finns ifråga om behandling av känsliga

personuppgifter, tillsammans med de iakttagelser som Datainspektionen har gjort, bedömer inspektionen sammanfattningsvis att FRA ändå har goda förutsättningar för att säkerställa att hanteringen uppfyller kraven i 1 kap. 11 §. Inspektionen har i sin granskning inte heller gjort några iakttagelser som indikerar att FRA behandlar personuppgifter i strid med 1 kap. 11 §.

Förstöringsplikt

Bestämmelser om förstöringsskyldighet för uppgifter under vissa förutsättningar finns i LSF. Av 2 a § följer att om signaler mellan avsändare och mottagare i Sverige inte kan avskiljas redan vid inhämtningen ska upptagningen eller uppteckningen förstöras så snart det står klart att sådana signaler har inhämtats. Av 7 § framgår bland annat att upptagning eller uppteckning av uppgifter ska förstöras om innehållet saknar betydelse för försvarsunderrättelseverksamheten eller avser uppgifter för vilka tystnadsplikt gäller.

Vad FRA har anfört

Närmare regler om hur förstöringsplikten enligt 2 a § och 7 § LSF ska hanteras finns i FRA:s interna föreskrifter. Varje medarbetare ska se till att förstöring sker i det system som vederbörande arbetar i.

När det gäller den absoluta förstöringsplikten av s.k. inhemsk trafik enligt 2 a § LSF bedrivs inhämtning i internationella gränssnitt varför det ligger i sakens natur att den trafik som är åtkomlig för FRA oftast har minst en av de kommunicerande parterna belägen i utlandet. Eftersom viss inrikes trafik förmedlas via utländska kommunikationstjänster kommer dock även sådan trafik löpa risk att inhämtas. FRA filtrerar bort inrikes trafik i fall när det är möjligt att med automatiska metoder identifiera sådan trafik. I övrigt hanteras frågan genom utbildning av personalen. Det sker en löpande bedömning och dokumentation avseende sådana fall där det är svårt att avgöra huruvida viss inhämtad trafik träffas av förstöringsplikten eller inte. Försvarsunderrättelseverksamheten får endast avse utländska förhållanden. Därför är förekomsten av förstöringspliktiga meddelanden enligt 7 § 2 och 3 LSF, dvs. uppgifter för vilka tystnadsplikt gäller och uppgifter i meddelanden som avser kommunikation mellan en brottsmisstänkt och dennes försvarare, mycket sällan förekommande. Om ett meddelande förstörs av en medarbetare i det system som vederbörande arbetat i, ska därefter en särskilt utpekad befattningshavare kontaktas för uppföljning av förekomst av uppgifterna i andra system.

Förstöringsplikten i 7 § 1 LSF av uppgifter som har bedömts sakna betydelse för verksamheten uppfylls genom två olika metoder, ”ta bort” respektive ”förstöra”. Användning av ”ta bort” innebär att uppgifterna tas bort från det egna projekt i vilket uppgifterna bedömts sakna betydelse. Användning av ”förstöra” innebär att uppgifterna förstörs i samtliga projekt. Uppgifter lämnade under bikt eller enskild själavård regleras i 7 § 4 LSF och ska förstöras om det inte finns synnerliga skäl att behandla uppgifterna för försvarsunderrättelsesyften. Ett synnerligt skäl kan vara att skydda svensk personal eller avvärja hot mot svenska intressen vid svenskt deltagande i eller genomförandet av fredsfrämjande och humanitära internationella insatser.

Det system där merparten av allt inhämtat meddelandeinnehåll behandlas är försett med en inbyggd automatisk förstöringsfunktion vilken innebär att meddelanden automatiskt förstörs om de inte granskats av en analytiker inom 30 dagar efter att inhämtning skett.

Datainspektionens bedömning

Datainspektionen konstaterade i sin rapport från 2010 att inhämtning av signaler mellan avsändare och mottagare som båda befinner sig i Sverige (så kallad inhemsk trafik) enligt 2 a § LSF i första hand bör uteslutas genom automatiska processer. FRA har anfört att sådana automatiska processer eller metoder finns och används när det är möjligt men att det samtidigt inte går att fullt ut undvika inhämtning av inhemsk trafik. Datainspektionen konstaterar, såsom FRA också anfört, att det sätt på vilket kommunikation över Internet sker (t.ex. genom förmedling via olika mailservrar runt om i världen) innebär att det inte alltid finns någon koppling mellan teleadress och användarens geografiska position. Det är i sådana fall inte möjligt att med hjälp av automatiska processer helt utesluta inhämtning av inhemsk trafik. Detta medför enligt Datainspektionens mening i sin tur att bestämmelserna om förstöringsplikt avseende sådan trafik blir än viktigare. I rapporten från 2010 betonade inspektionen vikten av att det finns fungerande rutiner för hur förstöring av inhemsk trafik ska hanteras. Datainspektionen har tagit del av FRA:s verksamhetsföreskrifter i detta avseende och finner att det i dessa finns konkreta och detaljerade anvisningar för hur de enskilda medarbetarna ska hantera frågor om förstöring av inhemsk trafik. FRA har också uppgett att personalen ges utbildning i dessa frågor och att det finns rutiner för hur det praktiska arbetet ska bedrivas och för löpande utvärdering av hanteringen.

Även när det gäller förstöringsplikten i 7 § LSF ansåg Datainspektionen i sin rapport från 2010 att det fanns behov av rutiner och utbildning av personal för att säkerställa att meddelanden som inhämtats inte blir föremål för vidare behandling utan att det först har kontrollerats att meddelandena inte innehåller förstöringspliktig information. Inspektionen kan konstatera att FRA:s verksamhetsföreskrifter tydligt anger hur förstöringsplikten i 7 § ska hanteras.

Sammanfattningsvis gör Datainspektionen bedömningen att de rutiner och verksamhetsföreskrifter som finns gällande förstöringsplikt innehåller detaljerade anvisningar ifråga om hantering av förstöringspliktig information. Datainspektionen har i sin granskning inte gjort några iakttagelser som visar att förstöringspliktig information behandlas i strid med bestämmelserna. Mot denna bakgrund bedömer Datainspektionen att FRA tillämpar reglerna om förstöringsplikt i LSF på ett korrekt sätt.

I detta sammanhang kan också erinras om att SIUN har till uppgift att granska den förstöring som FRA utför i enlighet med 2 a § och 7 § LSF.

Gallring

I 6 kap. 1 § FRA-PuL anges att personuppgifter ska gallras så snart uppgifterna inte längre behövs för det ändamål för vilket de behandlas. I 2 § FRA-PuF finns närmare bestämmelser om gallring i vissa särskilda fall.
Av 2 § FRA-PuF följer att personuppgifter får behandlas i uppgiftssamlingar för råmaterial och att sådant material ska gallras senast ett år efter det att behandlingen av uppgifterna påbörjades.

Vad FRA har anfört

För uppgiftssamlingar för råmaterial finns interna gallringsrutiner som generellt bygger på en automatisk gallring. FRA har inte upplevt något fall där den automatiska gallringen inte fungerat. I vissa av uppgiftssamlingarna gallras personuppgifterna tidigare än vad lagen kräver, exempelvis efter fem dagar, 30 dagar eller tre månader. Tidsgränserna varierar av olika anledningar, exempelvis kan det röra sig om utrymmesskäl vad gäller lagringskapacitet. System avsedda för råmaterial är inte byggda utifrån långtidslagring av information. En annan anledning kan vara att en bedömning har gjorts att inhämtat material inte fyller syftet för behandlingen efter en viss tid.

Ett fåtal uppgiftssamlingar för råmaterial har manuella rutiner för gallring. I dessa uppgiftssamlingar gallras personuppgifterna löpande i det dagliga arbetet samt med viss periodicitet.

Datainspektionens bedömning
Mot bakgrund av att allt fler personers kommunikation riskerar att inhämtas till FRA i form av trafikdata (se s. 6) är det viktigt att så långt som möjligt begränsa det integritetsintrång som härigenom kan uppkomma. Ett sätt att uppnå detta är att ha bestämmelser som innebär att personuppgifter inte får behandlas i verksamheten under längre tid än nödvändigt. En effektiv försvarsunderrättelseverksamhet kan i vissa fall kräva mycket långa bevarandetider (se bland annat prop. 2006/07:46, s. 110f). Beträffande uppgiftssamlingarna för råmaterial, dvs. information vars relevans för verksamheten ännu inte bedömts, gäller emellertid en gallringsfrist om högst ett år. Enligt vad som framkommit gallras uppgifter i vissa av uppgiftssamlingarna långt tidigare än vad som följer av FRA-PuL, vilket är positivt ur integritetssynpunkt.

Datainspektionen har inom ramen för detta tillsynsärende inte gjort några iakttagelser som visar att uppgifter som är äldre än ett år finns kvar i uppgiftssamlingar för råmaterial och har därför inga synpunkter på hanteringen i detta avseende.

Loggning och logguppföljning

Enligt 3 kap. 2 § FRA-PuL ska FRA vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är.

Vad FRA har anfört
I FRA:s interna föreskrifter samt särskilda beslut finns krav på säkerhetsfunktioner och säkerhetsloggning i myndighetens IT-system som är avsedda för behandling av hemliga uppgifter utifrån vilken informationssäkerhetsklass uppgifterna tillhör.
Möjlighet till uppföljning och kontroll genom loggning ska finnas i provdriftsatta och produktionssatta system.

Sök- och förstöringsloggar sparas idag i de it-system som genererar dem. Det sker i dagsläget inte någon centraliserad analys av sök- och förstöringsloggar. Det är berörd informationsägares ansvar att se till att logganalys sker. Idag sker logguppföljning genom stickprovskontroller av sökloggar. Under 2015 har FRA påbörjat ett arbete med att inrätta en central logganalysfunktion (SOC). Målet är att funktionen ska vara driftsatt 2017. SOC:en ska samla in och granska sök- och förstöringsloggar från samtliga it-system för att bland annat kunna upptäcka otillbörlig behandling av personuppgifter. Nödvändiga regelverk och rutiner för den systematiska uppföljningen av loggar ska vara framtagna och beslutade vid slutet av 2017.

Datainspektionens bedömning

Enligt FRA-PuL åligger det FRA att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Ett led i detta är att genom loggning och logguppföljning säkerställa att de bestämmelser som ska skydda den personliga integriteten tillämpas korrekt. Ett grundläggande säkerhetskrav är att genom loggar skapa en sådan spårbarhet att man till exempel kan upptäcka otillåten tillgång till personuppgifter eller att det sker otillåtna sökningar. Loggarna ska följas upp regelbundet och för att skapa en förebyggande effekt ska användarna informeras om att loggning och logguppföljning sker. I FRA:s verksamhet sker en omfattande personuppgiftsbehandling som också många gånger innebär att känsliga personuppgifter behandlas. Därför är det enligt Datainspektionens mening viktigt att ställa långtgående krav på kontroll och uppföljning av loggar.

Datainspektionen konstaterade i sin rapport från 2010 att det fanns brister i den logguppföljning som då gjordes och att logguppföljningen därför borde förstärkas. I tillsynsärendet har framkommit att dessa brister fortfarande kvarstår trots att det har gått ett antal år sedan påpekandet gjordes. Genom avsaknad av regelbunden logguppföljning bedömer Datainspektionen att FRA inte har de nödvändiga säkerhetsåtgärder på plats som krävs enligt 3 kap. 2 § FRA-PuL. FRA har anfört att det pågår ett arbete inom myndigheten med att införa ett system samt regler och rutiner som bedöms nödvändiga för att säkerställa logguppföljning. Datainspektionen noterar att den brist ifråga om logguppföljning som inspektionen påtalade redan 2010 ännu inte har avhjälpts. Datainspektionen förutsätter att FRA inför den centrala logganalysfunktion som myndigheten har redogjort för i ärendet. Med anledning av den långa tid som gått sedan Datainspektionen påtalade frågan

finns skäl att förelägga FRA att till Datainspektionen senast den 1 maj 2017 lämna en skriftlig redogörelse för de åtgärder som myndigheten har vidtagit och avser att vidta i fråga om den centrala logganalysfunktionen.

Den av SIUN anmälda frågan om tolkningen av 1 kap. 13 § FRA-PuL

I 1 kap. 13 § FRA-PUL anges att behandling som innebär inhämtning av uppgifter genom signalspaning, lagring av uppgifter som sker omedelbart därefter samt bearbetning av information i form av kryptoforcering och språklig översättning inte skall anses som oförenlig med bestämmelserna i 1 kap. 6 och 8-12 §§ (bestämmelser om grundläggande krav, tillåtlighet, känsliga personuppgifter och personnummer) i det skede av behandlingen då det ännu inte kunnat fastställas om informationen innehåller personuppgifter.

Vad FRA har anfört

Praktiskt taget all information innehållande kommunikation mellan människor som inhämtas med stöd av tillstånd innehåller personuppgifter. Det är dock okänt för FRA – intill dess att uppgifterna forcerats, översatts och bedömts av en analytiker – vilka dessa personuppgifter är.

Begreppet ”behandling av personuppgifter” i FRA-PuL omfattar all slags behandling inklusive sådan som sker på automatisk väg. Detta innebär att personuppgiftsbehandling sker redan i det tidiga skede när informationen i tillståndsgivna signalbärare genomgår urval med hjälp av sökbegrepp i FRA:s inhämtningssystem. Detta innebär att personuppgiftsbehandling sker även för all den information som inte inhämtas.

Mycket av de personuppgifter som behandlas på automatisk väg blir aldrig föremål för manuell granskning. Det är därför en omöjlighet för FRA att, såvida inte en analytiker bearbetat och bedömt personuppgifterna, hävda att personuppgifterna behandlas i enlighet med bestämmelser om grundläggande krav, ändamål samt behandling av känsliga personuppgifter och personnummer. FRA uppfattar att det är denna situation lagstiftaren försökt lösa genom bestämmelsen i 1 kap. 13 § FRA-PuL.

FRA:s tolkning av bestämmelsen är således att det är först när FRA fått klarhet i vilka personuppgifter som behandlas som det är möjligt för FRA att behandla dem i överensstämmelse med 1 kap 6 och 8-12 §§ FRA-PuL. Bestämmelsen får anses reglera det fall *”då det ännu inte kunnat fastställas om informationen innehåller personuppgifter och vilka dessa är”*. Denna tolkning kommer också till uttryck i FRA:s interna föreskrifter. Huruvida den

inhämtade informationen innehåller personuppgifter som t.ex. har (eller saknar) anknytning till preciserad inriktning kan, som anförts ovan, bedömas först när uppgifterna behandlats manuellt.

Eftersom det kan förutsättas att praktiskt taget all information som finns i signalbärarna i något avseende innehåller personuppgifter innebär en bokstavlig tolkning av ”då det ännu inte kunnat fastställas om informationen innehåller personuppgifter” att bestämmelsen i 1 kap. 13 § FRA-PuL i praktiken aldrig kan tillämpas. Detta skulle i sin tur bland annat innebära att behandling av personuppgifter i all den information som inte inhämtas bryter mot 1 kap. 8 § FRA-PuL eftersom sådana personuppgifter av naturliga skäl oftast saknar koppling till preciserad inriktning.

Eftersom en bokstavstrogen tolkning av 1 kap. 13 § FRA-PuL i praktiken inte går att förena med inhämtning genom signalspaning är frågan om hur bestämmelsen ska tolkas av väsentlig betydelse för FRA:s verksamhet.

Datainspektionens bedömning

SIUN har i enlighet med 15 § förordningen (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten anmält att det finns anledning att uppmärksamma Datainspektionen på FRA:s tolkning och tillämpning av 1 kap. 13 § FRA-PuL. Frågan gäller FRA:s tolkning, att undantaget i bestämmelsen inte bara avser det skede då det ännu inte kunnat fastställas *om* informationen innehåller personuppgifter, utan även det skede då FRA ännu inte vet *vilka* dessa personuppgifter är.

I prop. 2006/07:46 s. 76 ff. anförs följande om skälen för bestämmelsen.

Försvarets radioanstalt behandlar en mycket stor mängd information som inhämtas genom signalspaning. Inhämtningen sker endast för att Försvarets radioanstalt skall uppfylla sin grundläggande uppgift att genom signalspaning bedriva försvarsunderrättelse- och utvecklingsverksamhet. Inhämtning av signaler sker såväl manuellt utan urval som automatiskt med särskilda sökbegrepp. Oavsett hur inhämtningen sker tillförs Försvarets radioanstalt stora mängder obearbetad information. I informationen kan det dölja sig uppgifter om enskilda personer och också känsliga personuppgifter och personnummer. Försvarets radioanstalt har utöver den begränsning av inhämtningen som användandet av sökbegrepp innebär liten möjlighet att påverka innehållet i den information som inhämtas. I princip inhämtas all den information som träffas av sökbegreppen, oavsett dess relevans för verksamheten. Det är följaktligen i viss mån okänt för Försvarets radioanstalt vid

själva inhämtningen och den efterföljande lagringen vad den inhämtade informationen innehåller. Därtill kommer att informationen ofta är såväl krypterad som avfattad på ett främmande språk. Det är i detta skede således inte möjligt för myndigheten att ”censurera” innehållet i information som på detta sätt kommer in i elektronisk form genom att ta bort t.ex. känsliga personuppgifter. Det är först sedan de inhämtade signalerna lagrats och därefter bearbetats genom att signalskyddet forcerats och informationen översatts som informationen kan tas fram i klartext eller sändningarnas innehåll kan beskrivas. Det är då myndigheten får klart för sig om det insamlade materialet innehåller personuppgifter och om det även är fråga om t.ex. känsliga personuppgifter. Med hänsyn till att de inhämtade signalerna således utan Försvarets radioanstalts vetskap kan innehålla personuppgifter, kan fråga uppkomma om myndigheten i ett initialt skede kan anses behandla dessa personuppgifter enligt de regler om ändamål m.m. som föreslås här. (…) Först sedan uppgifterna bearbetats genom kryptoforcering och språklig översättning kan Försvarets radioanstalt konstatera om det är fråga om personuppgifter. Därefter får inte ytterligare personuppgiftsbehandling, som t.ex. vidare bearbetning eller lagring, ske utan att behandlingen överensstämmer med de övriga bestämmelser som föreslås gälla för personuppgiftsbehandlingen.

Sedan FRA-PuL:s ikraftträdande har förutsättningarna för inhämtning ändrats genom att FRA i och med att LSF, som trädde ikraft 2009, fått möjlighet att bedriva signalspaning mot kommunikation i tråd. Detta har inneburit att den mängd trafik som inhämtas är avsevärt större och att inhämtningen i större omfattning riktar sig mot det globala nätet, det vill säga miljöer och förhållanden där det inte bara finns sådan trafik som kan vara relevant för försvarsunderrättelseverksamheten. Inhämtningen träffar i stor utsträckning enskilda människors kommunikation vilket innebär att integritetsaspekterna gör sig gällande på ett ännu tydligare sätt än tidigare då endast satellitburna delar av det globala nätet inhämtades.

Att integritetsskyddsbestämmelserna i FRA-PuL gäller vid behandling av personuppgifter som inhämtats enligt LSF framgår av lagens 12 a §. I förarbetena till LSF finns inga uttalanden som visar att lagstiftaren mot bakgrund av de förändrade förutsättningarna för signalspaning sett något behov av särreglering eller undantag från 1 kap. 13 § eller andra bestämmelser i FRA-PuL.

Genom att signalspaningen riktas mot kommunikation mellan enskilda personer ligger det i sakens natur att en betydande mängd av den inhämtade informationen innehåller personuppgifter. Bestämmelsen i 1 kap. 13 § FRA-PuL ger utrymme för att inte tillämpa FRA-PuLs bestämmelser i ett initialt

skede, uttryckt som *”det skede av behandlingen då det ännu inte kunnat fastställas om informationen innehåller personuppgifter”*. Datainspektionen konstaterar att bestämmelsen enligt sin ordalydelse inte undantar tillämpning av 1 kap. 6 § och 8-12 §§ i de fall man redan från början vet att den inhämtade informationen innehåller personuppgifter. FRA har anfört att bestämmelsen istället får anses reglera det skede då det ännu inte kunnat fastställas *vilka dessa personuppgifter är*. Enligt Datainspektionen finns det inte stöd för en sådan tolkning vare sig i bestämmelsens ordalydelse eller i förarbetena till FRA-PuL.

FRA är den myndighet som har i uppdrag att inhämta signaler i elektronisk form vid signalspaning enligt LSF. Myndigheten har därigenom getts möjlighet att inhämta information som i mycket stor utsträckning innehåller personuppgifter. Med den utgångspunkten och mot bakgrund av vad FRA har anfört i fråga om hur verksamheten bedrivs och måste bedrivas, kan det ifrågasättas om det överhuvudtaget är möjligt att, såsom förutsätts i 1 kap. 13 § FRA-PuL, gå in och granska all inhämtad kommunikation för att avgöra om bestämmelserna i 1 kap. 6 och 8-12 §§ är uppfyllda.

Förutsättningarna för den försvarsunderrättelseverksamhet som FRA bedriver är under ständig förändring både med hänsyn till förändringar i omvärlden och med hänsyn till den tekniska utvecklingen, vilken ger nya möjligheter att inhämta information. Detta innebär att de regelverk som styr verksamheten också måste kunna tillämpas under sådana förhållanden. Det råder av naturliga skäl en starkt begränsad insyn i den verksamhet som FRA bedriver. Möjligheterna för den enskilde att få kännedom om och insyn i den personuppgiftsbehandling som sker är därför mycket små. Det medför att det måste ställas extra stora krav på att lagstiftningen är klar och tydlig så att det finns en förutsebarhet som till viss del kompenserar bristen på insyn för den enskilde.

Frågan om hur bestämmelsen i 1 kap. 13 § FRA-PuL ska tolkas och tillämpas är av central betydelse. Datainspektionen anser, i likhet med FRA, att bestämmelsen i sin ordalydelse i praktiken inte går att förena med inhämtning genom signalspaning på det sätt som det förefaller ha förutsatts genom införandet av LSF. Det är således uppenbart att bestämmelsen inte är anpassad till de behov och förutsättningar som gäller för FRA:s verksamhet idag. Datainspektionen kan konstatera att det finns en konflikt mellan bestämmelsen i 1 kap. 13 § och den personuppgiftsbehandling som LSF

genererar hos FRA efter inhämtningsskedet. Lagstiftaren har uttalat att både LSF och FRA-PuL måste beaktas när det gäller skyddet mot att människors personliga integritet kränks genom den personuppgiftsbehandling som signalspaningen ger upphov till (prop. 2008/09:201, s. 83). Sambandet har tydliggjorts i 12 § a LSF som hänvisar till FRA-PuL.

Datainspektionen bedömer dock att det inte är möjligt att tillämpa 1 kap. 13 § FRA-PuL i samband med signalspaning enligt LSF. Frågan om hur bestämmelsen ska tolkas borde enligt inspektionen ha tagits upp vid införandet av LSF. Detta gjordes dock inte. Det är Datainspektionens uppfattning att bestämmelsen behöver ses över och anpassas till det nya mandat som lagstiftaren har gett FRA genom LSF. Datainspektionen finner mot den angivna bakgrunden anledning att uppmärksamma regeringen (Försvarsdepartementet) på detta behov.

Detta beslut har fattats av generaldirektören Kristina Svahn Starrsjö efter föredragning av juristen Elisabeth Jilderyd. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom, enhetschefen Nicklas Hjertonsson och juristen Cecilia Agnehall deltagit.

Kristina Svahn Starrsjö

Elisabeth Jilderyd

Kopia till:

Försvarsdepartementet, 103 33 Stockholm (för kännedom)
Statens inspektion för försvarsunderrättelseverksamheten, Box 1140, 164 22 Kista (för kännedom)