Skatteverket

Datum 2017-04-25
Dnr 131 98780-17/112

Justitiedepartementet
Enheten för lagstiftning om allmän ordning och säkerhet och samhällets krisberedskap

Remiss av promemorian Tillhandahållande av tekniska sensorsystem – ett sätt att förbättra samhällets informationssäkerhet

Ju2017/02002/L4 Skatteverket

1 Sammanfattning

Skatteverket instämmer i promemorians bedömning att användningen av sensorsystem är av stor betydelse för att kunna upprätthålla ett heltäckande och funktionellt it-skydd mot antagonistiska hot och störningar. Möjligheten att använda sensorsystem för både verksamhetsutövare, för egen verksamhet, och för MSB, för samordning och överblick, är centralt för en uppbyggnad av ett nationellt it-skydd.

Skatteverket anser dock att flera av de rättsliga analyser som görs i promemorian är bristfälliga och att slutsatserna kan ifrågasättas. Även fullständigheten i vilka rättsliga frågor som analyserats kan ifrågasättas.

Med hänsyn till sensorsystemens betydelse för informationssäkerheten i det moderna samhället bör särskilt frågorna om fördelningen av personuppgiftsansvaret mellan verksamhetsutövare och tillhandahållare samt behovet av sekretessbrytande reglering upptas till förnyad utredning.

Postadress: 171 94 Solna Telefon: 0771-567 567
huvudkontoret@skatteverket.se, www.skatteverket.se

2 Skatteverkets synpunkter

Nedan lämnar Skatteverket synpunkter på några av de frågor som behandlas i promemorian.

2.1 Integritetsavvägningen enligt 2 kap. 6 § regeringsformen (s. 10)

I promemorian bortses helt från att den uppgiftssamling som skapas i trafikflödesdatabasen kommer att beskriva enskildas interaktion med verksamhetsutövare. Idag har många myndigheter och andra kunskap om IP-adresser och dessas koppling till enskilda individer. Kopplingen är inte sällan säkerställd via t.ex. e-legitimation då användaren loggat in till en e-tjänst. Med den kunskapen som utgångspunkt blir trafikflödesdatabaserna hos den samlade skaran verksamhetsutövare en rik informationskälla över enskildas interaktion med myndigheter och ev. andra. Den här aspekten borde ha haft en naturlig plats i promemorians integritetsavvägning enligt 2 kap. 6 § regeringsformen. Möjligheten till kartläggning och övervakning i detta hänseende är uppenbar och intrånget i den enskildes integritet är, i varje fall, inte oväsentligt.

2.2 Behandling av personuppgifter vid MSB:s tillhandahållande av sensorsystem

2.2.1 Ändamålsbestämmelsen i personuppgiftslagen (s. 14)

Skatteverket delar bedömningen att behandlingen av personuppgifter i sensorsystemet i syfte att upprätthålla såväl egen som samhällets informationssäkerhet i normalfallet inte bör anses stå i strid med finalitetsprincipen. Därmed dock inte sagt, såsom antyds i promemorian, att samtliga grundläggande krav i 9 § PuL kan anses uppfyllda.

2.2.2 Personuppgiftsansvaret (s. 16)

I 3 § personuppgiftslagen definieras den personuppgiftsansvarige som den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Enligt promemorian ska verksamhetsutövaren vara den som är personuppgiftsansvarig för den personuppgiftsbehandling som kan komma att ske inom sensorsystemet. Förläggningen av personuppgiftsansvaret hos verksamhetsutövaren kan förefalla rimlig med hänsyn till att det är denne som frivilligt efterfrågar tjänsten hos MSB och att den nätverkstrafik som passerar sensorerna tillhör verksamhetsutövaren. MSB anges agera personuppgiftsbiträde i förhållande till verksamhetsutövaren och biträdets behandling av uppgifter sker i enlighet med det regelverk och de ändamål som gäller för verksamhetsutövaren.

Om man i frågan om förläggningen av personuppgiftsansvaret beaktar hur ändamålen med sensorsystemen formuleras, dels att bistå anslutna verksamhetsutövare att upptäcka och hantera IT-incidenter och dels att få en samlad lägesbild över IT-incidenter i samhället och att kunna stödja och varna andra aktörer i samhället, framträder tydligt att en inte oväsentlig del av ändamålet uteslutande betingas av MSB:s verksamhet och inte alls av den enskilde

verksamhetsutövarens. Detta är behandlingar som en enskild verksamhetsutövare inte kan eller har förmåga att ta ett personuppgiftsansvar för.

Promemorians slutsats att ensidigt lägga personuppgiftsansvaret på verksamhetsutövaren kan inte vara riktig. Personuppgiftsansvaret bör istället fördelas mellan verksamhetsutövare och tillhandahållare på ett sådant sätt att ansvarsförhållandet inte hindrar eller försvårar den viktiga funktion som sensorsystem har. Samtidigt ska fördelningen vara sådan att den som är ansvarig har förutsättningar att ta ansvar och möjlighet att tillmötesgå den enskildes legitima krav på värnad integritet.

2.3 Frågor om offentlighet och sekretess (s. 21)

Skatteverket instämmer i uppfattningen att sensorsystemet hos resp. ansluten verksamhetsutövare bör omfattas av sekretess enligt 18 kap. 8 § OSL. Enligt Skatteverkets uppfattning borde promemorian ha varit tydligare med att redan uppgift om anslutning till ett sensorsystem bör omfattas av nämnda sekretess.

En farhåga i sammanhanget är i vilken omfattning som uppgifterna i trafikflödesdatabasen kan skyddas med stöd av 18 kap. 8 § OSL. Uppgifterna i trafikflödesdatabasen utgörs av en kontinuerlig avläsning av den nätverkstrafik som går till och från den anslutna verksamhetsutövaren. Uppgiftssamlingen i trafikflödesdatabasen kommer, beroende på den anslutna verksamhetsutövarens verksamhet, att inom kort tid bli omfattande. Uppgifterna bör rimligen i allt övervägande del utgöras av trafikuppgifter som inte har något med antagonistiska aktiviteter eller it-hot att göra samt bestå av uppgifter som idag är normalt tillgängliga för alla och envar med stöd av handlingsoffentligheten. Man kan därför fråga sig om det verkligen kommer att vara möjligt att skydda enstaka uppgifter i trafikflödesdatabasen med stöd av 18 kap. 8 § OSL.

Promemorians resonemang kring behov och tillämpning av sekretess utgår i huvudsak från den information som samlats in av sensorsystemet och som blir föremål för behandling i larmdatabasen, i förteckningen eller i trafikflödesdatabasen. En aspekt som över huvud taget inte berörs i promemorian är att redan en tillämpning av sensorsystemet innebär att uppgifter som hör till verksamhetsutövarens verksamhet kommer att röjas för tillhandahållaren. När sensorsystemet läser av trafikinformationen till och från verksamhetsutövaren röjs trafikuppgifter. När larmsensorerna ger signal om ett uppmärksammat hot och en inspelning görs kommer uppgifter i t.ex. e-postmeddelanden att röjas i klartext.

Inom Skatteverket finns ett antal självständiga verksamhetsgrenar. Den största av dessa verksamhetsgrenar är beskattningsverksamheten inom vilken bl.a. sekretess enligt 27 kap. 1 § OSL gäller. Sekretessen enligt nämnda bestämmelse är absolut. För att kunna röja information som omfattas av sekretessbestämmelsen i 27 kap. 1 § OSL krävs en sekretessbrytande bestämmelse. Finns ingen sådan tillämplig sekretessbrytande bestämmelse saknas det rättsliga förutsättningar för att röja aktuella uppgifter från Skatteverkets nätverkstrafik.

Någon särskild sekretessbrytande bestämmelse som avser säkerhets- eller bevakningsåtgärder finns inte som är tillämpliga på uppgifter inom Skatteverkets

beskattningsverksamhet. Generella sekretessbrytande bestämmelser finns, t.ex. 10 kap. 2 och 27 §§ OSL. Båda dessa bestämmelser ska tillämpas med restriktivitet och normalt inte för rutinbetonade utlämnanden. Med hänsyn till att anslutningen till sensorsystem dels är frivillig och dels, i avläsningen och för behandling i trafikflödesdatabasen, avser all nätverkstrafik till och från myndigheten kan en tillämpning av nämnda sekretessbrytande bestämmelser ifrågasättas.

Skatteverkets uppfattning är, med hänsyn till den sekretess som gäller inom myndighetens beskattningsverksamhet, att de rättsliga förutsättningarna för myndigheten att utnyttja det föreslagna sensorsystemet är oklara. Ett klargörande om aktuell och nödvändig information får röjas inom ramen för sensorsystemet till tillhandahållaren utan stöd av en ny sekretessbrytande regel är önskvärt.

2.4 Oklart hur myndigheters IT-samverkan eller värd- och nämndmyndigheter ska hanteras

Skatteverket tillhandahåller infrastruktur och tjänster för datatrafik och e-post till ett antal andra myndigheter, exempelvis Kronofogdemyndigheten och Valmyndigheten. Dessa myndigheter behöver inte nödvändigtvis ha ett särskilt ansvar i enlighet med förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Skatteverket har normalt inte personuppgiftsansvar för dessa myndigheters behandlingar.

Ett sensorsystem kan sannolikt filtrera vilken trafik som ska analyseras. Exempelvis kan all e-post som är adresserad till den samverkande myndigheten filtreras så att det inte analyseras eller spelas in. Vid en sådan filtrering kan dock inte alla hot mot gemensam infrastruktur och tjänster upptäckas. Värdet av sensorsystemet begränsas då i en okänd omfattning.

Skatteverket anser att promemorian helt saknar underlag för att beskriva denna typ av användningsfall och hur de ska hanteras med föreslagen förordningsbestämmelse och med stöd av den författning som promemorian hänvisar till.

Skatteverket föreslår att departementet utreder hur dessa frågor ska hanteras och att förordningsbestämmelsen utformas efter detta.

2.5 Övriga synpunkter

2.5.1 Detekteringssensorerna (s. 6)

Promemorian anger att detekteringssensorerna placeras utanför verksamhetsutövarens brandvägg och går igenom all in- och utgående trafik från verksamhetsutövaren. Skatteverket tolkar det som att sensorsystemet kommer att genomföra en så kallad passiv kommunikationsavläsning av all trafik som passerar sensorsystemets sensorer.

En sådan passiv avläsning innebär att det endast är elektroniskt kommunikation som inte är krypterad som kommer att kunna analyseras avseende skadligt innehåll. Då en stor och ökande mängd kommunikation är krypterad kommer endast en begränsad analys av trafiken att kunna utföras.

Av underlaget framgår inte i vilken mån det uppstår begränsningar i förmågan att upptäcka hot när så kallad passiv detektering av krypterad kommunikation används. Även om Skatteverket har förståelse för att inga detaljer om sensorsystemets förmåga kan beskrivas av säkerhetsskäl så ser Skatteverket ser det som en brist i underlaget.

Vidare så framhåller promemorian att sensorsystemet "ger ett utökat skydd" framför kommersiella lösningar. En kommersiell lösning kan dock placeras på insidan och där även analysera trafik som inte är krypterad.

2.5.2 Påverkan på Skatteverkets förtroende

Medborgare och företag kommunicerar med Skatteverket via digitala kanaler i mycket stor omfattning. Detta förutsätter att Skatteverket hanterar den information som erhålls på ett säkert och rättsligt korrekt sätt. Att Skatteverket arbetar för en bra IT-säkerhet är sannolikt förtroendeskapande. Ur den aspekten kan en användning av sensorsystem vara till fördel för samhällets förtroende för Skatteverket.

Om det skulle inträffa händelser som innebär att medborgares eller företags information sprids till obehöriga eller hanteras fel med en ökad risk för integritetskränkningar är påverkan på förtroendet för Skatteverket dock motsatt. Även ett scenario där användning av sensorsystem medför störningar som påverkar tillgängligheten till Skatteverkets IT-system kan leda till förtroendeskada.

2.5.3 Konsekvenser och ikraftträdande (s. 23)

Konsekvensanalysen av förslaget till ny förordningsbestämmelse är i promemorian endast rudimentärt beskriven och ger ingen vägledning för att Skatteverket ska kunna bedöma konsekvenser med tillförlitlig grund. Promemorian anger att kostnader för anslutning och löpande anpassning ska belasta verksamhetsutföraren. I detta anges inga uppgifter om belopp eller resurstimmar som bedöms vara relevanta. Sådana kostnader bör dessutom vara olika beroende på hur verksamhetsutövarens kommunikationsvägar är konstruerade.

Detta remissvar har beslutats av generaldirektören Ingemar Hansson och föredragits av säkerhetsstrategen Roland Jidrot. Vid den slutliga handläggningen har också följande deltagit: avdelningschefen Fredrik Rosengren, säkerhetschefen Lotta Oscarsson och rättsliga experten Gunnar C Svensson.

Ingemar Hansson

Roland Jidrot