SÄKERHETS- OCH INTEGRITETSSKYDDSNÄMNDEN

Uttalande

2012-09-04 Dnr 117-2012

Granskning av polismyndigheternas användning av centrala säkerhetsloggen

1 SAMMANFATTNING

Nämnden har granskat de 83 beställningar av loggutdrag från den centrala säkerhetsloggen (CSL) vid Rikspolisstyrelsen (RPS) som polismyndigheterna gett in till Verksamhetsskyddsenheten under tiden 1 mars – 30 juni 2012 och som avser IT-system som regleras av polisdatalagen (2010:361) (PDL).
Av granskningen framgår att flertalet polismyndigheter inte har gjort någon logguppföljning alls för de CSL-anslutna IT-systemen under den granskade perioden, och att logguppföljningen har varit av mycket begränsad omfattning även hos vissa av de större polismyndigheterna. De flesta beställningar är reaktioner på misstänkt otillåtna slagningar och avser förfluten tid. Nämnden förutsätter att loggutdrag från CSL i större utsträckning än vad som framgår av det granskade materialet kommer att användas löpande och i förebyggande syfte, för att säkerställa att användare endast tar del av information de behöver för att kunna fullgöra sina arbetsuppgifter. Nämnden anser vidare att dokumentationen i beställningsärendena bör förbättras för att möjliggöra mer ändamålsenlig tillsyn.

2 BAKGRUND

Syftet med PDL är att ge polisen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin brottsbekämpande verksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling. Mer konkret är syftet med lagen bland annat att möjliggöra att personuppgifter kan behandlas hos polisen i större system i stället för i flera separata register. Det är också polisens ambition att successivt samla de uppgifter som behandlas i polisens verksamhet i större, centrala IT-system.[1] Vid personuppgiftsbehandling i stora uppgiftssamlingar blir begränsningar av tillgängligheten för användarna ett viktigt integritetsskydd, vilket avspeglas i den nya lagstiftningen. Tilldelning av behörigheter och olika typer av uppföljning, såsom loggning, blir

[1] Prop. 2009/10:85 s. 60 f.

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

därmed centrala verktyg för att upprätthålla integritetsskyddet vid behandling av personuppgifter enligt PDL.

För att förbättra den tekniska kontrollen över IT-användningen har polisen utvecklat ett system för att samla in och analysera loggar från polisens IT-system; CSL. Systemet drivs och underhålls av RPS. Syftet med CSL är dels att skydda enskildas integritet, dels att skydda den information som polisen behandlar mot otillåten behandling och angrepp.[2]

Befintliga IT-system ansluts successivt till loggen, medan CSL-anslutning byggs in från början i nya system. Enligt uppgift från RPS var bland annat det nya ärendehanteringssystemet PUST, förundersöknings-registret DurTvå och det centrala kriminalunderrättelseregistret (KUR) anslutna till CSL i april 2012. Beställningsverksamheten vid CSL har varit i fullt bruk sedan november 2011.

3 RÄTTSLIG REGLERING

I 2 kap. 1 och 2 §§ PDL föreskrivs att 31 § personuppgiftslagen (1998:204) (PUL) gäller för polisens personuppgiftsbehandling enligt PDL. Enligt 31 § PUL ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas.

Enligt 2 kap. 11 § PDL ska tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Bestämmelsen riktar sig till dem som deltar i polisens dagliga verksamhet, till dem som ansvarar för utformningen av nya datasystem liksom till dem som avgör vilken tillgång till personuppgifter respektive tjänsteman behöver.[3] I förarbetena betonas att det åligger polisen att följa upp att lagstiftningen tillämpas med respekt för enskildas integritet samt att PDL ställer högre krav än tidigare på att polisen genom tekniska åtgärder begränsar den enskilde tjänstemannens tillgång till information. Loggning nämns som ett sätt för polisen att försäkra sig om att varje användare bara får del av den information han eller hon behöver.[4]

I RPS föreskrifter om säkerhet vid Polisens informationsbehandling med stöd av IT (RPSFS 2009:4, FAP 174-1) finns bestämmelser om behörighetskontroll och loggning. Av 9 kap. 11-16 §§ i föreskrifterna

[2] Prop. 2009/10:85 s. 271.
[3] A. prop. s. 326.
[4] A. prop. s. 271.

framgår bland annat att myndigheten ska se till att loggar följs upp och vid behov analyseras. Myndighetschefen, den denne bestämmer eller chefen för en internutredningsenhet får beställa utdrag ur loggar. Utdrag ur en logg som inte finns tillgänglig vid myndigheten ska beställas hos RPS. RPS ansvarar för att beslut om beviljande av utdrag ur logg som beställs hos RPS dokumenteras.

4 TILLSYNENS OMFATTNING

Nämnden har från Verksamhetsskyddsenheten vid RPS inhämtat samtliga beställningar av utdrag från CSL som inkommit under tiden 1 mars – 30 juni 2012. Nämnden har även begärt uppgifter om fördelning mellan olika polismyndigheter under perioden.

5 SAMMANSTÄLLNING AV DET GRANSKADE MATERIALET

Under den granskade perioden har sammanlagt 85 beställningar avseende loggutdrag från CSL tagits emot av Verksamhetsskyddsenheten, varav 83 avsåg kontroller i IT-system som regleras av PDL. Av dessa har 26 beställningar gjorts av RPS internutredningsenhet i Stockholm, elva av Polismyndigheten i Stockholms län, nio av Polismyndigheten i Västernorrlands län samt mellan en och fem av RPS respektive internutredningsenheter i Göteborg, Linköping, Malmö, Umeå, Västerås och hos RPS centralt. Därutöver har polismyndigheterna i Dalarna, Kalmar, Skåne, Södermanland, Västra Götaland och Värmland samt RPS, Rikskriminalpolisen och Säkerhetspolisen gjort en till tre beställningar vardera.

Av beställningarna framgår att i vart fall 60 av dem är föranledda av en misstanke om att en användare har tagit del av uppgifter i polisiära register som han eller hon inte har rätt att ta del av. I dessa fall framgår oftast av beställningen att internutredning eller förundersökning pågår.

I nio av de granskade beställningarna anges att syftet är ”stickprov”. I samtliga dessa beställningar är beställaren Polismyndigheten i Västernorrlands län. De nio beställningarna avser nio olika personer och är inkomna den 1 och 2 mars 2012.

Åtminstone tio beställningar har gjorts i verksamhetsskyddssyfte, exempelvis för att säkerställa att uppgifter i en viss utredning inte sprids eller har spritts till obehöriga personer. Av dessa har tre särskilt avsett kontroll av om användare har spritt information till personer med koppling till grov organiserad brottslighet. I två beställningar har säkerhetsprövning angetts vara syftet. En beställning avser utlämnande av allmän handling. Fyra beställningar saknar ett

tydligt angivande av syftet. Två av dessa fyra beställningar är tillägg som hänvisar till tidigare ingivna beställningar

Fem beställningar gäller övervakning av loggar i realtid, övriga beställningar avser historiska uppgifter.

6 NÄMNDENS IAKTTAGELSER

Granskningen avser en relativt kort tidsperiod. Det är därför inte möjligt att dra långtgående slutsatser av det granskade materialet. Det bör även beaktas att beställningsverksamheten vid CSL endast har pågått sedan november 2011. Nämnden anser dock att granskningen föranleder följande påpekanden.

Endast åtta av 21 polismyndigheter har utnyttjat möjligheten att begära loggutdrag från CSL under den granskade perioden. Storstadsregioner som Skåne och Västra Götaland har bara gjort tre beställningar vardera. Enligt uppgift från Verksamhetsskyddsenheten på RPS kan inte loggkontroll avseende CSL-anslutna system göras på annat sätt än genom en sådan begäran. Det innebär att flertalet polismyndigheter inte har gjort någon logguppföljning alls för flera av de största systemen sedan PDL trädde i kraft den 1 mars 2012 och under den granskade perioden, och att logguppföljningen för CSL-anslutna system har varit av mycket begränsad omfattning även hos de större polismyndigheterna med undantag för Polismyndigheten i Stockholms län.

I vart fall två tredjedelar av de granskade beställningarna syftar till att följa upp en misstanke om överskriden befogenhet av en användare. Endast nio beställningar, från en polismyndighet vid samma tillfälle, har gjorts som stickprov och få i realtid.

För att loggning ska bli det centrala verktyg för att upprätthålla integritets-skyddet som förutsätts i förarbetena till PDL, måste loggutvärdering ske frekvent och såväl förebyggande som reaktivt. Nämnden förutsätter att samtliga polismyndigheter kommer att utnyttja möjligheten att begära loggutdrag från CSL i större utsträckning än vad som framgår av det granskade materialet samt att loggutdragen i högre grad kommer att användas även för löpande kontroller utan särskild indikation. Att sådana kontroller sker med viss frekvens – och att användarna är medvetna om detta – är ett viktigt sätt att säkerställa att användare endast tar del av information de behöver för att kunna fullgöra sina arbetsuppgifter och att på så sätt skydda de registre-rades integritet.

I en stor del av de granskade beställningarna är syftet med beställningen mycket kortfattat beskrivet. Enligt Verksamhetsskyddsenheten kompletteras

alltför knapphändigt beskrivna beställningar muntligen. Vad som framkommer vid sådana kompletteringar dokumenteras dock inte i ärendet. Enligt nämndens uppfattning bör muntliga kompletteringar dokumenteras i ärendet hos Verksamhetsskyddsenheten för att möjliggöra en mer ändamålsenlig tillsyn.

7 FORTSATT GRANSKNING

Nämnden avser följa upp polismyndigheternas användning av CSL i kommande projekt.

_____

Säkerhets- och integritetsskyddsnämnden beslutar att delge Rikspolisstyrelsen och polismyndigheterna detta uttalande.