Polisens personuppgiftsbehandling är alltför omfattande och får nu ny kritik från tillsynsmyndigheter.

Polisen får kritik för ▶ OBS-portalen

Datainspektionen har i ett nyligen fattat beslut kritiserat Polismyndighetens behandling av personuppgifter i den s.k. OBS-portalen. I beslutet föreläggs Polismyndigheten att vidta flera förändringar av systemet och i rutinerna avseende personuppgiftsbehandling. OBS-portalen har tidigare kritiserats av Säkerhets- och integritetsskyddsnämnden för att möjliggöra alltför omfattande behandling av känsliga personuppgifter.

Polisens behandling av personuppgifter är föremål för omfattande reglering i flera olika lagar, förordningar och föreskrifter. Anledningen till det omfattande regelverket är inte svår att förstå – personuppgifter om individers misstänkta kriminella aktiviteter får anses vara bland de mest integritetskänsliga uppgifterna som överhuvudtaget kan behandlas. Den övergripande lagstiftningen är polisdatalagen (2010:361) (”PDL”) med tillhörande polisdataförordning (2010:1155), vilka kompletteras av Rikspolisstyrelsens föreskrifter. Vidare finns en mängd så kallade registerförfattningar, det vill säga registerspecifik lagstiftning för enskilda register. Därutöver är också personuppgiftslagen (1998:204) tillämplig, men endast ”subsidiärt” (det vill säga bestämmelserna i annan lagstiftning gäller före bestämmelserna i personuppgiftslagen).

DATAINSPEKTIONEN OCH SÄKERHETS- och integritetsskyddsnämnden (”SIN”) utövar tillsyn över Polismyndighetens personuppgiftsbehandling. Dessa tillsynsmyndigheter har under senare år ägnat stor uppmärksamhet åt Polismyndighetens IT-system, inte minst det system som kallas ”OBS-portalen”. Detta system används för att internt inom polisen sprida brotts-, spanings- och kriminalunderrättels einformation. OBS-portalen har drygt 22 000 användare.

I samband med att Polismyndigheten år 2013 tog OBS-portalen i bruk riktade SIN allvarlig kritik mot den omfattande behandling av känsliga personuppgifter som polisen avsåg att utföra i systemet. Efter en uppföljning år 2015 uttalade SIN att Polismyndigheten trots kritiken inte vidtagit tillräckliga åtgärder för att begränsa personuppgiftsbehandlingen i OBS-portalen.

I ett nyligen fattat beslut från Datainspektionen (dnr 211-2015 daterat 2016-04-18) riktas på nytt omfattande och delvis hård kritik mot OBS-portalen. I beslutet från Datainspektionen lämnas åtta förelägganden och fem rekommendationer på åtgärder som krävs respektive föreslås för att Polismyndighetens personuppgiftsbehandling ska uppfylla tillämpliga lagkrav.

Följande är ett urval av den viktigaste kritiken som Datainspektionen i sitt beslut riktar mot personuppgiftsbehandlingen i OBS-portalen:

POLISENS BEHANDLING ÄR mera omfattande än vad som är nödvändigt utifrån ändamålen med OBS-portalen. En grundprincip för all laglig personuppgiftsbehandling är att varje behandling måste omfattas av angivna och preciserade ändamål samt att eventuell behandling utanför dessa ändamål är förbjuden. Polisdatalagen anger vilka ändamål som är tillåtna för polisens verksamhet (PDL 2 kap 7§). Personuppgiftsbehandlingen i OBS-portalen sker för ändamålet att tillgängliggöra information för att effektivisera brottsbekämpningen. Detta innebär att varje publicering i OBS-portalen i princip måste ha ett brottsbekämpande syfte. Datainspektionen fann i sin granskning emellertid en rad exempel på personuppgifter i systemet som inte har något samband med brott, t.ex. uppgifter om försvunna personer eller om personer som omhändertagits av annan anledning än brott. Enligt Datainspektionen var det inte tillräckligt att, såsom Polismyndigheten hävdade, att uppgifterna kan vara av brottsförebyggande betydelse.

Användarnas behörigheter i systemet är alltför vida. Enligt polisdatalagen är Polismyndigheten skyldig att begränsa tillgången till personuppgifter till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter (PDL 2 kap 11 §). I OBS-portalen är användares behörighet inte knuten till någon geografisk nivå, t.ex. lokal eller regional nivå. Även i övrigt saknas, enligt Datainspektionens uppfattning, lämpliga begränsningar av användarnas behörighet i OBS-portalen. Enkelt uttryckt så medför detta att för många användare ges tillgång till för mycket information och, framförallt, utan en direkt koppling till vad som krävs för att den enskilde tjänstemannen ska kunna utföra sitt arbete.

Information om uppgiftslämnares trovärdighet och uppgifters riktighet saknas. Av polisdatalagen följer att uppgifter i underrättelseverksamhet som ”kan antas ha samband med misstänkt brottslig verksamhet ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak” (PDL 3 kap 4 §). Datainspektionen fann vid sin granskning flera exempel på publiceringar där sådan information saknades. Polismyndighetens invändning om att regelverket skulle vara oklart och kunna tolkas på ett annat sätt godtogs inte av Datainspektionen.

> **”Det är svårt att tänka sig ett IT-system som är mera integritetskänsligt än Polismyndighetens OBS-portal**

RUTINER FÖR BEHANDLING av känsliga personuppgifter saknas. Särskilt strikta lagregler gäller för polisens behandling av känsliga personuppgifter, d.v.s. uppgifter om exempelvis ras, etniskt ursprung, politiska åsikter, religiös uppfattning, hälsa eller sexualliv. Sådana uppgifter får endast behandlas om det är ”absolut nödvändigt för syftet med behandlingen” och då endast som ett komplement till annan information (PDL 2 kap 10 §). I denna del identifierade Datainspektionen inte några omfattande brister när det gäller den faktiska personuppgiftsbehandlingen i OBS-portalen, utan fann endast ”få registreringar” av känsliga personuppgifter. Däremot saknades riktlinjer och rutiner för hur och under vilka omständigheter det kan anses ”absolut nödvändigt” att registrera sådana uppgifter, vilket Polismyndigheten uppmanas att ta fram.

Otillräckliga tekniska spärrar. Ett annat närliggande område som kritiseras av Datainspektionen är att Polismyndigheten inte infört ”tekniska spärrar eller motsvarande funktioner” för att förhindra sökningar på känsliga personuppgifter. Polismyndigheten har istället förlitat sig på en varningsruta som visas i samband med inloggning till OBS-portalen. I denna del valde dock Datainspektionen att rekommendera, snarare än att förelägga, Polismyndigheten att förändra systemet.

Logguppföljning avseende sökningar på känsliga personuppgifter utförs inte. Loggning är ett grundläggande säkerhetskrav vid behandling av personuppgifter för att kunna identifiera ändringar och upptäcka otillåten tillgång till uppgifterna. I OBS-portalen loggas alla sökningar i en central säkerhetslogg. I ett system med så många användare och som behandlar så många personuppgifter krävs dock enligt Datainspektionen (och faktiskt även av Polismyndighetens interna föreskrifter!) regelbundna uppföljningar av systemets loggar. Det bör nämnas att Polismyndigheten delade denna uppfattning och har nu infört logguppföljningar.

DET SKA UNDERSTRYKAS att ovanstående punkter är ett urval av de anmärkningar som Datainspektionen lämnar i det aktuella beslutet. Det finns alltså ytterligare en rad ytterligare områden och frågor där Polismyndighetens användning av OBS-portalen kritiseras av Datainspektionen.

Det är svårt att tänka sig ett IT-system som är mera integritetskänsligt än Polismyndighetens OBS-portal. Det är därför angeläget och positivt att både Datainspektionen och SIN med viss regelbundenhet granskar Polismyndighetens användning av systemet. En fungerande rättsstat måste både möjliggöra en effektiv brottsbekämpning och innehålla en omfattande reglering (med tillsyn) av hur brottsbekämpningen genomförs. Trots den relativt omfattande kritik som Datainspektionen i sitt senaste beslut riktar mot OBS-portalen är ändå min sammantagna – och högst personliga – uppfattning att polisens användning av detta system i huvudsak förefaller relativt korrekt och balanserad. Naturligtvis finns utrymme för förbättringar, vilket Datainspektionens beslut tydligt visar, men det är samtidigt relativt enkelt att föreställa sig hur OBS-portalen skulle kunna (miss)brukas på betydligt värre sätt än vad Datainspektionen lyckats påvisa! ●

DANIEL LUNDQVIST
Daniel Lundqvist är advokat och delägare i Advokatfirman Kahn Pedersen. Daniel är specialiserad på juridik relaterad till integritetsskydd, datasäkerhet och IT-avtal.