Polismyndigheten

Hemställan om översyn av polisens brottsdatalag

Sammanfattning

Polismyndigheten hemställer om en fullständig översyn av polisens brottsdatalag och sammanhörande dataskyddslagstiftning. Vidare bör Polismyndighetens personuppgiftsbehandling som rör nationell säkerhet undantas från brottsdatalagens område och en ändamålsenlig reglering för myndighetens personuppgiftsbehandling på det området införas. Även delar av brottsdatalagen och annan lagstiftning som rör personuppgiftsbehandling kan behöva ses över samtidigt.

Polismyndigheten har de senaste åren getts nya verktyg som ger tillgång till information, t.ex. när det gäller hemlig dataavläsning och preventiva tvångsmedel. Lagstiftning som bryter sekretess och om informationsutbyte är också på gång. Ett tredje och nödvändigt steg för att ge önskad effekt kvarstår, nämligen att ge förutsättningar för myndigheten att också behandla de uppgifter som myndigheten får tillgång till. En utredning som ser över dataskyddsregleringen som rör Polismyndighetens brottsbekämpande verksamhet behöver därför tillsättas så snart som möjligt.

Bakgrund

Förändringar i samhället kräver förändringar av Polismyndighetens arbetssätt

Organiserad brottslighet som bedrivs av bl.a. kriminella nätverk utgör ett allvarligt hot mot det fria och öppna samhället. De senaste åren har den negativa utvecklingen i Sverige accelererat, med stigande nivåer av otrygghet och en kraftig ökning av det dödliga skjutvapenvåldet. Det kriminella klimatet har hårdnat markant med sprängdåd i bostadshus och en ökad gängkriminalitet som blivit vardag. Den kriminella ekonomin är samhällsskadlig då den hotar välfärdssystemet och förtroendet för demokratin. Den allvarliga, organiserade brottsligheten är systemhotande. Till detta kan läggas ett ökat terrorhot gentemot Sverige.

Tillgång till information är avgörande för att Polismyndigheten ska kunna utföra sitt brottsbekämpande uppdrag. Minst lika viktigt är rättsliga förutsättningar att behandla informationen. Det handlar i dag om mycket stora informationsmängder som kommer in till myndigheten och som behöver

hanteras. Brottsligheten är ofta komplex och uppgifter som kommer in i ett sammanhang kan ofta ha samband med uppgifter som redan behandlas inom myndigheten. Såväl underrättelseverksamhet som utredningsverksamhet handlar till stor del om att lägga stora pussel av olika delmängder information. Den inkomna informationen som behöver bearbetas och analyseras består ofta av ostrukturerat, helt obearbetat material.

Polismyndigheten strävar kontinuerligt efter att utveckla sin brottsbekämpande förmåga. Polismyndigheten måste kunna behandla personuppgifter i stora informationsmängder och med modern teknik. För att snabbt kunna hantera stora mängder obearbetat material behöver myndigheten använda sig av olika AI-förmågor.

Myndigheten behöver också kunna hämta in och behandla uppgifter som förekommer i digital miljö, som är en arena för brottsligheten. Med ökad digitalisering och ny teknik öppnas också nya möjligheter för kriminalitet. Kriminella använder i allt större omfattning avancerad teknologi för att utsätta andra människor för brott. Det rör inte bara brott som helt och hållet begås digitalt, utan i princip alla brott har en digital komponent. Tekniken används också för att begå brott eller undvika upptäckt.

Systemhotande brottslighet och nationell säkerhet

I januari 2017 antog regeringen en svensk nationell säkerhetsstrategi. I strategin konstaterade regeringen att säkerhetsfrågorna nu måste ses ur ett betydligt bredare perspektiv än tidigare. Säkerhet för människor i Sverige handlar enligt strategin inte enbart om att rusta sig för att möta militära hot och väpnade angrepp, utan även bl.a. kampen mot terrorism och organiserad brottslighet måste räknas in i det bredare säkerhetsarbetet.

Regeringen har tidigare i år presenterat tre nya nationella strategier för ökad trygghet och säkerhet i Sverige. Det handlar om en strategi för ett stärkt arbete mot våldsbejakande extremism och terrorism, en strategi mot organiserad brottslighet och en strategi med fokus på sociala brottsförebyggande åtgärder.

Den organiserade brottsligheten är systemhotande. Det våldskapital, de finansiella strukturer och de parallella samhällsstrukturer som aktörerna inom organiserad brottslighet har byggt upp i Sverige innebär enligt regeringen både en direkt och indirekt påverkan på människors trygghet och säkerhet, liksom på samhällsviktiga funktioner, vilket framförs t.ex. i regeringens strategi mot organiserad brottslighet (skr. 2023/24:67). Polismyndigheten anser att den organiserade brottsligheten utgör ett minst lika allvarligt hot mot samhället som terrorism, vars bekämpande anses vara en fråga om nationell säkerhet. Samhälls- och systemhotande kriminella nätverk utgör ett betydande hot mot Sverige som stat. Detta innebär enligt Polismyndigheten att det finns brottslighet som myndigheten har i uppdrag att verka mot som rör nationell säkerhet.

Dataskyddsregleringen har inte ändrats i takt med behoven att möta brottsligheten med modern teknik

Polismyndigheten har de senaste åren getts nya verktyg som ger tillgång till information men dataskyddsregleringen har inte förändrats. Förutom att brottsligheten har förändrats i grunden kräver det ständigt ökande informationsinflödet samt behovet att behandla personuppgifter med modern teknik att dataskyddsregleringen anpassas till de nya förhållandena.

Detta är också i enlighet med vad som anges i regeringens strategi mot organiserad brottslighet avseende det mål som inkluderar en effektiv informationsförsörjning. I det arbetet ingår enligt strategin bl.a. att:

- förbättra möjligheterna att inhämta, lagra, utbyta och på andra sätt behandla information
- förbättra tillgången till information i digitala miljöer och
- öka användningen av tekniska hjälpmedel.

Dataskyddsregleringen som gäller för den brottsbekämpande verksamheten har inte ändrats i sak på ett stort antal år. Den s.k. dataskyddsreformen medförde ytterst få ändringar i sak och därmed har den huvudsakliga regleringen varit oförändrad sedan år 2012. Polismyndigheten har i stort liknande problem och begränsningar med gällande lagstiftning som Säkerhetspolisen har lyft i sin hemställan om Säkerhetspolisens informationshantering, och som har lett till en utredning (Ju 2023:02). Begränsningar i dataskyddslagstiftningen som gäller för Polismyndigheten som är omotiverade och inte följer av tvingande EU-regler behöver undanröjas. Utan att Sveriges största brottsbekämpande myndighet har rätt verktyg för utförandet av sitt uppdrag kan inte eskaleringen av våldet och brottsligheten stoppas.

Gällande rätt

EU-rättslig reglering om personuppgiftsbehandling

Vid den s.k. dataskyddsreformen infördes ny dataskyddsreglering på EU-nivå, och det föranledde ett stort antal författningsändringar och nya författningar på nationell nivå.

Det finns två grundläggande rättsakter på dataskyddsområdet på EU-nivå, av vilka den ena är Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), förkortad dataskyddsförordningen. Den andra är Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, förkortad dataskyddsdirektivet. Dataskyddsförordningen gäller inte sådan personuppgiftsbehandling som omfattas av tillämpningsområdet för dataskyddsdirektivet.

Enligt artikel 2.3 a ska dataskyddsdirektivet inte tillämpas på personuppgiftsbehandling som utgör ett led i verksamhet som inte omfattas av unionsrätten. Av skäl 14 framgår att bl.a. verksamhet som rör nationell säkerhet inte omfattas av tillämpningsområdet. Verksamhet som rör nationell säkerhet ligger således utanför både dataskyddsförordningens och dataskyddsdirektivets tillämpningsområde.

Nationell reglering om personuppgiftsbehandling på det brottsbekämpande området

Den grundläggande rättsliga regleringen för personuppgiftsbehandling vid brottsbekämpning är brottsdatalagen (2018:1177), förkortad BDL. För Polismyndighetens del gäller även lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område (polisens brottsdatalag eller PBDL). Den senare lagen innehåller regler som är specifika för Polismyndighetens behandling av personuppgifter i brottsbekämpande syfte. Utöver detta finns bestämmelser som rör personuppgiftsbehandling i flera andra författningar, t.ex. lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen (PNR-lagen) och kamerabevakningslagen (2018:1200), KBL.

Brottsdatalagen genomför dataskyddsdirektivet. I svensk rätt har undantaget i direktivet genomförts i 1 kap. 4 § BDL, enligt vilken lagen inte gäller vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen. Säkerhetspolisens personuppgiftsbehandling regleras i stället i lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter. Regleringen är i vissa avseenden mer tillåtande än den reglering som styr Polismyndighetens personuppgiftsbehandling. Brottsdatalagen gäller inte heller i verksamhet enligt lagen (2021:1171) om behandling av personuppgifter vid Försvarsmakten.

Polisens brottsdatalag trädde i kraft den 1 januari 2019 och ersatte polisdatalagen (2010:361) som hade gällt sedan den 1 mars 2012. Lagen gäller utöver brottsdatalagen. Även om polisens brottsdatalag är relativt ny överfördes de flesta bestämmelserna oförändrade från 2010 års polisdatalag.

Polisens brottsdatalag innehåller särregler som är specifika för främst Polismyndighetens personuppgiftsbehandling, när uppgifter behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet. Vissa bestämmelser ersätter bestämmelser i brottsdatalagen, men lagen innehåller också bestämmelser om undantag från flera av brottsdatalagens bestämmelser.

Av lagstiftningen framgår att behandlingen av personuppgifter ska vara nödvändig för vissa rättsliga grunder, att personuppgifter enbart får behandlas för särskilda, uttryckligt angivna och berättigade ändamål och att känsliga personuppgifter endast får behandlas om de kompletterar annan information och när behandlingen är absolut nödvändig. Varje personuppgift ska bedömas utifrån krav på nödvändighet och uppgiftsminimering i förhållande till de tillåtna rättsliga grunderna och ändamålen.

Polisens brottsdatalag vilar i likhet med dess föregångare polisdatalagen också på en uppdelning av personuppgifter som har gjorts gemensamt tillgängliga och personuppgifter som endast ett fåtal har rätt att ta del av. Det gäller särskilda krav för att få göra uppgifter gemensamt tillgängliga. Vidare ställs högre krav på uppgifter som görs eller har gjorts gemensamt tillgängliga, såsom krav på särskilda upplysningar.

I polisens brottsdatalag finns fastslagna yttersta tidsgränser för behandling av personuppgifter, som varierar bl.a. beroende på i vilket sammanhang som personuppgifterna behandlas.

Förslag till översyn

Polismyndigheten hemställer om en fullständig översyn av polisens brottsdatalag och därmed sammanhängande reglering. Dagens dataskyddsreglering är inte anpassad efter de behov som finns att hantera information och begränsar på ett betydande sätt Polismyndighetens förmåga att utöva sitt uppdrag. Begränsningar som inte är tvingande eller motiverade bör tas bort.

En väsentlig del av gällande dataskyddslagstiftning är inte en direkt följd av lagstiftning på EU-nivå, utan är resultatet av nationella överväganden. Det finns således utrymme att göra förändringar inom ramen för en nationell översyn, utan att det kräver förändringar på EU-nivå.

Minskad detaljreglering och ökad möjlighet till bedömningar på generell nivå

Polisens brottsdatalag innehåller ett stort antal bestämmelser som är mycket detaljerade och anpassade till specifika situationer. Många av bestämmelserna orsakar tillämpningssvårigheter hos myndigheten och fördröjer eller försvårar behandlingen av personuppgifter på ett negativt sätt, inte bara för Polismyndighetens brottsbekämpande uppdrag utan även för den personliga integriteten. Detaljnivån i sig medför att det ofta uppstår situationer som inte passar in i de specifika bestämmelserna, eller att behandling som är tillåten enligt kraven på rättslig grund och närmare ändamål ändå är svår att utföra. Även om bestämmelserna har utformats med integritetsaspekten som en tungt vägande faktor kan det därför ifrågasättas om en så ingående detaljreglering verkligen skyddar på avsett sätt. I brottsdatalagen finns reglering som enligt Polismyndighetens mening i många fall medför ett tillräckligt skydd för den personliga integriteten.

Regleringen motsvarar inte de faktiska behoven i fråga om hur Polismyndigheten behöver behandla personuppgifter för att kunna fullgöra sitt brottsbekämpande uppdrag. En stor del av Polismyndighetens arbete i dag handlar om att analysera större informationsmängder. Vid sådan verksamhet är det ofta mycket svårt att motivera varje enskild behandling av personuppgifter, medan det kan motiveras på en mer generell eller aggregerad nivå. Lagstiftningen är dock så formulerad och detaljerad att den synes kräva en motivering av varje personuppgift som behandlas. Det är av avgörande betydelse att myndigheten kan göra bedömningar av tillåten personuppgiftsbehandling på en mer aggregerad eller generell nivå än på individ-/enskild uppgiftsnivå

eller i det enskilda fallet. Polisens brottsdatalag behöver därmed minskas i sin detaljrikedom och ge tydligare utrymme till bedömningar på en högre nivå än för varje enskild personuppgift.

Det måste vara möjligt för myndigheten att behandla stora mängder personuppgifter med modern teknik. Detta är också i linje med regeringens inriktning i ovan nämnda strategi mot organiserad brottslighet. I strategin lyfts att mängden data ökar, att det är nödvändigt att myndigheterna kan hålla jämna steg med utvecklingen och att en ändamålsenlig informationsförsörjning förutsätter att myndigheterna kan inhämta information från digitala miljöer eftersom dessa är en viktig arena för brottslighet. Polismyndigheten instämmer helt i dessa slutsatser.

Tekniska/digitala verktyg är avgörande för att kunna analysera stora mängder data och effektivisera brottsbekämpningen. Detta innefattar bl.a. användningen av s.k. AI-förmågor. Dagens detaljreglering som tar sikte på varje enskild personuppgift är svår att uppfylla i praktiken, men den är inte heller anpassad för utvecklingsarbete. För mer om utvecklingsarbete, se särskild rubrik nedan.

Även regeringen vidgår att utveckling och användning av digitala verktyg, exempelvis artificiell intelligens, är av stor betydelse för myndigheters förmåga att bekämpa organiserad brottslighet. I strategin mot organiserad brottslighet nämns att det inte bara handlar om att använda digitala verktyg för att utreda vissa typer av brott och för att säkerställa allmän ordning och säkerhet. Det handlar också om att kunna identifiera, hantera, sortera och dra slutsatser utifrån datamängder i alla typer av informationshantering i såväl brottsförebyggande som brottsutredande syfte. Vid sidan av att myndigheterna själva kan dra fördel av artificiell intelligens är det viktigt att förebygga och motverka att utvecklingen av AI-tjänster används för kriminella ändamål. Teknikutvecklingen behöver följas för att ge förståelse för vilka sårbarheter som kan utnyttjas för brottslighet i framtiden.

I regeringens strategi mot våldsbejakande extremism och terrorism (skr. 2023/24:56) anges bl.a. att myndigheterna behöver ha möjlighet att samla in och utbyta information och använda sig av ny teknik för att t.ex. skanna stora mängder av digital information.

Dagens reglering försvårar kraftigt möjligheten att bearbeta stora mängder material på ett ändamålsenligt sätt. Det innebär också att personuppgifter ofta behöver behandlas under en längre tid, i väntan på att kunna bearbetas och analyseras – och därmed också kunna avfärdas som inte nödvändiga.

Det kan finnas skäl att samtidigt beakta att den nyligen antagna AI-förordningen medför särskilda krav vid användning av AI-system, inklusive krav på bedömningar avseende grundläggande rättigheter, se Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

Den brottsliga verksamheten sträcker sig över många olika brottstyper. Behoven av förändringar i polisens brottsdatalag som belyses i denna hemställan gäller inte bara bekämpning av grov brottslighet utan också bekämpningen av mindre allvarlig brottslighet och s.k. mängdbrottslighet, som också orsakar stort lidande. Mindre kvalificerad brottslighet är också ofta en länk i allvarlig grov organiserad brottslighet.

Gemensamt tillgängliga uppgifter – slopad reglering

I polisens brottsdatalag finns detaljerad reglering om i vilka situationer som personuppgifter får göras gemensamt tillgängliga och särskilda krav på behandlingen som då gäller, såsom krav på särskilda upplysningar, sökbegränsningar m.m. (3 kap. PBDL). Bestämmelserna om längsta tid för behandling (4 kap.) är också kopplade till om uppgifter anses gemensamt tillgängliga eller inte. Regleringen om gemensamt tillgängliga uppgifter medför att uppgifter vars behandling har rättslig grund och godtagbara ändamål i många fall ändå inte får användas gemensamt i verksamheten. För vissa informationstyper, såsom stora mängder inkommet material, är upplysningskraven t.ex. ofta varken tekniskt eller praktiskt möjliga att uppfylla. Därmed förhindras Polismyndigheten att behandla personuppgifter som myndigheten har tillgång till. Då brottsdatalagen innehåller bestämmelser till skydd för den personliga integriteten kan skälen för dessa begränsningar ifrågasättas.

Vidare medför detaljregleringen många oklarheter, som innebär onödiga begränsningar vid den fortsatta behandlingen av personuppgifter som har gjorts gemensamt tillgängliga. Som exempel kan nämnas att de upplysningskrav som gäller för gemensamt tillgängliga uppgifter kan variera beroende på enligt vilken grund som uppgifter har gjorts gemensamt tillgängliga. Vid byte av ändamål för vilka personuppgifter behandlas uppstår ofta oklarheter i fråga om vilka upplysningskrav som då gäller.

Den EU-reglering som nu aktuella författningar vilar på, dataskyddsdirektivet, innehåller ingen distinktion mellan gemensamt och ej gemensamt tillgängliga uppgifter eller reglering om detta. Nu aktuell reglering är resultatet av överväganden på nationell nivå.

Polismyndigheten har gett in en hemställan till regeringen om ändringar i 3 kap. PBDL (dnr A286.201/2024). Förslagen syftar till att undanröja vissa av hindren i regleringen på kort sikt, men förtar inte behovet av en total översyn. Befintlig reglering i brottsdatalagen bör i många fall kunna vara tillräcklig. Regleringen i polisens brottsdatalag om gemensamt tillgängliga uppgifter bör därför utgå helt.

Längsta tid för behandling – större flexibilitet

Enligt brottsdatalagen gäller att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Denna bestämmelse gäller alltid.

I polisens brottsdatalag och i tillhörande förordning regleras yttersta tidsramar för behandling av personuppgifter. Bestämmelserna är omfattande både

till antal och innehåll och tar sikte på varje enskild personuppgift. Regleringen gör också skillnad på om personuppgifter behandlas i ett ärende eller inte, enligt vilken grund som personuppgifter har gjorts gemensamt tillgängliga och i vilket sammanhang som personuppgifter behandlas. Det är inte möjligt för en myndighet av Polismyndighetens storlek och med den informationsmängd myndigheten har tillgång till att som standard göra bedömningar av behandlingen i det enskilda fallet, detta även om myndighetens it-stöd är avancerade och förfinade. Att kunna motivera varje enskild personuppgifts förenlighet med regleringen i 4 kap. PBDL är en praktisk omöjlighet. Vidare behandlas personuppgifter ofta för flera olika ändamål samtidigt, vilket gör tillämpningen av nämnda reglering mycket svår.

Regleringen om längsta tid för behandling av personuppgifter behöver ses över för att möjliggöra bedömningar på mer aggregerad nivå och tillåta olika lösningar. Med nuvarande ordning löper Polismyndigheten risken vid mycket stora uppgiftssamlingar att behöva radera information innan den har hunnit bearbetas och tas om hand. Detta leder till att Polismyndighetens möjligheter att fullgöra sitt uppdrag försämras, inte minst i förhållande till att förebygga, förhindra och upptäcka brottslig verksamhet. Behovet av distinktionen mellan uppgifter som behandlas i ett ärende och inte kan behöva ses över i detta sammanhang.

Behovet och lämpligheten i att alls slå fast längsta tider för behandling i lag kan också ifrågasättas. Jfr också SOU 2023:100, vari bedöms att fastslagna tidsfrister inte bör finnas i de flesta författningar som reglerar de aktuella myndigheternas personuppgiftsbehandling, utan att det är något som myndigheterna själva måste avgöra.

Skarp data vid utveckling och uppföljning – tydliggöranden

Sedan länge har gällt att genomförande av planering, uppföljning och utvärdering av verksamhet inte kräver något särskilt stöd i registerförfattningar, tidigare kallat outtalat primärändamål. Personuppgiftsbehandling för sådana syften är således tillåten även utan uttrycklig reglering (se t.ex. prop. 2017/18:232 s. 118 och 119). Jfr också uttalanden i SOU 2023:100 s. 514 och 515, där utredningen bedömer att utveckling av nya digitala arbetssätt genom tester m.m. utgör en integrerad del av myndigheternas verksamhet och sådan behandling självklart ingår i de föreslagna ändamålsbestämmelserna.

Även om det är positivt att sådan behandling är tillåten uppstår ofta svåra bedömningar i fråga om vilken rättslig grund och närmare ändamål som behandling av s.k. skarp data i bl.a. utvecklings- eller uppföljningssyfte har. Ibland uppkommer fråga om behandlingen faller under brottsdatalagens eller dataskyddsförordningens tillämpningsområde. Även i de fall den gränsdragningen inte är svår att göra, uppstår ofta oklarheter om vad som gäller i fråga om förutsättningarna för gemensamt tillgängliggörande, upplysningskrav och inte minst längsta tid för behandling för sådana uppgifter. Det finns behov av förtydliganden av de närmare rättsliga förutsättningarna när det gäller denna slags behandling.

Behandling för viss verkställighet – anpassad reglering

Det förekommer också behandling av personuppgifter inom Polismyndigheten som faller inom brottsdatalagens tillämpningsområde utan att det finns reglering om det i polisens brottsdatalag. Som exempel kan nämnas Polismyndighetens verksamhet enligt 3 § utlänningsdatalagen (2016:27) som anses falla under brottsdatalagens tillämpningsområde om behandlingen sker för något av de syften som anges i 1 kap. 2 § BDL. Eftersom utvisning är en särskild rättsverkan av brott, som innebär att en straffrättslig påföljd verkställs, bedöms Polismyndighetens behandling av personuppgifter vid utvisning på grund av brott falla under brottsdatalagens tillämpningsområde (se prop. 2017/18:254 s. 24 och 25). Detta område regleras dock inte alls i polisens brottsdatalag. Detta medför otydligheter när det gäller hur personuppgifter får behandlas i dessa ärenden. Vid en översyn av polisens brottsdatalag bör frågan om behov av ändamålsenliga bestämmelser för sådan personuppgiftsbehandling analyseras.

Nationell säkerhet – undantag från brottsdatalagen och ändamålsenlig reglering

När det rör nationell säkerhet styrs dataskyddsregelverket inte av EU:s dataskyddsreglering. Brottsdatalagen har dock gjorts tillämplig på det området med undantag för Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. Även Polismyndighetens behandling av personuppgifter när myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen är undantagen. Undantag gäller också för viss verksamhet som Försvarsmakten utför.

Detta innebär att brottsdatalagen gäller för Polismyndighetens behandling av personuppgifter, även om det rör nationell säkerhet (förutom då Polismyndigheten övertagit en arbetsuppgift från Säkerhetspolisen). I förarbetena till brottsdatalagen uttalade regeringen att det inte bör göras ett generellt undantag för nationell säkerhet från brottsdatalagens tillämpningsområde och att det inte heller finns skäl att undanta ”den mycket begränsade personuppgiftsbehandling som rör nationell säkerhet” i bl.a. Polismyndighetens verksamhet (prop. 2017/18:232 s. 103 och 104). Som framgår av denna hemställan stämmer inte längre detta påstående. Polismyndigheten utför brottsbekämpande verksamhet som rör nationell säkerhet, varvid också personuppgifter behandlas.

Polismyndigheten har i stort liknande problem och begränsningar med gällande lagstiftning som Säkerhetspolisen har lyft i sin hemställan om Säkerhetspolisens informationshantering. Den utredning som nämns ovan (Ju 2023:02) avser de bestämmelser som reglerar Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet. Polismyndigheten har verkat för att den utredningen även ska omfatta Polismyndighetens personuppgiftsbehandling på området men har inte fått gehör för detta.

När det gäller våldsbejakande extremism och terrorism lyfts i regeringens strategi mot detta (skr. 2023/24:56) bl.a. att de brottsbekämpande myndigheterna behöver ha ändamålsenliga, rättssäkra och effektiva verktyg för att kunna förhindra hatbrott, ideologiskt motiverad brottslighet, våldsbejakande

extremism och terrorism. En anpassad lagstiftning måste enligt Polismyndigheten anses vara ett grundläggande, nödvändigt verktyg.

Polismyndighetens behandling av personuppgifter som rör nationell säkerhet bör därför, i likhet med vad som gäller för Säkerhetspolisen, vara undantagen från brottsdatalagens tillämpningsområde. Det behövs också en ändamålsenlig reglering för personuppgiftsbehandlingen som möjliggör för myndigheten att bl.a. få tillgång till och hantera information på detta område. Härigenom kan regleringen anpassas efter de särskilda behov som finns när det gäller att skydda nationell säkerhet.

Känsliga personuppgifter – större flexibilitet

När det gäller känsliga personuppgifter gäller både ett förbud mot att, som huvudregel, behandla sådana uppgifter och att utföra sökningar som avser känsliga personuppgifter. I polisens brottsdatalag finns reglering som under vissa förutsättningar möjliggör sökbegrepp och sökningar trots sökförbudet i brottsdatalagen. Det finns också särreglering om behandling av biometriska och genetiska uppgifter.

Särskilt när det gäller stora informationsmängder kan svårigheter uppstå med att uppfylla samtliga krav i brottsdatalagen och polisens brottsdatalag, så som de är utformade i dag. Det handlar främst om att behandlingen behöver motiveras för varje enskild personuppgift, se under tidigare rubrik. Då det finns ett stort antal andra skyddsåtgärder i både dataskyddsregleringen och genom myndighetens rutiner kan det ifrågasättas om samtliga de nationella regler som begränsar möjligheten till sökning fortsatt är nödvändiga och befogade. I dataskyddsdirektivet finns inget förbud mot att använda känsliga personuppgifter vid sökning.

Regleringen medför problem inte enbart gällande stora uppgiftsmängder. Ett exempel där gränsdragningsproblem uppkommer i fråga om möjligheten att behandla personuppgifter är när uppgiftslämnare använder begrepp som kan utgöra känsliga personuppgifter. Av rättssäkerhetsskäl finns det ofta behov att återge en källas information ordagrant, för att inte riskera förvanska informationen, t.ex. genom att polisanställda lägger på egna värderingar vid den tidpunkten som information från en källa ska dokumenteras. Möjligheten att behandla känsliga personuppgifter när det gäller uppgifter som kommer från källor bör säkerställas.

Vid en översyn av regleringen som rör känsliga personuppgifter bör samtidigt behoven för fler delar inom Polismyndigheten att behandla genetiska uppgifter samtidigt ses över, varvid även innebörden av genetiska uppgifter kan behöva klargöras.

Dataskyddsregleringens förhållande till annan reglering och dess räckvidd – klargöranden

Även om rättslig grund för inhämtning av personuppgifter finns uppstår ofta oklarheter i fråga om hur Polismyndigheten kan använda information utöver det ändamål för vilket den samlats in, när inhämtning sker med stöd av särskild lagstiftning. Fortsatt behandling av personuppgifter som hämtas in med

stöd av kamerabevakningslagen kan t.ex. medföra komplicerade bedömningar, då kameraregleringen om inhämtningen inte tydligt förhåller sig till dataskyddsreglerna om hur personuppgifter får behandlas, t.ex. gemensamt tillgängliggörande, behandling för flera ändamål eller längsta tid för behandling. Detsamma kan sägas gälla för inhämtning med stöd av rättegångsbalkens regler. Vid en översyn finns det därför skäl att se över dataskyddsregleringens förhållande till annan reglering, om inte detta omhändertas i andra, redan pågående lagstiftningsärenden.

En annan fråga gäller brottsdatalagens och polisens brottsdatalags räckvidd när det gäller personuppgifter som finns utanför myndighetens rådighet, t.ex. sådana som finns på internet eller finns offentliggjorda av andra på andra tillgängliga ytor utanför myndighetssfären, men som myndigheten har tillgång till. Den äldre polisdatalagen (1998:622) gällde utöver personuppgiftslagen (1998:204) och det framgår av förarbeten till den äldre polisdatalagen att det som avsågs särregleras i förhållande till personuppgiftslagen var personuppgiftsbehandlingen i polisens egna register. Vad som gäller för dagens reglering är inte lika tydligt då det saknas förarbetsuttalanden om detta. Det finns situationer då bestämmelser i brottsdatalagen eller polisens brottsdatalag, trots att de enligt sin ordalydelse synes vara tillämpliga, inte ska eller kan tillämpas. Vid en översyn av dataskyddsregleringen efterfrågas klargöranden i dessa frågor.

Konsekvenser

Förändringarna syftar till att förbättra Polismyndighetens förutsättningar att bedriva sin brottsbekämpande verksamhet. Minskad brottslighet och ökad lagföring leder till större trygghet för samhället och dess invånare.

De förslag som läggs fram av en kommande utredning behöver vara proportionerliga och i övrigt i enlighet med dataskyddsrättsliga principer. Att fler brott kan utredas och lagföras, och brottslig verksamhet kan förebyggas, förhindras och upptäckas är till fördel för enskildas personliga integritet.

Genom förändringarna förväntas Polismyndighetens brottsbekämpande arbete och administration effektiviseras och medföra minskade kostnader för personal och administration. Resurser kan fördelas mer effektivt. It-stöd kommer att behöva anpassas till förändringarna, vilket dock är ett syfte med förändringarna. Minskad detaljreglering förväntas dock medföra färre krav på funktioner i it-stöden.

Om förändringarna inte genomförs kommer Polismyndigheten fortsatt inte kunna behandla information på ett effektivt och ändamålsenligt sätt. Brottslig verksamhet kan komma att fortgå och brott kan komma att begås trots att det kan finnas, eller skulle kunna inhämtas, information inom myndigheten som skulle kunna förhindra detta. Fullgörandet av de uppdrag som Polismyndigheten är ålagd av riksdag och regeringen försvåras och målen i regeringens strategier på området blir svårare att uppnå. Effekten av myndighetens brottsbekämpande insatser begränsas.

De verktyg som Polismyndigheten har getts hittills på t.ex. tvångsmedels- och informationsutbytesområdet kommer inte att ge effekt, om inte även nu aktuella förändringar genomförs.

Personuppgifter som inte har relevans kan komma att ligga obearbetade, därför att det saknas rättsliga förutsättningar att analysera dem på ett effektivt sätt. Personuppgifter kan också fortsatt behöva tas bort och värdefull information gå förlorad, trots att behov av uppgifterna finns.

Denna hemställan har beslutats av rikspolischefen Petra Lundh efter föredragning av rättsliga experten Leena Mildenberger. I den slutliga beredningen har rättschefen Gunilla Hedwall deltagit.

POLISMYNDIGHETEN

Petra Lundh

Leena Mildenberger