



Kommittédirektiv

Polismyndighetens behandling av personuppgifter

Beslut vid regeringssammanträde den 12 mars 2026

Sammanfattning

För att stå väl rustad i det brottsbekämpande arbetet behöver Polismyndigheten moderna och effektiva regler som är anpassade efter samhälls- och teknikutvecklingen. En särskild utredare ska därför göra en översyn av de bestämmelser som reglerar myndighetens behandling av personuppgifter inom brottsdatalagens område och föreslå författningsändringar. Syftet är att säkerställa att Polismyndigheten har möjligheter att behandla personuppgifter på ett så effektivt sätt som möjligt samtidigt som skyddet för enskildas personliga integritet och andra grundläggande fri- och rättigheter säkerställs.

Utredaren ska bl.a.

- undersöka och bedöma i vilken utsträckning dagens regelverk för behandling av personuppgifter på brottsdatalagens område försvårar en effektiv informationshantering i Polismyndighetens verksamhet,
- lämna förslag på hur personuppgifter kan behandlas av Polismyndigheten på ett mer ändamålsenligt sätt än i dag, och
- lämna nödvändiga författningsförslag.

Uppdraget ska redovisas senast den 13 september 2027.

Varför behövs det en utredning?

Teknik- och samhällsutvecklingen kräver nya åtgärder

Till Polismyndighetens uppgifter hör bl.a. att förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten samt att utreda och beivra brott. Kriminaliteten, inte minst den organiserade brottsligheten, har över tid blivit alltmer komplex och samhällsskadlig. Det ställer nya krav på Polismyndighetens förmåga. Den organiserade brottslighetens gränsöverskridande karaktär innebär också att bekämpningen av brottsligheten måste bedrivas gemensamt med andra myndigheter och med andra stater.

Tillgång till information är avgörande för att Polismyndigheten ska kunna utföra sitt brottsbekämpande uppdrag. För att informationen ska kunna göra nytta i verksamheten behöver det också finnas rättsliga förutsättningar att behandla den. Digitaliseringen och den tekniska utvecklingen har förändrat samhället i grunden. Förändringen har inneburit att det produceras enorma mängder information, och allt större mängder behöver hanteras inom myndigheten. Uppgifter som kommer in i ett sammanhang kan ofta ha samband med uppgifter som redan behandlas inom myndigheten i ett annat sammanhang. Såväl underrättelseverksamhet som utredningsverksamhet handlar till stor del om att lägga stora pussel av olika delmängder information. Den information som kommer in består ofta av ostrukturerat, helt obearbetat material och behöver därför bearbetas och analyseras.

Digitalisering och teknikutveckling har också bidragit till nya möjligheter för den organiserade brottsligheten. Nya digitala plattformar ger förbättrade förutsättningar för kommunikation och möjligheter att hitta och påverka andra, t.ex. för att rekrytera unga in i 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 undvika upptäckt.

De möjligheter som teknikutvecklingen innebär behöver tas tillvara också i Polismyndighetens arbete. För att lösa uppdraget behöver myndigheten ha tillgång till relevant information och på ett effektivt sätt kunna hantera och bearbeta de stora informationsmängderna, exempelvis genom att använda modern teknik. Detta ställer nya krav på Polismyndighetens arbetsmetoder

och på den lagstiftning som reglerar myndighetens informationshantering. För att snabbt kunna hantera stora mängder obearbetat material behöver myndigheten använda sig av exempelvis AI-hjälpmiddel. Till skillnad mot tidigare finns det i dag effektiv programvara som kan automatisera informationshanteringen och generera snabbare och mer träffsäkra resultat. Sådan programvara kan exempelvis göra en initial granskning av stora datamängder och flagga upp information som sannolikt är relevant. En manuell granskning behöver då endast göras av en mindre mängd information som har mer direkt relevans för Polismyndighetens uppdrag.

Dagens regelverk behöver ses över

EU:s dataskyddsdirektiv ((EU) 2016/680) gäller behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott, verkställa straffrättsliga påföljder eller skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Direktivet har i svensk rätt i huvudsak genomförts genom brottsdatalagen (2018:1177), som trädde i kraft den 1 augusti 2018. För Polismyndighetens del kompletteras brottsdatalagen bl.a. av lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område (polisens brottsdatalag).

Regleringen av Polismyndighetens personuppgiftshantering fanns tidigare i den numera upphävda polisdatalagen (2010:361). Många av bestämmelserna togs i princip oförändrade in i brottsdatalagen och polisens brottsdatalag och har därför inte fullt ut anpassats till de behov som Polismyndigheten har i dag. Det innebär att stora delar av det regelverk som påverkar möjligheterna att behandla personuppgifter kommer från en tid då inte bara brottsligheten utan också de tekniska möjligheterna att behandla personuppgifter var annorlunda mot i dag. Regelverket är alltså inte anpassat till dagens förhållanden.

Polismyndigheten har de senaste åren fått nya verktyg som ger tillgång till mer information, t.ex. utökade möjligheter att använda hemliga och preventiva tvångsmedel. En ny sekretessbrytande uppgiftsskyldighet som syftar till att öka informationsflödet till bl.a. Polismyndigheten och en ny generell sekretessbrytande bestämmelse trädde i kraft under förra året (prop. 2024/25:65 och prop. 2024/25:180). Vidare står det klart att den tekniska utvecklingen har inneburit att det produceras enorma mängder information och att det samtidigt har skapats nya möjligheter för Polismyndigheten att med hjälp av automatiserade processer behandla personuppgifter på ett

annat sätt än tidigare. Det finns dock enligt nuvarande regelverk tydliga begränsningar för Polismyndighetens möjligheter att behandla personuppgifter, t.ex. med hjälp av tekniska hjälpmedel. En del av de gällande reglerna 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.

Begränsningar i dataskyddslagstiftningen som är omotiverade och inte följer av tvingande EU-regler behöver undanröjas för att Polismyndigheten ska kunna lösa sitt uppdrag på ett effektivt och framgångsrikt sätt. Polismyndigheten varnar för att effekten av myndighetens brottsbekämpande insatser annars begränsas och att eskaleringen av våldet och brottsligheten inte kan stoppas. (Polismyndighetens hemställan om översyn av polisens brottsdatalog, Ju2024/02401).

Att förbättra myndigheternas möjligheter att inhämta, lagra, utbyta och på andra sätt behandla information på ett ändamålsenligt, rättssäkert och effektivt sätt är också ett av de uttalade målen i regeringens strategi mot den organiserade brottsligheten (skr. 2023/24:67). Sammantaget finns det starka skäl för en översyn av den reglering som styr Polismyndighetens behandling av personuppgifter.

Uppdraget att se över Polismyndighetens personuppgiftsreglering i syfte att skapa moderna och effektiva regler

Vissa begränsningar som det nuvarande regelverket medför

Detaljreglering försvårar behandlingen

Av 2 kap. 1 § polisens brottsdatalog framgår att personuppgifter får behandlas om det är nödvändigt för att myndigheten ska kunna utföra vissa uppgifter som räknas upp i paragrafen. Uppgifterna korresponderar i stort med 2 § polislagen (1984:387) som anger Polismyndighetens huvudsakliga uppgifter, bl.a. att förebygga, förhindra eller upptäcka brottslig verksamhet samt att utreda och beivra brott. Nödvändighetsrekvisitet innebär i detta sammanhang att personuppgiftsbehandlingen ska behövas för att uppgiften ska gå att fullgöra på ett effektivt sätt (prop. 2017/18:232 s. 440). Känsliga personuppgifter får som huvudregel inte behandlas, men uppgifter som behandlas får kompletteras med känsliga personuppgifter om det är absolut

nödvändigt (2 kap. 11 § brottsdatalogen). Polismyndigheten får bara behandla personuppgifter för särskilda, uttryckligt angivna och berättigade ändamål (2 kap. 3 § brottsdatalogen). Att ändamålet ska vara särskilt innebär att det måste vara tillräckligt preciserat för att det ska kunna avgöras om de personuppgifter som behandlas är adekvata och relevanta för ändamålet med behandlingen eller om för många personuppgifter behandlas. Att ändamålen ska vara berättigade innebär en koppling till den rättsliga grunden. Personuppgifter får således inte behandlas för ett ändamål som inte är berättigat i förhållande till den tillämpliga rättsliga grunden.

Polisens brottsdatalog innehåller ett stort antal bestämmelser som är mycket detaljerade och anpassade till specifika situationer. Många av bestämmelserna orsakar enligt Polismyndigheten tillämpningssvårigheter 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. En stor del av Polismyndighetens arbete i dag handlar om att analysera större informationsmängder. Vid sådan verksamhet kan det vara mycket svårt att motivera behandlingen av varje enskild personuppgift, medan behandlingen kan motiveras på en mer generell eller aggregerad nivå. Lagstiftningen är dock så formulerad och detaljerad att Polismyndigheten anser att det krävs en motivering för varje personuppgift som behandlas. Det är av avgörande betydelse för myndigheten att kunna göra bedömningar av tillåten personuppgiftsbehandling på en mer aggregerad eller generell nivå.

Detaljrikedomen i den nuvarande regleringen försvårar alltså en effektiv informationshantering och det behövs tydligare utrymme för bedömningar på en högre nivå än för varje enskild personuppgift.

Detaljregleringen begränsar användningen av tekniska hjälpmedel

I regeringens strategi mot den organiserade brottsligheten framgår att utveckling och användning av digitala verktyg kommer att vara av stor betydelse för myndigheters förmåga att bekämpa organiserad brottslighet. Det handlar inte bara 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.

Dagens detaljreglering som tar sikte på varje enskild personuppgift är inte fullt ut anpassad efter användningen av tekniska hjälpmedel. Regleringen försvårar enligt Polismyndigheten kraftigt möjligheten att bearbeta stora mängder material med tekniska hjälpmedel på ett ändamålsenligt sätt. Den innebär också att personuppgifter ofta behöver behandlas under en längre tid, i väntan på att kunna bearbetas och analyseras – och därmed också på att kunna avfärdas som inte nödvändiga.

Reglerna om gemensamt tillgängliga uppgifter begränsar möjligheterna att behandla uppgifter inom Polismyndigheten

I polisens brottsdatalog görs en uppdelning mellan personuppgifter som har gjorts gemensamt tillgängliga och personuppgifter som endast ett fåtal har rätt att ta del av (3 kap. 1 §). Bestämmelserna, som inte bygger på EU-rätt, har motiverats med att risken för otilbörliga intrång i den personliga integriteten får anses större när personuppgifter används av flera tjänstemän gemensamt i verksamheten, än när personuppgifter behandlas av endast en eller ett fåtal tjänstemän (se prop. 2009/10:85 s. 68 och 125). Av 3 kap. 2 § polisens brottsdatalog följer att enbart vissa personuppgifter får göras gemensamt tillgängliga. När en uppgift har gjorts gemensamt tillgänglig finns det krav på att i vissa fall genom en särskild upplysning eller på något annat sätt lämna information i anslutning till uppgiften (3 kap. 3 och 4 §§). Det finns också vissa begränsningar kring vilka uppgifter som får tas fram vid sökningar i automatiserade behandlingssystem, om uppgifterna har gjorts gemensamt tillgängliga (3 kap. 5 och 6 §§). Bestämmelserna om längsta tid för behandling (4 kap. polisens brottsdatalog) är också kopplade till om uppgifter anses gemensamt tillgängliga eller inte.

Regleringen om gemensamt tillgängliga uppgifter medför att uppgifter i många fall, trots att det finns rättslig grund och godtagbara ändamål, inte får användas gemensamt i verksamheten. Detaljregleringen medför också att det kan uppstå oklarheter. Upplysningskraven som gäller för gemensamt tillgängliga uppgifter varierar t.ex. beroende på enligt vilken grund uppgifterna har gjorts gemensamt tillgängliga.

Regeringen har nyligen beslutat propositionen Ökade möjligheter att dela uppgifter inom Polismyndigheten. Förslagen i propositionen – som bl.a. innebär att uppgifter som endast en särskilt avgränsad krets personer har rätt att ta del av inte anses som gemensamt tillgängliga – syftar till att undanröja vissa av hindren i regleringen på kort sikt, men löser inte alla problem med

regelverket om gemensamt tillgängliga uppgifter. Det regelverket kom till efter överväganden på nationell nivå i en tid då Polismyndighetens organisation och verksamhet såg annorlunda ut än i dag. Det finns därför anledning att överväga om reglerna har spelat ut sin roll.

Reglerna om längsta tid för behandling innebär en risk för att viktiga uppgifter raderas

Enligt brottsdatalagen gäller att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Bestämmelsen gäller generellt. I 4 kap. polisens brottsdatalag och i tillhörande förordning finns bestämmelser om den längsta tid som personuppgifter får behandlas i olika situationer. Syftet med bestämmelserna är att skydda den personliga integriteten. Regelverket är komplext och gör 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.

Att motivera varje enskild personuppgifts förenlighet med regleringen i 4 kap. polisens brottsdatalag är enligt Polismyndigheten en praktisk omöjlighet. Vidare behandlas personuppgifter ofta för flera olika ändamål samtidigt, vilket gör tillämpningen av nämnda reglering mycket svår. Med nuvarande ordning finns risk att Polismyndigheten behöver radera information innan den har hunnit bearbetas och tas om hand, om det t.ex. rör sig om mycket stora uppgiftssamlingar. Detta leder till att Polismyndighetens möjligheter att fullgöra sitt uppdrag på ett effektivt sätt försämras, inte minst i underrättelseverksamheten.

I 5 kap. polisens brottsdatalag finns bestämmelser om den längsta tid som personuppgifter får behandlas i vissa av Polismyndighetens register, bl.a. biometriregistren. I registren sparas bl.a. dna-profiler och fingeravtryck. Uppgifterna i biometriregistret över dömda får t.ex. inte behandlas längre tid än tre månader efter det att uppgifterna om det avgörande som ligger till grund för registreringen gallrats från belastningsregistret. Det framstår inte som självklart att längsta tid för behandling av biometriska uppgifter om dömda – som är ett mycket effektivt medel för att upptäcka en gärningsman som återfaller i brott, även efter mycket lång tid – alltid ska vara kopplad till gallringen av belastningsregistret. Det finns mot den bakgrunden anledning att överväga om lagringstiderna i vissa fall bör förlängas, särskilt vid allvarlig

brottslighet, i syfte att säkerställa att sådan brottslighet kan förebyggas, förhindras och utredas på ett effektivt sätt.

Förbudet mot att behandla känsliga personuppgifter kan innebära svårigheter

När det gäller känsliga personuppgifter gäller både ett förbud mot att, som huvudregel, behandla sådana uppgifter och att utföra sökningar i syfte att få fram ett urval av personer grundat på sådana uppgifter (2 kap. 11, 12 och 14 §§ brottsdatalagen). I polisens brottsdatalag finns bestämmelser som under vissa förutsättningar medger sökningar trots sökförbudet i brottsdatalagen (2 kap. 5 och 6 §§ polisens brottsdatalag). 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. Regleringen medför problem även i andra sammanhang. Uppgiftslämnare kan t.ex. använda begrepp som utgör känsliga personuppgifter. Av rättssäkerhetsskäl finns det ofta behov av att återge en källas information ordagrant, för att inte riskera att förvanska informationen.

Genetiska uppgifter betraktas som känsliga personuppgifter och avser personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen. Genetiska uppgifter får behandlas endast om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen (2 kap. 12 § brottsdatalagen). Inom Polismyndigheten är det bara Nationellt forensiskt centrum som under vissa förutsättningar har stöd för att behandla sådana uppgifter (6 kap. 4 § polisens brottsdatalag). Det kan konstateras att definitionen av vad som utgör en genetisk uppgift är betydligt bredare i brottsdatalagen än i dataskyddsdirektivet, vilket kan leda till att förbudet blir mer omfattande än vad som avsetts. Någon närmare genomlysning av vilka uppgifter som omfattas av definitionen har inte gjorts i tidigare förarbeten. Beroende på vad som innefattas i definitionen av genetiska uppgifter kan det finnas behov för fler delar inom Polismyndigheten att behandla sådana uppgifter.

Oklart rättsligt stöd för behandling i syfte att utveckla datasystem, göra uppföljningar m.m.

Planering, uppföljning och utvärdering av verksamheten anses vara en integrerad del av själva verksamheten vid en myndighet. Det krävs därför normalt inte någon särskild bestämmelse som ger stöd för personuppgiftsbehandling för sådana syften (se t.ex. prop. 2017/18:232 s. 118 och 119). Även testverksamhet som en myndighet genomför t.ex. för att säkerställa att den har väl fungerande it-system kan normalt genomföras utan uttryckligt stöd (se t.ex. prop. 2019/20:113 s. 19).

För att på bästa sätt kunna utnyttja de tekniska möjligheter som numera finns att behandla information automatiskt måste programvarans förmåga utvecklas genom att tränas på data. Enligt Polismyndigheten uppstår ofta svåra bedömningar i fråga om vilken rättslig grund och närmare ändamål som behandling av exempelvis s.k. skarp data i utvecklings- eller uppföljningssyfte har. Ibland uppkommer t.ex. oklarheter om vad som gäller i fråga om förutsättningarna för gemensamt tillgängliggörande, upplysningskrav och längsta tid för behandling för sådana uppgifter.

Viss personuppgiftsbehandling regleras inte i polisens brottsdatalog

Viss behandling av personuppgifter inom Polismyndigheten faller inom brottsdatalogens tillämpningsområde utan att det finns reglering om behandlingen i polisens brottsdatalog. Som exempel kan nämnas Polismyndighetens verksamhet enligt 3 § utlänningsdatalagen (2016:27). Eftersom utvisning är en särskild rättsverkan av brott, som är direkt kopplad till påföljdsbestämningen, faller Polismyndighetens behandling av personuppgifter vid verkställande av utvisning på grund av brott under brottsdatalogens tillämpningsområde (se prop. 2017/18:254 s. 24).

Utlänningsdatalagen är då inte tillämplig (4 c §) samtidigt som området inte alls regleras i polisens brottsdatalog. Ett annat exempel är att polisens brottsdatalog inte heller i övrigt gäller för personuppgiftsbehandling som sker i syfte att verkställa straffrättsliga påföljder (förutom uppbörd). Det kan medföra otydligheter när det gäller hur personuppgifter får behandlas i dessa ärenden.

Dataskyddsregleringens förhållande till annan reglering och dess räckvidd

När uppgifter samlats in med stöd av särskild lagstiftning, t.ex. tvångsmedel enligt rättegångsbalken kan det enligt Polismyndigheten uppstå oklarheter i fråga om hur myndigheten kan använda informationen för andra ändamål än

för vilket den samlats in. Det beror enligt myndigheten på att reglerna som styr inhämtningen inte alltid förhåller sig på ett tydligt sätt till dataskyddsreglerna, om t.ex. gemensamt tillgängliga uppgifter, behandling för flera ändamål eller längsta tid för behandling. Det finns också anledning att överväga om dataskyddsregelverket i dessa avseenden är ändamålsenligt.

En angränsande fråga som Polismyndigheten har lyft gäller brottsdatalagens och polisens brottsdatalags räckvidd i fråga om personuppgifter som myndigheten har tillgång till men som finns utanför myndighetens rådighet, t.ex. personuppgifter som finns tillgängliga fritt på internet. Det finns enligt Polismyndigheten situationer då bestämmelser i brottsdatalagen eller polisens brottsdatalag, trots att de enligt sin ordalydelse synes vara tillämpliga, inte kan tillämpas.

Det kan alltså finnas behov av att klargöra hur dataskyddsregleringen förhåller sig till annan reglering och för vilken personuppgiftsbehandling den gäller.

En översyn av regelverket

Polismyndigheten har pekat på att regelverket som styr myndighetens personuppgiftshantering inte ger de förutsättningar som krävs för att myndigheten ska kunna fullgöra sina uppgifter. Den nuvarande lagstiftningen fungerar i vissa avseenden väl. Samtidigt stöter Polismyndigheten i dag på problem bl.a. vid tillämpningen av de grundläggande bestämmelserna i polisens brottsdatalag. De bestämmelser som reglerar Polismyndighetens behandling av personuppgifter på brottsdatalagens område behöver därför ses över.

De författningar som står i fokus för utredningen är polisens brottsdatalag med tillhörande förordning och i viss mån brottsdatalagen. Även andra författningar kan dock aktualiseras.

I det föregående avsnittet redovisas ett antal begränsningar i det nuvarande regelverket som utredaren inom ramen för översynen får anledning att ägna särskild uppmärksamhet. Dessa blir centrala frågor, men uppdraget att göra en översyn av regleringen gäller inte endast dessa.

Det är mycket angeläget att Polismyndigheten har ändamålsenliga regler för personuppgiftsbehandling, som skapar goda förutsättningar för myndigheten

att fullgöra sitt uppdrag på ett effektivt sätt. Polismyndigheten behöver få ökade möjligheter att behandla personuppgifter och en reglering som är anpassad efter de behov och möjligheter som finns i dag och kan tänkas finnas i framtiden.

Utredaren ska därför

- göra en översyn av de bestämmelser som reglerar Polismyndighetens behandling av personuppgifter på brottsdatalagens område,
- undersöka och bedöma i vilken utsträckning dagens regelverk försvårar en effektiv informationshantering i Polismyndighetens verksamhet,
- lämna förslag på hur personuppgifter kan hanteras av Polismyndigheten på ett mer ändamålsenligt sätt än i dag, och
- lämna nödvändiga författningsförslag.

I utredningen behöver Polismyndighetens behov av att behandla personuppgifter vägas noga mot den enskildes rätt till skydd för sin personliga integritet. Särskilda integritetsskyddande åtgärder kan behövas. Det är också viktigt att förslagen utformas så att tillsynsmyndigheterna ges förutsättningar att kunna fullgöra sin uppgift att utöva tillsyn över personuppgiftsbehandlingen på ett effektivt och ändamålsenligt sätt. På vissa områden överlappar tillsynsmyndigheternas uppgifter, t.ex. vad gäller skyldighet att på begäran kontrollera om personuppgiftsbehandlingen är författningsenlig (jfr 5 kap. 3 § brottsdatalagen och 3 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet). Det kan ifrågasättas om det är nödvändigt att båda myndigheterna har en sådan kontrollskyldighet, och det bör därför övervägas om de parallella skyldigheterna ska kvarstå.

Det ingår inte i utredarens uppdrag att se över sekretessregleringen eller andra regler som kan påverka vilka uppgifter Polismyndigheten har möjlighet att ta del av. Det kan dock finnas behov av sekretessregler för att skydda den informationshantering som utredarens förslag medför.

Den 1 juli 2025 trädde nya regler om biometri i brottsbekämpningen i kraft (prop. 2024/25:37). Utredarens uppdrag omfattar därför inte att göra någon fullständig översyn av förutsättningarna för att använda biometri som verktyg i brottsbekämpningen. Det utesluter dock inte att det kan finnas anledning att föreslå ändringar även avseende detta i någon del, t.ex. vad gäller längsta tid för behandling.

Andra myndigheters behov kan behöva beaktas

Polisens brottsdatalog gäller även för personuppgiftsbehandling i viss verksamhet vid Ekobrottsmyndigheten och Säkerhetspolisen (1 kap. 1 §) och de behov som finns där behöver därför beaktas. De förslag som utredaren lämnar bör som utgångspunkt gälla även för sådan personuppgiftsbehandling, om inte särskilda skäl talar emot det.

Polismyndigheten är inte den enda myndigheten som i stor utsträckning tillämpar brottsdatalogen. Även bl.a. Ekobrottsmyndigheten, Kustbevakningen, Skatteverket, Tullverket och Åklagarmyndigheten tillämpar lagen i sin brottsbekämpande verksamhet. Polismyndigheten har ett nära samarbete med dessa myndigheter och med Säkerhetspolisen, vilket i vissa delar underlättas genom bestämmelser i polisens brottsdatalog. Flera av de brottsbekämpande myndigheterna får t.ex. medges direktåtkomst till Polismyndighetens register. Det är viktigt att möjligheterna för Polismyndigheten att samverka med övriga myndigheter inte inskränks och det ingår i uppdraget att vid behov lämna följdförslag för att motverka detta.

Även om det är Polismyndighetens förutsättningar att behandla personuppgifter som står i fokus för uppdraget måste det beaktas att även andra myndigheter kan bli berörda av förslagen. Andra myndigheter kan ha specifika behov utifrån sina respektive uppdrag eller behov som motsvarar Polismyndighetens. Det kan också finnas frågor som lämpligen behandlas i ett sammanhang för de brottsbekämpande myndigheterna. Ett exempel är definitionen av och möjligheten att behandla genetiska uppgifter. Utredaren är oförhindrad att lämna förslag som gäller för fler brottsbekämpande myndigheter, om det bedöms lämpligt.

Det EU-rättsliga regelverket och frågan om nationell säkerhet

Det svenska regelverket för personuppgiftsbehandling måste vara förenligt med det EU-rättsliga regelverket. Dataskyddsdirektivet är centralt för denna översyn men även andra rättsakter, t.ex. AI-förordningen ((EU) 2024/1689), kan vara relevanta.

Personuppgiftsbehandling som utförs i verksamhet som rör nationell säkerhet omfattas inte av dataskyddsdirektivets tillämpningsområde (se artikel 2.3 a och skäl 14). Sådan personuppgiftsbehandling är dock inte generellt undantagen från brottsdatalogens tillämpningsområde. Brottsdatalogen gäller inte vid Säkerhetspolisens behandling av

personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen. Brottssdatalagen gäller dock i övrigt för Polismyndighetens behandling av personuppgifter, även om den skulle röra nationell säkerhet.

Brottsbekämpning på området för nationell säkerhet ankommer normalt på Säkerhetspolisen (3 § polislagen). Polismyndigheten har argumenterat för att den organiserade brottsligheten utgör ett minst lika allvarligt hot mot samhället som terrorism, vars bekämpande är en fråga om nationell säkerhet. Polismyndigheten bedömer att 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. Polismyndigheten anser därför att myndighetens personuppgiftsbehandling som rör nationell säkerhet bör undantas från brottssdatalagens tillämpningsområde och att en ändamålsenlig reglering för myndighetens personuppgiftsbehandling på det området bör införas.

Utredaren ska därför

- analysera och bedöma om Polismyndighetens personuppgiftsbehandling i någon del kan anses falla utanför dataskyddsdirektivets tillämpningsområde och om behandlingen därför bör undantas från brottssdatalagens tillämpningsområde, och i så fall
- ta ställning till vilka regler som bör gälla för sådan behandling, och
- lämna nödvändiga författningsförslag.

Grundläggande fri- och rättigheter måste beaktas

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Inskränkningar i det grundlagsfästa skyddet kan endast göras genom lag och bara under de förutsättningar som anges i 2 kap. 20–22 och 25 §§ regeringsformen.

Rätten till respekt för privat- och familjelivet och för korrespondens skyddas också av bl.a. artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen), artiklarna 3, 7 och 8 i EU:s stadga om de

grundläggande rättigheterna (stadgan) och artikel 16 i FN:s konvention om barnets rättigheter (barnkonventionen). Av artikel 3 i barnkonventionen framgår det att vid alla åtgärder och beslut som rör barn ska vad som bedöms vara barnets bästa beaktas i första hand.

Detta grundläggande skydd för enskildas integritet är inte absolut. Av såväl regeringsformen som Europakonventionen och stadgan framgår att skyddet under vissa förutsättningar får begränsas. En begränsning i utövande av rättigheten får göras endast om det sker i enlighet med lag och det är nödvändigt för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En begränsning får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den.

Eftersom det inte ingår i uppdraget att föreslå grundlagsändringar måste de förslag som utredaren lämnar vara förenliga med regeringsformen och naturligtvis också med Europakonventionen, stadgan, barnkonventionen och Sveriges internationella förpliktelser i övrigt.

Närliggande frågor

Utredaren får ta upp och lämna förslag även i andra frågor än de som nämns i dessa direktiv, om frågorna har samband med uppdraget och uppdraget ändå kan redovisas i tid.

Konsekvensbeskrivningar

Utredaren ska utöver vad som följer av kommittéförordningen (1998:1474) och förordningen (2024:183) om konsekvensutredningar noga redovisa förslagets effekter för den personliga integriteten. Utredaren ska också lägga särskild vikt vid att beskriva förslagets betydelse för möjligheten att förebygga, förhindra, upptäcka, utreda och lagföra brott. Om förslagen bedöms innebära behov av anpassningar av Polismyndighetens it-system ska en bedömning även göras av hur anpassningarna påverkar övrig it-utveckling på myndigheten inklusive gemensamma utvecklingsinsatser inom Rättsväsendets digitalisering. Utredaren ska också redovisa hur förslagen förhåller sig till Sveriges internationella åtaganden om mänskliga rättigheter.

Kontakter och redovisning av uppdraget

Utredaren ska under arbetet samråda med och hämta in synpunkter och upplysningar från Polismyndigheten. Vid behov ska utredaren hämta in synpunkter och upplysningar även från andra myndigheter och aktörer som

kan vara berörda. Utredaren ska också hålla sig informerad om och ta hänsyn till relevant arbete som pågår inom Regeringskansliet och kommittéväsendet samt inom ramen för Sveriges internationella åtaganden.

Uppdraget ska redovisas senast den 13 september 2027.

(Justitiedepartementet)