Några reflektioner om särregleringen av personuppgiftsbehandling för brottsbekämpning

Gunnel Lindberg

Två olika regelsystem – ett generellt och ett specialiserat

Alla känner till dataskyddsförordningen (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, vanligen kallad GDPR), men inte lika många är bekanta med dataskyddsförordningens mindre syskon, dataskyddsdirektivet. Medan GDPR reglerar dataskyddet generellt gäller dataskyddsdirektivet bara för ett speciellt område. I artikel 3 i GDPR klargörs att GDPR inte gäller om dataskyddsdirektivet är tillämpligt.

Dataskyddsdirektivet (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) behandlar dataskyddet vid framför allt brottsbekämpning, lagföring och straffverkställighet. Eftersom det, i motsats till dataskyddsförordningen som är direkt tillämplig, är ett direktiv har det i svensk rätt genomförts genom nationell lagstiftning, brottsdatalagen (2018:1177) och brottsdataförordningen (2018:1202). Brottsdatalagen är en ramlag, som trädde i kraft den 1 augusti 2018 (Brottsdatalag, prop. 2017/18:232). För de myndigheter som har huvudansvar för brottsbekämpning, lagföring och straffverkställighet (Polismyndigheten, Tullverket, Kustbevakningen, Skatteverket, åklagarväsendet, de allmänna domstolarna och Kriminalvården) kompletteras brottsdatalagen av särskilda lagar om personuppgiftsbehandlingen inom brottsdatalagens område (SFS 2018:1693–1699).

Från både GDPR:s och dataskyddsdirektivets tillämpningsområden undantas sådan personuppgiftsbehandling som rör nationell säkerhet, eftersom det är något som ligger utanför unionsrätten. Av det skälet

regleras Säkerhetspolisens personuppgiftsbehandling i en särskild lag, lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter. Den lagen är nu föremål för översyn (dir. 2023:64).

Varför finns det en särreglering?

Tanken bakom uppdelningen mellan GDPR och dataskyddsdirektivet är att det behövs särskilda regler om skydd av personuppgifter inom direktivets tillämpningsområde.

Direktivet gäller på områden där samhällsintresset väger särskilt tungt; brottsbekämpning, lagföring och straffverkställighet samt ordning och säkerhet. En effektiv sådan verksamhet förutsätter att personuppgifter får behandlas oberoende av individens samtycke. Brottsbekämpning och lagföring är dessutom områden som generellt sett kräver omfattande personuppgiftsbehandling och i betydande utsträckning även behandling av känsliga personuppgifter. Sådan verksamhet skulle över huvud taget inte fungera om enskilda personers inställning till personuppgiftsbehandlingen skulle ha betydelse. Utöver samhällsintresset av dels ordning och säkerhet, dels att brott förhindras och, om de begås, utreds och lagförs täcker direktivet områden där typiskt sett olika personers intressen står mot varandra. Brottsoffrens och gärningsmännens intressen är som regel direkt motstridiga. Om flera personer har planerat eller medverkat i ett brott kan de också ha motstående intressen, t.ex. att lägga skulden på varandra. De som har uppgifter om ett brott är dessutom i många fall ovilliga att lämna information till brottsbekämpande myndigheter. Det kan gälla oavsett om de är gärningsmän, vittnen eller brottsoffer. Information inhämtas därför i stor utsträckning genom tvångsåtgärder. Mot den bakgrunden är en särreglering nödvändig.

Särregleringen innebär att personuppgifter får behandlas i större utsträckning än vad som skulle varit möjligt om GDPR hade tillämpats. Det finns emellertid en mycket viktig begränsning. Endast behöriga myndigheter får enligt brottsdatalagen behandla personuppgifter enligt den lagen. Med behörig myndighet avses en myndighet som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder, eller upprätthålla allmän ordning och säkerhet eller en annan aktör som har anförtrotts myndighetsutövning för ett sådant syfte. Det är således bara när vissa specifika uppgifter utförs som brottsdatalagen och den kompletterande lagstiftningen får tillämpas. Dessutom krävs det att personuppgifterna behandlas för ett sådant syfte som nyss angetts. När t.ex. Polismyndig-

heten behandlar personuppgifter i sin tillståndsverksamhet eller Tullverket behandlar personuppgifter i sin kontrollverksamhet görs det med stöd av GDPR och den lagstiftning som anknyter till den lagen, inte brottsdatalagen.

Brottsdatalagen är visserligen generellt tillämplig inom det område som dataskyddsdirektivet reglerar, men lagen är samtidigt subsidiär i förhållande till annan lag eller förordning. Sedan länge har det funnits särskilda lagar för de behöriga myndigheternas personuppgiftsbehandling inom brottsdatalagens område. Den 1 januari 2019 infördes nya lagar om personuppgiftsbehandling inom brottsdatalagens område för polisen, Tullverket, Kustbevakningen, Skatteverket, åklagarväsendet, de allmänna domstolarna och Kriminalvården. De lagarna gäller utöver brottsdatalagen, men de innehåller enbart bestämmelser som innebär preciseringar, undantag eller avvikelser från den lagen.

Skillnader mellan GDPR och brottsdatalagen

Den rättsliga grunden för behandling av personuppgifter skiljer sig mellan GDPR och brottsdatalagen. Uppgifter får enligt artikel 6 i GDPR behandlas bl.a. om den registrerade har lämnat samtycke (punkt a), om behandlingen är nödvändig för att fullgöra ett avtal (punkt b) eller en rättslig förpliktelse (punkt c) eller om den är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (punkt e). Enligt 2 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning får personuppgifter behandlas med stöd av artikel 6.1 e i EU:s dataskyddsförordning om behandlingen är nödvändig antingen för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning, eller som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning. Även inom GDPR:s tillämpningsområde finns det sektorsvisa kompletterande lagar om personuppgiftsbehandling.

Enligt 2 kap. 1 § brottsdatalagen får personuppgifter behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Även myndigheter och andra organ som inte har något av detta som sin primära uppgift kan vara behöriga myndigheter i brottsdatalagens mening när de utför sådana uppgifter, t.ex. kommuner vid verkställighet av ungdomstjänst.

En stor skillnad mellan GDPR och den reglering som bygger på dataskyddsdirektivet är, som redan framgått, den enskildes möjlighet att påverka personuppgiftsbehandlingen. Samtycke från den enskilde saknar betydelse vid den behandling av personuppgifter som görs med stöd av regleringen inom brottsdatalagens område. Även den enskildes rätt till insyn i personuppgiftsbehandlingen är av naturliga skäl mer begränsad än det som gäller enligt GDPR. Däremot är t.ex. personuppgiftsansvarigas skyldigheter, tillsynen och rätten till skadestånd i stora delar likartat reglerad.

Det förhållandet att brottsdatalagen och den kompletterande lagstiftningen ger större utrymme för personuppgiftsbehandling kompenseras till viss del genom att den enskilde har en uttrycklig rätt att vända sig till tillsynsmyndigheter (både Integritetskyddsmyndigheten och Säkerhets- och integritetsskyddsnämnden) för laglighetsprövning. Enskilda får begära att tillsynsmyndigheten kontrollerar om personuppgiftsbehandling har förekommit och i så fall om den har varit författningsenlig. Myndigheten är skyldig att utföra den begärda kontrollen. Någon motsvarande rätt finns inte enligt GDPR.

Dataskyddet enligt brottsdatalagen minst lika viktigt som skyddet enligt GDPR

Medan GDPR och det skydd förordningen ger enskilda inte sällan diskuteras både i media och litteraturen röner dataskyddet enligt brottsdatalagen och den kompletterande lagstiftningen inte lika stort intresse, trots att dataskyddet enligt den senare lagstiftningen kan vara minst lika viktigt för enskilda. Det beror inte bara på att personuppgiftsbehandlingen görs utan den enskildes samtycke utan även på att den enskilde i många fall inte ens känner till att uppgifter om honom eller henne behandlas, eftersom det råder sekretess till skydd för det allmännas verksamhet både i underrättelseverksamhet och för förundersökningar enligt 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400).

Dessutom får vissa av personuppgifterna, enligt den lagstiftning som kompletterar brottsdatalagen, behandlas längre än vad som krävs för att slutföra det enskilda ärendet. Något som har stor betydelse i sammanhanget är nämligen att polisen, för att kunna dra nytta av den kunskap man fått om bl.a. misstänkta gärningsmän och brottsmönster, får behandla uppgifter om brott och brottslig verksamhet under viss tid efter det att det enskilda ärendet har avslutats (se Integritet och effektivitet i polisens brottsbekämpande verksamhet, prop. 2009/10:85,

s. 208 f.). Det beror bl.a. på risken för återfall i brott och behovet av att kunna förebygga brott.

Det bör också framhållas att det förhållandet att uppgifter om en person behandlas av polisen kan ge ringar på vattnet i form av fler kontroller, annat bemötande när personen påträffas etc. Om personen varit misstänkt för brott kan det i förlängningen också påverka möjligheterna att få vissa tillstånd eller söka vissa tjänster, där det ställs särskilda krav på laglydighet. Om en uppgift skulle vara felaktig kan den därför få svåra konsekvenser. Ett väl fungerande dataskydd är därmed extra viktigt i den brottsbekämpande verksamheten.

Begreppet behörig myndighet behöver värnas

Eftersom brottsdatalagen ger betydligt större utrymme för att behandla personuppgifter än GDPR och regleringen förutsätter att behandlingen görs av en behörig myndighet för de syften som anges i brottsdatalagen blir begreppet behörig myndighet centralt. Vem som är behörig myndighet pekas inte ut i brottsdatalagen (prop. 2017/18:232 s. 429). Det beror på att det knappast skulle gå att peka ut alla myndigheter som kan ha vissa sådana uppgifter i författningstext. Dessutom skulle det krävas omfattande undantag, eftersom många av dem bara är behörig myndighet när de utför en specifik uppgift (se Brottsdatalag, SOU 2017:29, s. 169 f.). De uppgifter som gör en myndighet behörig tydliggörs i stället i annan lagstiftning, t.ex. vilka myndigheter som verkställer straffrättsliga påföljder. Det framgår också av annan lagstiftning vilka myndigheter eller tjänstemän inom myndigheterna som har till uppgift att upptäcka eller förhindra brott eller som får utreda och lagföra brott eller vem får ingripa för att trygga ordning och säkerhet. Ett viktigt krav för att någon aktör som inte är myndighet ska vara behörig myndighet i brottsdatalagens mening är att vederbörande agerar i myndighetsutövning för ett sådant syfte som anges i den lagen. Även om det i andra avseenden kan finnas vissa gränsdragningsproblem är kraven för att vara behörig myndighet enligt brottsdatalagen tydliga och enkla att kontrollera i de fallen.

Däremot är det inte lika tydligt vad begreppet ”förebygga brott” innebär och vilka myndigheter som har till uppgift att förebygga brott, särskilt mot bakgrund av att allt fler myndigheter uppmanas att göra vad de kan för att förebygga att brott begås inom deras verksamhetsområde. Det råder ingen tvekan om att Polismyndigheten och Säkerhetspolisen har den uppgiften generellt enligt 2 respektive 3 § polislagen (1984:387). Tullverket har en motsvarande, men mer begränsad, uppgift enligt 3 § förordningen (2016:1332) med instruktion för Tullverket och detsamma

gäller Skatteverket enligt 6 § lagen (1997:1024) om Skatteverkets brottsbekämpande verksamhet.

Inte ens för de myndigheter som har till uttrycklig uppgift att förebygga brott är det emellertid klart vad som ligger i uppgiften. Allmän information om hur enskilda ska skydda sig mot brott kan knappast räknas dit, t.ex. om polisen besöker skolor, pensionärsorganisationer eller föreningar för att upplysa om riskerna för brott eller om Tullverket eller Skatteverket varnar företag för viss rättstillämpning. Inte heller när myndigheter samlar in information i syfte att skaffa underlag till författningsändringar bör det räknas till brottsförebyggande verksamhet i brottsdatalagens mening.

Om en myndighet, som i övrigt helt saknar brottsbekämpande uppgifter, inom sitt verksamhetsområde får till uppgift att förebygga brott beror det oftast på att regeringen vill understryka skyldigheten för myndigheten i fråga att informera regeringen om nya risker eller tendenser till brott som kan kräva författningsändringar. Varje uttalande från riksdag eller regering om att myndigheter ska bidra till att förebygga brott kan därför enligt min mening inte göra dem till behöriga myndigheter i brottsdatalagens mening. Det krävs en betydligt mer konkret uppgift än så. Även om en myndighet har till uppgift att stödja polisen i dess verksamhet krävs att det är en konkret, författningsreglerad skyldighet, som t.ex. att utföra rättsmedicinska obduktioner, för att myndigheten i fråga ska betraktas som behörig myndighet i brottsdatalagens mening (se SOU 2017:29 s. 183).

Vissa myndigheter ska enligt sina instruktioner eller annan lagstiftning delta i det myndighetsgemensamma arbetet mot den grova och organiserade brottsligheten. Samarbetet regleras i lagen (2016:774) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet och förordningen med samma namn. Enligt förarbetena till brottsdatalagen gör emellertid uppgiftsskyldighet eller skyldighet att anmäla brott inte en myndighet till behörig myndighet i brottsdatalagens mening (prop. 2017/18:232 s. 430).

För att kunna komma till rätta med bl.a. gängkriminalitet och annan organiserad brottslighet och att kunna varna presumtiva brottsoffer ökar polisens behov av att kunna delge andra delar av samhället information. Det gäller inte bara information om brottslingars tillvägagångssätt och riskerna för att utsättas för brott utan även information om personer och företag som kan vara inblandade i brottslig verksamhet. För mottagarna av informationen kan det vara ett problem hur de ska handskas med vad de får veta av polisen om personer som kan vara inblandade i brottslig verksamhet. Som regel är det som framgått GDPR som ska tillämpas, inte brottsdatalagen.

Från dataskyddssynpunkt är det olyckligt om den nuvarande osäkerheten om vem som är behörig myndighet leder till att information, som inte är lika robust som t.ex. information om att någon har dömts för brott, riskerar att spridas och användas på fel sätt. För samhället är det dock lika olyckligt om viktig information som kan förhindra brott aldrig kommer till nytta därför att mottagaren inte vet hur den får hanteras. En extensiv tolkning av begreppet behörig myndighet i brottsdatalagen är emellertid inte lösningen. Det skulle undergräva dataskyddet för enskilda. Mot den bakgrunden kan det enligt min mening behövas ytterligare förtydliganden i brottsdatalagen rörande vilka som är behöriga myndigheter.

Underrättelseverksamheten är oreglerad

Ett skäl till att dataskyddet är särskilt viktigt i den brottsbekämpande verksamheten är att information är av avgörande betydelse för att den verksamheten ska kunna bedrivas effektivt och likaså att den information som finns är tillgänglig för alla som kan behöva den. I den lagstiftning som kompletterar brottsdatalagen finns det därför särskild reglering om behandlingen av personuppgifter som ska vara tillgängliga för fler än ett fåtal personer.

Det största problemet i sammanhanget är att underrättelseverksamhet är oreglerad. Underrättelseverksamhet definieras negativt, som en verksamhet som rör information som inte når upp till de krav som ställs för att starta en brottsutredning. Med underrättelseverksamhet avses arbete med insamling, bearbetning och analys av information i syfte att förhindra eller upptäcka brottslig verksamhet när det ännu inte finns misstankar om att ett visst konkret brott har begåtts (se prop. 2008/09:85 s. 318).

Samhällsutvecklingen innebär att underrättelseverksamhet blivit mycket viktigare när framför allt den organiserade brottsligheten i allt större utsträckning strider om narkotikamarknader, angriper välfärdssystem och utnyttjar företag för att tvätta pengar från kriminalitet och att investera vinster från brott.

Det finns i dag inga regler som anger när och hur underrättelseverksamhet får bedrivas eller vem som får fatta beslut om att sådan verksamhet ska påbörjas eller avslutas. Det är inte ens självklart att myndigheter som bedriver underrättelseverksamhet inom brottsdatalagens område har det som en tydlig arbetsuppgift. Det är enligt min mening en betydande brist att det saknas grundläggande lagstiftning om underrättelseverksamhet.

Det kan inte sällan vara svårt att avgöra om en person som har någon form av kontakt med någon som misstänks vara inblandad i kriminalitet också är inblandad eller är helt oskyldig. En tillsynsmyndighet har därför oftast inte saklig grund för att kritisera personuppgiftsbehandlingen trots att den kan förefalla tvivelaktig. Även om personerna i fråga inte på något sätt har någon koppling till brottslig verksamhet behöver polisen inte sällan ha uppgifter om dem för att kunna följa den brottsliges förehavanden. Den sistnämnde kan ju t.ex. låna någon anhörigs eller annans mobiltelefon eller fordon i syfte att undgå polisens spaning. Därför krävs det en välbalanserad lagstiftning, som sätter tydliga gränser för när uppgifter om personer som inte misstänks vara inblandade i konkreta brott får behandlas.

Så länge underrättelseverksamheten förblir oreglerad finns det emellertid en betydande risk att uppgifter om personer som inte på något sätt är inblandade i kriminell verksamhet behandlas, t.ex. uppgifter om anhöriga eller flickvänner till dem som misstänks för att delta i sådan verksamhet. Även uppgifter om personer med ytliga kontakter med dem som är inblandade i brottslig verksamhet kan, med dagens reglering, komma att behandlas. Det finns i och för sig en motsvarande risk för att uppgifter om utomstående behandlas vid förundersökning och lagföring av brott. Då har emellertid personerna i fråga en väldefinierad roll, t.ex. som målsägande, vittne eller vårdnadshavare. Därmed riskerar de inte att misstas för att själva vara inblandade i brottsligheten. I underrättelseverksamhet är risken betydligt större för att enskildas personuppgifter behandlas, trots att de inte har någon anknytning till brottsligheten.

Hur påverkar nya krav på bekämpningen av allvarlig brottslighet integritetsskyddet?

Samhällsförändringarna under senare år, särskilt det förhållandet att organiserad brottslighet och brottslighet som begås inom ramen för kriminella nätverk breder ut sig, ställer större krav på polisens förmåga att ha god kännedom om personer som kan antas vara inblandade i brottsligheten och om deras kontakter. Antalet personer som är knutna till exempelvis kriminella nätverk ändras fortlöpande. Det påverkas också av att vissa av dem häktas och lagförs och därmed åtminstone tillfälligt hindras från fortsatt brottslig verksamhet. Det innebär att de brottsbekämpande myndigheternas behov av att kunna behandla personuppgifter för att hålla jämna steg med brottsligheten successivt ökar.

Dataskyddet syftar till att värna enskildas integritet och sätta gränser för hur bl.a. myndigheter får behandla personuppgifter. Det skyddet blir allt viktigare ju fler uppgifter om enskilda som behandlas av de brottsbekämpande myndigheterna. De brottsbekämpande myndigheterna, främst polisen, har under senare år fått avsevärda resursförstärkningar med utgångspunkten att de effektivare ska kunna bekämpa framför allt gängbrottsligheten. Genom att de har fått större resurser växer kraven på att de ska redovisa förbättrade resultat när det gäller brottsbekämpningen. Om det inte blir fallet kan de förvänta sig kritik och ökade krav från den politiska nivån.

Det är naturligtvis angeläget att satsningarna på bekämpning av bl.a. gängbrottsligheten ger positiva resultat. Det kan emellertid leda till att både myndigheter och tjänstemän tänjer på lagstiftningen, inte minst då dataskyddet, för att nå de önskade resultaten. All lagstiftning ger utrymme för tolkningar, men det är viktigt att reglering till skydd för grundläggande fri- och rättigheter inte tolkas så att skyddet riskerar att urholkas.

Det finns nämligen en risk att enskilda tjänstemän i sin ambition att lösa brott tolkar regleringen på ett sätt som inte är avsett eller blundar för viktiga dataskyddsregler. Ett talande exempel är att några tjänstemän inom Polismyndigheten laddade ned en applikation för ansiktsigenkänning och använde den för att göra jämförelser med tillgängliga ansiktsbilder. Det var således fråga om behandling av en särskild typ av känsliga personuppgifter, s.k. biometriska uppgifter. Behandlingen, som saknade stöd i lagstiftningen, gjordes utan att myndigheten hade vetskap om den eller hade godkänt den. När saken upptäcktes beslutade Integritetsskyddsmyndigheten att ålägga Polismyndigheten en sanktionsavgift enligt 6 kap. 1 § brottsdatalagen. Polismyndigheten överklagade beslutet som fastställdes av förvaltningsrätten men upphävdes av kammarrätten (Kammarrättens i Stockholm dom den 7 november 2022, dnr 7678-21).

Tillsyn över personuppgiftsbehandlingen är viktig

Den kraftigt ökade personuppgiftsbehandlingen inom brottsdatalagens område och polisens och andra brottsbekämpande myndigheters behov av att kartlägga bl.a. miljöer, kontakter och tillgång till lokaler och fordon leder med nödvändighet till att allt fler personuppgifter behandlas och att fler personer omnämns i register och uppgiftssamlingar. Det är då av stor betydelse för både skyddet av enskildas integritet och tilltron till verksamheten att det finns en väl fungerande tillsyn. Det finns

två myndigheter som bör nämnas särskilt i sammanhanget, Integritetsskyddsmyndigheten och Säkerhets- och integritetsskyddsnämnden (i fortsättningen nämnden).

Integritetsskyddsmyndigheten är enligt 2 a § förordningen (2007:975) med instruktion för myndigheten tillsynsmyndighet enligt artikel 41.1 i dataskyddsdirektivet. Det är samma roll som myndigheten har enligt GDPR och en rad andra EU-instrument. Tillsynsuppgiften motsvarar därmed myndighetens generella uppdrag att utöva tillsyn över personuppgiftsbehandling oavsett varför eller av vem uppgifterna behandlas. Det bör emellertid framhållas att inom brottsdatalagens område har Integritetsskyddsmyndigheten ett dubbelt uppdrag. Myndigheten ska enligt 5 kap. 1 § brottsdatalagen verka både för att fysiska personers grundläggande rättigheter och friheter skyddas i samband med behandling av personuppgifter och för att underlätta det fria flödet av personuppgifter inom lagens tillämpningsområde. Det tudelade uppdraget innebär att Integritetsskyddsmyndigheten inte bara kan se till enskildas intressen utan måste balansera det mot det allmännas intresse av att det fria flödet av personuppgifter underlättas inom detta specifika område.

Nämnden utövar tillsyn enligt 1 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet. Enligt den paragrafen ska nämnden utöva tillsyn över den behandling av personuppgifter som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten enligt brottsdatalagen, lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område och lagen om Säkerhetspolisens behandling av personuppgifter. Tillsynen ska särskilt avse behandling av känsliga personuppgifter. Nämnden har dessutom tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och är även skyldig att på begäran av enskilda kontrollera om deras personuppgifter har behandlats författningsenligt. Genom att nämnden har ett smalt tillsynsuppdrag, som enbart syftar till att värna enskildas intressen, har den möjlighet att gå mera på djupet i sin tillsynsverksamhet.

Eftersom både riksdagens ombudsmän (JO) och Justitiekanslern (JK) har generell tillsyn över myndighetsutövning har även de tillsyn över myndigheternas personuppgiftsbehandling, men med tanke på JO:s och JK:s breda tillsynsområden och att de är extraordinära tillsynsorgan aktualiseras deras tillsyn över personuppgiftsbehandling sällan. JK kommer emellertid i kontakt med frågor om personuppgiftsbehandling även till följd av sin skadereglerande roll, eftersom nämnden, när den uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten gentemot en fysisk eller juridisk person, anmäler saken till JK (se t.ex. JK:s beslut den 11 juli 2022, dnr 2021/2275).

Resurserna för tillsyn över personuppgiftsbehandling inom brottsdatalagens område har inte hållit jämna steg med informationssamhällets utveckling och att de brottsbekämpande myndigheterna har fått utökade möjligheter att behandla personuppgifter. Tyvärr räcker varken Integritetsskyddsmyndighetens eller nämndens resurser i dag till något annat än att skrapa på ytan.

Ny teknik ger nya möjligheter – hinner personuppgiftsregleringen med?

Under senare år har olika former av teknisk bevisning fått allt större betydelse vid brottsbekämpning och lagföring. Ny teknik och nya arbetsmetoder ökar successivt möjligheterna att utreda brott. Det gäller på olika områden och är naturligtvis i grunden positivt. Samtidigt kan det innebära utmaningar för dem som tillämpar lagstiftningen. Två tydliga exempel är tillämpningsområdena för hemliga tvångsmedel och för biometriska uppgifter. Ny teknik och nya sätt att kommunicera gör att hemliga tvångsmedel automatiskt får ett utökat tillämpningsområde, eftersom de är teknikneutrala. Det ger större möjlighet för brottsbekämpande myndigheter att få tillgång till information men skapar inga nya gränsdragningsproblem när det gäller personuppgiftsbehandlingen. Det gör däremot det förhållandet att nya sätt att använda kommunikationsutrustning gör att biometriska uppgifter om den som begagnar viss teknisk utrustning utnyttjas. Numera öppnas inte sällan mobiltelefoner och liknande kommunikationsutrustning med hjälp av fingeravtryck eller ansiktsigenkänning. Det innebär att biometriska uppgifter lagras och att de potentiellt kan komma att användas för andra ändamål än de ursprungliga. Vidare finns det kommersiella databaser som innehåller dna-uppgifter från ett stort antal personer som har lämnat sina uppgifter till företag för helt andra ändamål än brottsbekämpning.

Biometriutredningen föreslår nya regler som innebär att dna-baserad släktforskning ska få användas för att utreda mord, grov våldtäkt och grov våldtäkt mot barn om alla andra möjligheter att föra brottsutredningen framåt är uttömda (SOU 2023:32 s. 488 f.). Förslaget ska ses mot bakgrund av att det både i Sverige och i andra länder har kunnat påvisas att metoden har gett positiva resultat i vissa uppmärksammade brottsfall som länge varit olösta. Metoden väcker emellertid en rad principiella frågor, eftersom en förutsättning för att använda den är att dna-uppgifter överförs av polisen till en eller flera utländska kommersiella databaser som innehåller dna-profiler. Att Biometriutredningen tillsatts är ett exempel på behovet av att ta ett mera samlat grepp på frå-

gor som rör känslig personuppgiftsbehandling när ny teknik öppnar nya möjligheter för brottsbekämpningen. Utredningen framhåller att det krävs en uttrycklig reglering för att polisen ska få behandla biometriska uppgifter.

Utvecklingen av artificiell intelligens är en annan faktor som måste tas med i diskussionen. Där går utvecklingen snabbt. Hur bör de möjligheter som artificiell intelligens kan komma att skapa kunna utnyttjas i brottsbekämpningen i framtiden? Och vilka effekter får det på dataskyddet för enskilda? Där är diskussionen bara i sin linda, men kanske kan den aviserade översynen av Säkerhetspolisens personuppgiftsreglering ge en viss klarhet.

Den tekniska utvecklingen kan alltså skapa oväntade möjligheter, men lagstiftaren kan knappast förutse allt. Det råder inte någon tvekan om att det redan har eller i framtiden kommer att utvecklas nya metoder och andra möjligheter som kan underlätta brottsutredning och som kräver en ny syn på personuppgiftsbehandling. Det kan t.ex. vara fråga om dataprogram som kan söka reda på och samla in värdefull information eller metoder för att dra nytta av biometriska uppgifter på nya sätt. Det är då viktigt att dataskyddet ger ett tillfredsställande skydd, till dess att lagstiftaren har hunnit ta ställning till om de nya möjligheterna får utnyttjas inom brottsbekämpningen.

Det väcker frågan om lagstiftaren hinner med. Det är enligt min mening oundvikligt att tekniken utvecklas snabbare än lagstiftningen. Det som då är viktigt är att alla som ska tillämpa dataskyddsregler har rätt inställning till dem. De är till för att skydda enskildas friheter och rättigheter. Även om det i enskilda fall kan kännas frustrerande att dataskyddsregler hindrar viss personuppgiftsbehandling måste regleringen tillämpas korrekt. Dataskyddsregler får inte ses som hinder som kan rundas. Om lagstiftningen blir för komplicerad och svåröverskådlig finns det emellertid risk att den inte respekteras.

Erfarenheterna av dataskyddsreformen och möjliga slutsatser

När EU:s dataskyddsreform skulle genomföras i Sverige krävde den mycket omfattande resurser, först i form av utredningar och senare i form av lagstiftningsarbete i Regeringskansliet. Många andra lagstiftningsfrågor fick under några år stå tillbaka till förmån för dataskyddslagstiftning, vilket var frustrerande för politikerna som hellre ville lägga tid och resurser på frågor som betraktades som mer angelägna för partierna och väljarna. När väl lagstiftningen fanns på plats krävdes också

omfattande resurser hos myndigheter och andra organ för att de skulle leva upp till de nya krav som dataskyddsreformen medförde. Inte heller myndigheter och andra organ ville lägga omfattade resurser på ett område som inte gav några synbara vinster för deras kärnverksamhet. Det är enligt min mening därför inte sannolikt att någon vill satsa lika mycket på ett motsvarande lagstiftningsprojekt på många år. Då är det extra viktigt att den befintliga lagstiftningen vårdas och successivt anpassas till nya behov. Även om den nuvarande regleringen är ganska ny, leder teknikutvecklingen och samhällsförändringarna till att det kommer att behövas förändringar i regelsystemet.

Att vårda den befintliga regleringen kräver emellertid insatser där alla bidrar på olika sätt. Lagstiftaren genom att vara lyhörd för berättigade krav på ändringar när nya behov uppstår. Myndigheter och andra organ genom att vid tillämpningen av brottsdatalagen och den kompletterande lagstiftningen respektera de värden som dessa regelverk värnar. Det leder fram till frågan om det nuvarande regelverket om personuppgiftsbehandling och hur det ska samverka med annan lagstiftning, t.ex. rättegångsbalken, polislagen och offentlighets- och sekretesslagen, har blivit alltför komplext och svårtillämpat. Grunden för ett bra framtida dataskydd är lagd genom EU:s dataskyddsreform, men enligt min mening skulle det behövas en utredning som adresserar den frågan. Jag tror att den är viktig för att ge dataskyddet den legitimitet det förtjänar i tider när fokus i hög grad ligger på en effektivare brottsbekämpning.