Effektiv dataskyddstillsyn i AI-åldern – tryckfrihetsförordningen som ett potentiellt hinder

*Ulrika Söderqvist**

Bakgrund

När datalagen trädde ikraft 1973 bestod polisens automatiserade register av ett fåtal system helt utan möjlighet att kommunicera med varandra. Automatiserade register tycks över huvud taget inte ha funnits i underrättelseverksamheten.[1] Idag har polisen och andra brottsbekämpande myndigheter tillgång till ett helt annat it-stöd. I underrättelseverksamheten är ett viktigt syfte med personuppgiftsbehandlingen att kunna identifiera kopplingar mellan personer och på andra sätt bidra till analysen av stora mängder uppgifter, inte sällan känsliga sådana om till exempel hälsa, religion och politisk tillhörighet.

Mängden information som behandlas av de brottsbekämpande myndigheterna har också ökat under de senaste decennierna. I och med att omvärldens information om oss alla ökar, polisens egna förmågor och inhämtningsmetoder utvecklas och nya verktyg tillhandahålls – såsom det relativt nya tvångsmedlet hemlig dataavläsning – kan omfattningen och komplexiteten i den information som innehas av brottsbekämpande myndigheter inte jämföras med det de hade att hantera för femtio år sedan, eller ens ett decennium tillbaka.

En mycket viktig komponent i EU:s dataskyddsreform var att betona vikten av en stark, oberoende och effektiv tillsyn. Inom brottsbekämpningen – det område som täcks av EU:s direktiv om dataskydd för brottsbekämpande myndigheter[2] – framgår detta bland annat av artikel

* Kanslichef vid Säkerhets- och integritetsskyddsnämnden.

[1] SOU 1996:35 s. 38 f.

[2] 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.

42 där tillsynsmyndigheternas fullständiga oberoende regleras liksom medlemsstaternas skyldighet att säkerställa att varje tillsynsmyndighet förfogar över de personella, tekniska och finansiella resurser samt de lokaler och den infrastruktur som behövs för att myndigheten ska kunna utföra sina uppgifter. Motsvarande bestämmelser finns i EU:s dataskyddsförordning[3].

I svensk rätt finns bestämmelser om Integritetsskyddsmyndighetens och Säkerhets- och integritetsskyddsnämndens undersökningsbefogenheter mot de brottsbekämpande myndigheterna i 5 kap. 5 § brottsdatalagen (2018:1177) respektive i 4 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet. Integritetsskyddsmyndigheten har enligt brottsdatalagen rätt att få tillgång till uppgifter, upplysningar, lokaler, utrustning och andra medel som behövs för tillsynen, medan Säkerhets- och integritetsskyddsnämnden har rätt att få de uppgifter, upplysningar, information och det biträde som nämnden begär. Trots dessa relativt långtgående befogenheter är frågan om dataskyddstillsynen i Sverige har de verktyg som behövs när vi nu rör oss med hög hastighet in i en verklighet där artificiell intelligens (AI) används alltmer.

Denna artikel tar sitt avstamp i förutsättningarna för att utöva dataskyddstillsyn inom brottsbekämpningen utifrån mina erfarenheter från arbete vid Säkerhets- och integritetskyddsnämnden under de senaste tio åren. Utmaningarna som beskrivs i artikeln har nog i vart fall delvis relevans även vid tillsyn i andra samhällssektorer.

AI vid personuppgiftsbehandling i brottsbekämpningen

I takt med den tekniska utvecklingen ökar trycket på att få använda mer avancerade former av AI som en hjälp i de brottsbekämpande myndigheternas analys- och underrättelsearbete. I den framställan som ligger till grund för direktivet till den senast beslutade utredningen på området – Säkerhetspolisens informationshantering[4]– framhåller Säkerhetspolisen att det inte längre är möjligt att manuellt granska och strukturera uppgifter på grund av den enorma mängd information som kan vara av intresse för myndighetens verksamhet. För att kunna utnyttja den information som finns tillgänglig – framför allt i öppna källor – på ett effektivt sätt menar Säkerhetspolisen att de behöver rättsliga förutsättningar för att samla in stora mängder data på exempelvis sociala medier

[3] 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).

[4] Dir. 2023:64, Ju 2023:02.

och göra analyser med hjälp av automatiska processer. Utredningen ska lämna förslag som gör att information kan hanteras av Säkerhetspolisen på ett mer ändamålsenligt sätt än idag, och ska också beakta att tillsynsmyndigheterna ska ges förutsättningar att kunna fullgöra sin uppgift att utöva tillsyn över personuppgiftsbehandlingen på ett effektivt sätt.

Så kallad bulkinsamling av uppgifter aktualiserar svåra frågeställningar som rör nödvändighet, proportionalitet och kravet på behandling för bestämda ändamål. Oavsett var den ovan nämnda utredningen landar är den sannolikt inte den sista som rör förutsättningarna för myndigheters bulkinsamling och användning av AI vid behandling av personuppgifter. Liknande möjligheter för säkerhetstjänsterna i andra europeiska länder, till exempel i Norge, är i olika stadier av uppbyggnad[5]. Tekniken finns och samhällsintresset av att kunna använda den även inom annan brottsbekämpning är naturligtvis mycket stort.

Elektronisk åtkomst som en förutsättning för effektiv dataskyddstillsyn

Det man kan konstatera är att användningen av AI förändrar förutsättningarna för tillsynen på dataskyddsområdet. Om de brottsbekämpande myndigheterna får möjlighet att genom automatiska processer analysera och dra slutsatser från stora mängder ostrukturerad data är det otillräckligt med tillsyn enbart baserad på frågor om behandling i det enskilda fallet eller avseende viss person. Metoder som stickprov och tillsyn efter anmälan behöver kompletteras av annan typ av tillsyn för att säkerställa ett sådant effektivt skydd mot otillåtna intrång i den personliga integriteten som förutsätts i dataskyddsregleringen. Om myndigheters behandling av personuppgifter tillåts röra sig mot insamling av stora mängder data utan något på förhand definierat insamlingsändamål, och de avgränsningar och sökningar som görs inte styrs av människor utan av algoritmer, behöver tillsynen anpassas. Tillsynsmyndigheterna behöver dels verktyg och kompetens för att kunna granska själva programvarans algoritmer, och dels kunna använda sig av egna AI-verktyg för att effektivt göra urval och analysera innehållet i de lagrade personuppgifterna. En metod som framstår som allt mer nödvändig för att leva upp till kraven på effektiv, självständig tillsyn är att tillsynsmyndigheterna får tillgång till de granskade systemen för att med hjälp av sin egen tekniska kompetens självständigt kunna testa sökmöjligheter och granska själva förutsättningarna för behandlingen.

[5] Prop. 31 L (2022–2023), Endringer i politiloven og politiregisterloven (PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon).

Idag sker en utveckling hos Säkerhets- och integritetsskyddsnämndens motsvarigheter i andra europeiska länder, t ex Norge, Danmark och Nederländerna, där myndigheterna har gått från en organisation med i princip enbart jurister till en där teknikerna är ungefär lika många. Flera tillsynsmyndigheter har någon form av direkt åtkomst till de granskade myndigheternas system och möjlighet att relativt fritt göra sökningar. I Sverige har vi dock ett oklart rättsläge som försvårar utvecklingen av nya effektiva metoder för tillsyn. Som på många andra områden skapar regleringen i tryckfrihetsförordningen om allmänna handlingar stora utmaningar när den ska tillämpas i en digital miljö. I detta fall är det avsaknaden av en tydlig definition av direktåtkomst, tolkningen av begreppet ”förvarad” i 2 kap. 6 § tryckfrihetsförordningen och de konsekvenser det får i dataskyddstillsynen som står i fokus.

Rättsliga konsekvenser av direktåtkomst

Direktåtkomst är ett nödvändigt verktyg för många myndigheter idag och samtidigt svårreglerat i relation till regleringen om allmänna handlingar och skyddet av personuppgifter. En rättslig konsekvens av att elektronisk åtkomst definieras som direktåtkomst är att de upptagningar som åtkomsten omfattar hos den utlämnande myndigheten blir expedierade i den mening som avses i tryckfrihetsförordningen redan i och med att åtkomsten etablerats, dvs. i den stund då upptagningarna är tekniskt tillgängliga för den mottagande myndigheten så att de kan läsas, avlyssnas eller på annat sätt uppfattas. Att en expediering sker innebär att handlingarna är att anse som allmänna både hos den utlämnande och mottagande myndigheten. Huruvida den mottagande myndigheten genom någon åtgärd faktiskt har använt sig av direktåtkomsten har ingen betydelse, och inte heller i vilken omfattning. Genom att åtkomsten etablerats är alla handlingar som omfattas av direktåtkomsten alltså också att anse som inkomna till och förvarade hos den mottagande myndigheten.[6] Direktåtkomsten kan också aktualisera svårbedömda frågor om sekretess hos den mottagande myndigheten. För att lindra de konsekvenser ur integritetssynpunkt som direktåtkomsten föranleder omfattas så kallad överskottsinformation vid direktåtkomst av sekretess enligt 11 kap. 4 § offentlighets- och sekretesslagen (2009:400). En förutsättning är att uppgiften är sekretessreglerad hos den utlämnande myndigheten. I 11 kap. 8 § samma lag anges att om det finns primära

[6] SOU 2015:3 s. 139.

sekretessbestämmelser hos den mottagande myndigheten som är tillämpliga hos den mottagande myndigheten ska dessa tillämpas istället.

Som sekretessregleringen för uppgifter som omfattas av direktåtkomst ser ut idag blir bedömningen av vilka uppgifter som är sekretessbelagda allt annat än självklar exempelvis om åtkomsten avser stora mängder data som initialt inhämtats från öppna källor men sedan lagras och bearbetas hos en brottsbekämpande myndighet. Detta gäller särskilt, som för Säkerhets- och integritetsskyddsnämndens del, när uppgifter inhämtade i tillsynsverksamheten enbart omfattas av överförd – sekundär – sekretess. En dataskyddstillsyn som riskerar att bedömas som direktåtkomst innebär idag alltså ett oklart, och riskfyllt läge, inte minst när det gäller information som är känslig både för tillsynsobjekten och för de personer uppgifterna rör.

Definitionen av direktåtkomst

När är det då frågan om direktåtkomst? Begreppet förekommer i många registerförfattningar liksom i offentlighets- och sekretesslagen,[7] men saknar legaldefinition. I förarbetsuttalanden kan utläsas att med direktåtkomst avses vanligtvis att någon har direkt tillgång till någon annans register eller databas och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen. I begreppet ligger också att den som är personuppgiftsansvarig för databasen eller registret inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst söktillfälle tar del av.[8]

Ett visst tydliggörande av vad som avses med direktåtkomst gavs i Högsta förvaltningsdomstolens avgörande i det så kallade LEFI Online-målet (HFD 2015 ref. 61), där domstolen prövade vad som är direktåtkomst i socialförsäkringsbalkens mening. I målet var frågan om socialnämnder hade direktåtkomst till Försäkringskassans socialförsäkringsdatabas. Domstolen ansåg att det avgörande för om direktåtkomst kunde anses föreligga var om upptagningen redan i och med möjligheten att ta del av den kunde anses förvarad hos den mottagande myndigheten i den mening som avses i nuvarande 2 kap. 6 § tryckfrihetsförordningen. Socialnämnderna kunde inte på egen hand söka information i databasen, utan ett utlämnande förutsatte att Försäkringskassan reagerade på en begäran om att de efterfrågade uppgifterna skulle lämnas ut. Domstolen menade

[7] Se exempelvis 3 kap. 7 § lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område och rubriken till 11 kap. 4 § offentlighets- och sekretesslagen (2009:400).

[8] Se exempelvis prop. 2011/12:45 s. 133 och prop. 2017/18:269 s. 370.

att Försäkringskassan därigenom förfogade över frågan om och i så fall vilka uppgifter som kunde lämnas ut och att socialnämnderna därför inte hade sådan teknisk tillgång till upptagningar som avses i 2 kap. 6 § tryckfrihetsförordningen. Domstolen ansåg därmed inte att förfarandet var att betrakta som direktåtkomst.

Direktåtkomst vid tillsyn

Dåvarande Datainspektionen, numera Integritetsskyddsmyndigheten, har i yttrande den 19 februari 2013 (dnr 126-2013) lämnat vägledning till Inspektionen för socialförsäkringen om direktåtkomst i Pensionsmyndighetens ärendehanteringssystem, alltså en tillsynssituation. Datainspektionen uttalade sig utifrån ett antal förfaranden eller scenarier som på olika sätt innebar att den granskade myndigheten reagerade på en begäran om utlämnande av uppgifter i vissa ärenden med tekniska säkerhetsåtgärder som loggning och sökspärrar som avgränsade åtkomsten till de uppgifter som omfattades av begäran. Datainspektionen bedömde att förfarandet i samtliga fall trots dessa åtgärder innebar direktåtkomst.

Datainspektionens vägledning tycks innebära en betydligt vidare tolkning av begreppet direktåtkomst än den Högsta förvaltningsdomstolen tillämpade i LEFI-onlinemålet och får förutsättas vara överspelad genom Högsta förvaltningsdomstolens avgörande. Datainspektionens yttrande skapade ett osäkert rättsläge och har tolkats som att de granskade myndigheterna i praktiken alltid behövde delta vid inspektioner och i viss mån också ha möjlighet att styra granskningen.

LEFI-onlinemålet leder till bedömningen att gällande rätt i vart fall tillåter att tillsynsmyndigheten ges elektronisk tillgång till uppgifter efter en begäran som förutsätter en reaktion från den myndighet som tillsynas, utan att tillgången anses vara en direktåtkomst med de rättsliga följder detta har. Avgörandet ger dock ingen direkt ledning när det gäller hur den reaktion som krävs från den utlämnande myndigheten ska ordnas tekniskt för att effektivt utesluta att utlämnandet anses utgöra direktåtkomst, eller var gränsen går för hur stor en begäran får vara. Skulle en begäran från en tillsynsmyndighet kunna omfatta ett helt system inklusive programvarans algoritmer?

Avslutande reflektioner

Det kan ifrågasättas om den befintliga svenska regleringen lever upp till kraven på att medlemsstaterna ska säkerställa tekniska förutsättningar för oberoende och effektiv tillsyn i den europeiska dataskyddsregleringen. Detta kommer att bli alltmer påtagligt i och med ökad användning av så kallad bulkinhämtning och AI hos svenska myndigheter – inte minst inom brottsbekämpningen.

En lösning som möjliggör mer effektiv tillsyn redan under dagens regelverk är tydligare kravställning från myndigheter när nya it-system upphandlas eller byggs upp. Ett självklart inslag i nya system hos myndigheter som behandlar personuppgifter bör vara en tillsynsfunktion som tillåter elektronisk åtkomst till på förhand avgränsade delar av systemen där åtgärder som sökningar och urval loggas och hålls åtskilda från systemet i stort. En sådan funktion behöver utformas i nära samråd mellan tekniker och jurister och efter en tolkning av LEFI-onlinedomen. Att nya system anpassas eller byggs med effektiv tillsyn i åtanke borde ses som en del i det inbyggda dataskydd som krävs enligt EU:s dataskyddsreglering eller i vart fall en följd av skyldigheten för tillsynsobjekten att kunna visa efterlevnad av dataskyddsregleringen, och bör vara en prioriterad fråga för Integritetsskyddsmyndigheten vid exempelvis förhandssamråd.

Vi behöver samtidigt hitta mer långsiktiga lösningar på det problem som presenteras här. Informationshanteringsutredningen övervägde möjliga lösningar i delbetänkandet Överskottsinformation vid direktåtkomst, SOU 2012:90. Utredningen analyserade möjligheterna för att undanta överskottsinformation vid direktåtkomst från att vara allmänna handlingar hos mottagarmyndigheten. Utredningen kom fram till att det skulle vara förenat med stora avgränsnings- och tillämpningssvårigheter att införa ett sådant särskilt undantag i tryckfrihetsförordningen, och föreslog istället ändringar i offentlighets- och sekretesslagen. Utredningen förordade att den grundläggande konstruktionen av vad som utgör en handling i elektronisk miljö skulle ses över i ett bredare sammanhang. Inget av förslagen har blivit verklighet. Det är av många skäl hög tid att en sådan utredning tillsätts. Det problem jag har diskuterat i den här artikeln är ett. Det osäkra rättsläget bidrar till en försvagad och mindre relevant tillsyn. Rättsläget bör klargöras i takt med att myndigheters möjligheter att behandla personuppgifter med hjälp av AI ökar.