Sammanfattning av IMY´s integritetsskydds-rapport 2020

I januari 2021 lämnade Integritetsskyddsmyndigheten (tidigare Datainspektionen), IMY, över sin första integritetsskyddsrapport till regeringen. Rapporten är en del av IMY:s nya uppdrag att vart fjärde år lämna en redovisning av utvecklingen inom dataskyddsområdet till regeringen. IMY:s slutsats är att Sveriges ambitiösa digitaliseringspolitik behöver kompletteras med en tydlig och konkret integritetsskyddspolitik. I denna sammanfattning har Ciso i Vaggeryds Kommun tagit delar av rapporten och sammanfattat några av de viktigaste punkterna som IMY lyfter fram i sin rapport.

DIGITALISERINGSPOLITIKEN I EU OCH SVERIGE

I IMY´s rapport lyfts det fram att både EU och Sverige har en hög ambitionsnivå avseende tillvaratagande av digitaliseringsmöjligheter och digitaliseringspolitiken är högt upp på agendan. I Sverige har vi den nationella digitaliseringsstrategi och en nationell inriktning för AI. Inom EU märks det bland annat genom att det i februari 2020 presenterades flera strategiska dokument som anger inriktningen för EU:s digitala framtid: EU:s digitaliseringsstrategi, datastrategi och vitbok för AI.

VIKTIGA INITIATIV INOM EU - ETT ÖKAT SKYDD FÖR PERSONUPPGIFTER

För att möta den snabba tekniska utvecklingen och ökande insamlingen och delningen av personuppgifter infördes dataskydds-förordningen (GDPR) den 25 maj 2018. Genom den stärktes de enskildas rättigheter samtidigt som skyldigheterna för de verksamheter som

hanterar personuppgifter skärptes. Ett direktiv på det brottsbekämpande området, implementerades också i svensk rätt genom brottsdatalagen och brottsdataförordningen som trädde i kraft under 2018.

Genom dataskyddsförordningen inrättades också den Europeiska dataskyddsstyrelsen, EDPB. Styrelsen beslutar om yttranden och vägledningar men har även mandat att fatta beslut i gränsöverskridande ärenden.

Sedan GDPR trädde i kraft har EU-domstolen meddelat ett tiotal domar rörande integritetsskydd. I rapporten ges en kortfattad beskrivning av den praxis som hittills utvecklats. Rapporten tar bland annat upp EU-domstolens underkännande av Privacy Shield, målet där EU-domstolen klargör vad som gäller vid överföring av personuppgifter till tredje land (Schrems II).

DIGITALISERING OCH TEKNIKUTVECKLING

I rapporten beskriver IMY sexton olika teknikutvecklingsområden som tillsammans bidrar till utveckling och Sveriges förmåga att ta tillvara digitaliseringens möjligheter, men som samtidigt haft stor betydelse för den personliga integriteten.

Teknikutvecklingsområdena presenteras utifrån de olika sätt personuppgifter kan behandlas på (utifrån personuppgifternas livscykel).

TEKNIK FÖR ATT SAMLA IN DATA

Stora mängder data ger omfattande affärsmöjligheter vilket har skapat starka incitament för att utveckla teknik för att samla in data. Den ökande insamlingen av data om vårt beteende och rörelsemönster, dels på nätet, dels i den fysiska världen har påverkat och kommer även framöver att påverka den personliga integriteten. Ny teknik för att samla in data ger en mängd aktörer tillgång till en fullständig bild av våra liv, våra intressen, våra kontakter, vår hälsa, våra rörelsemönster, vanor och beteenden.

Risker för den enskilde individen med den ökande datainsamlingen handlar bland annat om att det blir allt svårare att upptäcka, kontrollera eller välja bort att data om oss samlas in. Det faktum att uppgifter delas mellan olika aktörer på ett sätt som ofta är svåröverblickbart både för den enskilde individen och för verksamheterna som delar data gör integritetsriskerna större. Det finns också en risk för ändamålsglidning, det vill säga att uppgifterna används för andra ändamål än de ursprungligen samlats in för.

Sensorer och sändare

Ett teknikutvecklingsområde som lyfts fram i den här delen är sensorer och sändare, Som exempel kan nämnas kroppsnära teknik som pulsklockor och träningsarmband och geospatial teknik för positioneringsdata.

Nya former för interaktion mellan människa och dator

På kort tid har röststyrningsteknik fått ett brett genomslag och spridits från mobiltelefoner och datorer till bland annat bilar, klockor, hörlurar och olika smarta prylar i hemmet som till exempel TV-apparater.

Internet of things (IoT)

Utvecklingen inom Internet of things, IoT, utgör ett särskilt riskområde ur ett integritets-perspektiv. IoT avser apparater, maskiner och fordon som har inbyggd teknik och internetuppkoppling, men typiskt sett inte ses som datorer. Det kan vara vardagsföremål som vitvaror, termostater, belysning, TV-apparater, elektroniska lås och larm, kläder eller bilar, men också utrustning i industri, infrastruktur eller vården. Utvecklingen går mot att IoT används inom allt fler samhällsområden och på allt fler geografiska platser för att samla in data. En stor andel IoT-enheter har visat sig ha bristande säkerhet. Forskare har till exempel visat hur man kan ta kontroll över en modern bil via ett trådlöst nät, eller via fjärrstyrning manipulera en pacemaker eller insulinpump.

Webbskrapning

Med teknik för webbskrapning som kombineras med artificiell intelligens, AI, är det förhållandevis enkelt att samla in och bearbeta mycket stora informationsmängder från nätet, exempelvis från sociala medier. Kännetecknande är ofta att informationsmängderna blir så stora att det blir oöverblickbart och kräver AI-teknik för bearbetning.

Biometrisk data

En särskild typ av datainsamling som i ökande utsträckning används inom allt fler samhällsområden handlar om insamling av biometriska uppgifter. Biometri innebär att mäta kroppens egenskaper (till exempel hand- eller fingeravtryck, mönster i ögats iris, ansikts- eller kroppsform och röstavtryck) eller individers beteenden (till exempel gångstil, rörelse- och talmönster, handstil, ansiktsuttryck och sömnmönster) för att verifiera, autentisera eller identifiera individer. Användning av biometriska uppgifter kan skapa ökad bekvämlighet, snabbhet och säkerhet. Samtidigt medför den ökande användningen av biometriska uppgifter betydande integritetsrisker. En av de främsta riskerna handlar om att biometriska data (till skillnad från till exempel lösenord eller passerkort) inte kan bytas ut om uppgifterna skulle hamna i orätta händer. De biometriska uppgifterna är beständiga, vilket gör en integritetsförlust svår att reparera.

TEKNIK FÖR ATT BEARBETA OCH ANALYSERA DATA

De ökade möjligheterna att samla in data skulle i praktiken vara värdelösa om inte tekniken för att bearbeta och använda uppgifterna också tagit stora utvecklingssprång.

AI – artificiell intelligens
Utvecklingen av artificiell intelligens (AI) har haft avgörande påverkan på den personliga integriteten under de senaste åren. De möjliga nyttorna med AI är stora och den outnyttjade potentialen fortfarande stor. I dagsläget uppges ungefär fem procent av svenska företag och tio procent i offentlig sektor använda AI i sina verksamheter.
Samtidigt innebär AI integritetsrisker för den enskilde i form av bland annat bristande transparens, diskriminering, försvårat ansvarsutkrävande, missbruk och fientlig användning. Särskilda risker finns vid automatiserade processer i beslutsfattande, när ett beslut kan få stora konsekvenser för den enskilde.

Riskområde -Digitala annonsmarknaden
De komplexa och icke transparenta processerna som kan inkludera hundratals aktörer inom den digitala annonsmarknaden gör det i praktiken omöjligt för den enskilde att utnyttja sina rättigheter, till exempel att få information raderad. Affärsmodellerna gör det i praktiken också mycket svårt för företagen att ha kontroll och uppfylla sina skyldigheter när det gäller enskildas rättigheter. Såväl norska som brittiska myndigheter har i färska analyser kommit till slutsatsen att stora delar av den digitala annonsmarknaden systematiskt bryter mot dataskyddslagstiftningen.

TEKNIK FÖR ATT LAGRA DATA

För att kunna utnyttja fördelarna med insamling av stora mängder data och tekniken för att bearbeta och använda data behövs lämpliga lagringsmöjligheter. Utifrån detta lyfter IMY fram teknikutvecklingsområdena molnlagring och edge storage. En utmaning med bearbetning eller lagring i molntjänster är att marknaden för molntjänster idag domineras av amerikanska aktörer vilket kan medföra att lagringen, efter EU-domstolens avgörande i juli 2020 i det så kallade Schrems II-målet, inte är laglig.

Edge computing
Ett utvecklingsområde som kan innebära fördelar ur ett integritetsperspektiv handlar om var data bearbetas – i centrala datacentra och serverhallar eller lokalt. Teknik för edge computing medför att bearbetning av data nu allt oftare kan ske lokalt, i uppkopplade enheter med låg kapacitet eller i lokala servrar. Detta innebär att data i mindre utsträckning behöver transporteras och delas, vilket kan skapa bättre kontroll. Med utvecklingen inom IoT ökar också behovet av lagring och säkring direkt i enheterna utan att behöva transportera data i nätet. Sådan teknik benämns ofta edge storage och edge security, det vill säga att personuppgifter kan lagras och säkras direkt i de lokala enheter där de samlas in, exempelvis i en privatpersons smarta mobiltelefon.

TEKNIK FÖR ATT TRANSPORTERA DATA

Den stora mängden insamlad data och förmågan att bearbeta och använda denna data ställer inte bara krav på lagringsmöjligheter utan också på teknik för att transportera stora datamängder. I denna del lyfter IMY fram 5G och andra former av digital kommunikationsteknik.

5G är nästa generation av mobila nätverk med extremt hög kapacitet för att transportera data. För EU-kommissionen är utvecklingen mot 6G redan en prioriterad fråga. Ett centralt användningsområde för 5G och 6G kommer att vara IoT med till exempel uppkopplade enheter i industrin och i smarta städer. En integritetsrisk kopplat till 5G handlar om att geografisk positionering kommer vara möjligt med mycket med större precision än idag. Ett annat exempel på integritetsrisker som 5G medför är kopplat till en ökad insamling av högupplöst bildmaterial. Möjligheten att utan fördröjning överföra stora mängder högupplösta bilder kommer sannolikt utgöra en pådrivande faktor för en ökad direkt och indirekt insamling av biometrisk data.

Andra former av digital kommunikationsteknik som utvecklas tar sikte på kommunikation på nära avstånd, till exempel mellan enheter i ett och samma rum eller i chip som kan monteras i prislappar.

TEKNIK FÖR ATT SÄKRA DATA

Teknik för att säkra data behövs under hela livscykeln och den sammanlagda teknikutvecklingen har medfört ökade krav på digitala säkerhetslösningar. I rapporten diskuteras AI-baserad säkerhetsteknik och edge security, krypteringsteknik och blockkedjor som exempel på teknikutvecklingsområden vilka kan användas för att stärka integritetsskyddet.

TEKNIK FÖR ATT FÖRSTÖRA DATA

Teknik för att förstöra data skiljer sig från de andra delarna av personuppgifternas livscykel. Medan teknikutvecklingen inom övriga områden har drivit på varandra har utvecklingen av teknik för att förstöra data snarare gått i motsatt riktning. Genom att lagringskapaciteten har ökat har incitamenten för att förstöra data minskat. Det teknikutvecklingsområde som lyfts fram i den här delen av rapporten handlar istället om teknik för att återskapa raderad eller på annat sätt förlorad data.

DEN EXPONENTIELLA TEKNIKUTVECKLINGEN

IMY framhåller vid upprepade tillfällen i rapporten den snabba teknikutvecklingen. IMY poängterar att många av de teknikutvecklingsområden som beskrivs i rapporten utvecklas exponentiellt och att utvecklingen de kommande 100 åren, på grund av detta, kommer att motsvara 20 000 år av teknikutveckling. IMY påpekar också att de olika teknikutvecklingsområdena hänger ihop och påverkar varandra. Exempelvis har den ökade insamlingen av biometriska uppgifter i stor utsträckning möjliggjorts och påskyndats av utvecklingen inom till exempel IoT, sensorer och sändare, AI och big data och molnifiering av lagring.

INTEGRITETSSKYDDET IDAG – OCH I FRAMTIDEN

I rapporten diskuteras också vilken nivå integritetsskyddet har idag. IMY:s bedömning är att det generellt finns stora brister av grundläggande karaktär hos många verksamheter i samhället.

De närmare 500 sanktionsavgifter som hittills utfärdats inom EU visar att de vanligaste överträdelserna handlar om att de grundläggande principerna inte följs, att rättslig grund för behandlingen saknas, att enskildas rättigheter inte hanteras som de ska eller att säkerhetsåtgärderna varit otillräckliga. Av de drygt 11 000 personuppgiftsincidenter som anmälts till myndigheten beror majoriteten av fallen på den mänskliga faktorn, vilket betyder att det finns ett behov av mer och bättre utbildning för att öka kunskapen hos medarbetare. I rapporten presenteras att grundläggande kunskap om dataskyddsförordningen hos medborgarna är bra och att de flesta vet att personuppgifter används men att få vet hur personuppgifterna används, vilket har lett till att oron för hur uppgifterna används har ökat hos befolkningen.

AVSLUTANDE KOMMENTAR

I rapporten dras tre huvudsakliga slutsatser. För det första har människor idag viss kunskap om att data samlas in, men inte i vilken utsträckning det görs. Detta kan för många leda till en känsla av otrygghet. För det andra innebär utvecklingen med IoT att datainsamling och personuppgifts-hantering flyttar in i människors hem, vilket gör det ännu viktigare att hanteringen sker på ett lagligt sätt. För det tredje innebär den ökade insamlingen av biometrisk data att det krävs särskilda insatser för att öka säkerheten avseende användandet av sådana uppgifter. IMY pekar på vikten av att man tidigt i lagstiftningsarbetet gör en ingående integritetsskyddsanalys. Ju mer genomarbetad nationell lagstiftning som kompletterar dataskyddsförordningen är, desto enklare blir det för företag, myndigheter och andra organisationer att tolka och tillämpa dataskyddsreglerna. Vi får då också en lagstiftning som är homogen och heltäckande och ger verksamheterna det stöd de behöver för sin personuppgiftshantering.

//Annika Lagerqvist
Ciso, Vaggeryds Kommun