IMY. Integritetsskydds myndigheten

Integritet och ny teknik 2020–2024

Redovisning av Integritetsskyddsmyndighetens uppdrag att följa, analysera och beskriva utvecklingen

Diarienummer
IMY-2024-2570

Datum
2025-01-28

IMY. Integritet och ny teknik 2020–2024.
Har du frågor om innehållet kontakta Integritetsskyddsmyndigheten,
telefon 08-657 61 00, e-post imy@imy.se,
eller besök www.imy.se

Förord

Integritetsskyddsmyndigheten (IMY) har fått i uppdrag av regeringen att följa, analysera och beskriva utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik. Vart fjärde år ska vi lämna en redovisning av utvecklingen på området till regeringen. Detta är vår redovisning för perioden 2020–2024.

Det finns många sätt att öka integritetsskyddet i samhället utan att det hämmar teknisk och ekonomisk utveckling eller utgör ett hinder mot ökad effektivitet. IMY är övertygad om att det är möjligt – och att det är den enda framkomliga vägen – att hela samhället arbetar för integritetsvänlig innovation och en hållbar digital framtid. Det tjänar vi helt enkelt alla på. I denna rapport kommer IMY därför till tre slutsatser:

- Vi vill se ett ökat fokus på integritetsvänlig teknik, genom att främja och utveckla integritetsstärkande tekniker och minska den regulatoriska osäkerheten genom tydlig vägledning.

- Vi vill att det skapas mer kunskap och bättre beslutsunderlag om integritetsskydd. I rapporten framhåller vi särskilt behovet av att utreda hur integritetsskyddet påverkas av den alltmer omfattande övervakningen på brottsbekämpningsområdet och i arbetslivet.

- Slutligen menar vi att tiden är mogen för att det genomförs en översyn av dataskydds-förordningen. I Sverige finns en utbredd uppfattning att dataskyddsförordningen är svår att tillämpa och att den skapar en stor administrativ börda, även när integritetsriskerna är små. För att säkerställa ett effektivt och balanserat skydd av den personliga integriteten behöver regleringen på området upplevas legitim. Om så inte är fallet kan det på sikt försvaga integritetsskyddet.

Tekniska framsteg kan vara svaret på många av vår samtids stora utmaningar. Tillsammans kan vi möta utmaningarna och på ett ansvarsfullt sätt bygga en hållbar digital framtid och skapa ett samhälle där vår och framtida generationers rätt till en privat sfär skyddas.

Eric Leijonram
Generaldirektör

Innehålls-förteckning

Sammanfattning

- Ny teknik och integritetsskydd är nära sammanflätade och påverkar varandra. De påverkas också av händelser och trender i samhället. Integritetsskyddet i Sverige de senaste fyra åren är under förändring. Eftersom inverkan kommer från motstående krafter både stärks och urholkas integritetsskyddet samtidigt. Under perioden 2020–2024 är det på samhällelig nivå framför allt teknikutvecklingen, pandemin, det försämrade säkerhetsläget och skiftet i svensk kriminalpolitik som har påverkat integritetsskyddet.

- Det går att förena en laglig och säker behandling av personuppgifter med innovation och teknisk utveckling. Det är sällan själva tekniken som utgör en risk eller en möjlighet, utan hur den används av människor och verksamheter.

- Takten i teknikutvecklingen, särskilt på AI-området, är snabb. I takt med att samhället anpassar sig och använder mer teknik samlas fler personuppgifter in. Dessutom införs AI, en teknik som kräver stora datamängder, i många verksamheter.

- På ett övergripande plan är en av de stora riskerna för integritetsskyddet att många verksamheter fortfarande har grundläggande brister i sitt dataskyddsarbete, vilket gör att gapet mellan teknikutvecklingen och integritetsskyddet fortsätter att öka.

- Utvecklingen på AI-området är särskilt snabb. AI skapar möjligheter till effektivare tjänster med högre kvalitet. Generativ AI, stora språkmodeller, fick stort genomslag under 2022. Det finns flera integritetsrisker kopplat till dessa. I rapporten tar vi upp till exempel hallucinationer, hur träningen går till, att modellerna kan användas på ett felaktigt sätt och att det ökar antalet deepfakes. Behovet av data till AI har också skapat en större efterfrågan av webbskrapning. Vi tar också upp frågan om AI och övervakning. Det är ett komplext område och vad som kan upplevas som ett stort integritetsintrång för någon kan vara ett värdefullt hjälpmedel för någon annan.

- Den tekniska utvecklingen innebär att biometriska data kan användas på nya sätt, till exempel för ansiktsigenkänning. Integritetsriskerna kopplade till biometriska data är stora, men eftersom även nyttorna är betydande kan det i vissa fall vara godtagbart att använda tekniken trots det intrång i den personliga integriteten som användningen innebär. Att hantera biometriska data ska alltid göras med försiktighet och hög nivå av säkerhet.

- Allt eftersom behovet att dela personuppgifter ökar så tilltar efterfrågan på integritetshöjande teknik. Tekniken kan komplettera befintligt skydd eller minska riskerna så att de blir färre eller mindre allvarliga. Integritetshöjande tekniker som tas upp i denna rapport är bland annat syntetiska data, differentiell integritet, kryptering, federerad och distribuerad analys och edge.

- På EU-nivå har fokus legat på det som kallas det digitala årtiondet, ett initiativ som syftar till att ställa om EU till en datadriven ekonomi. För att uppnå det har EU-kommissionen tagit fram omfattande ny lagstiftning på dataområdet, vilket kommer att påverka enskilda och verksamheter som behandlar personuppgifter lång tid framöver. Många verksamheter upplever en stor, och ibland innovationshämmande, regelbörda. Behovet av vägledning är stort, både i fråga om enskilda regler och helheten.

- Utvecklingen av den organiserade brottsligheten är en fråga som har präglat samhällsdebatten i Sverige i flera år. En av svårigheterna handlar om att hitta en balans mellan effektiv brottsbekämpning och respekt för den enskildes integritet. Problemet ställs ibland på sin spets när det kommer till formerna för att samla in bevisning för att förebygga, förhindra och utreda brott.

- Övervakning i arbetslivet är inte en ny fråga, men ny teknik har skapat fler och mer omfattande möjligheter till övervakning av anställda. I rapporten beskrivs tre olika former av övervakning: digital övervakning av anställda med hybrida arbetssätt, anställda vars position övervakas via GPS och anställda som övervakas med kamera för att säkerställa säkerhet, kvalitet eller minska brottslighet.

- Insamlingen och användningen av hälsodata fortsätter att öka, framför allt genom att allt fler personer använder sig av teknik för att själva samla in stora mängder hälsodata.

- Personuppgifter om barn anses särskilt skyddsvärda i dataskyddsförordningen. Det beror på att barn kan ha svårare att förutse riskerna med att lämna ifrån sig uppgifter eller att förstå vilka rättigheter de har. De flesta barn och unga lever stora delar av sina liv uppkopplade, och det kan vara svårt att få information om sig själv raderad efter att den en gång publicerats på internet.

- IMY lyfter fram tre slutsatser:

  A. Sverige bör **främja integritetsvänlig teknikutveckling**, genom att satsa på utveckling av integritetsstärkande tekniker, privacy enhancing techniques (PET), och minska regulatorisk osäkerhet genom tydlig vägledning.

  B. Det är viktigt att skapa kunskap och **bättre beslutsunderlag om integritetsskydd**. Vi vill framför allt se ett helhetsgrepp om integritetsfrågor på områden där utvecklingen har varit särskilt omfattande och snabb. Vi anser till exempel att det är svårt att urskilja det samlade integritetsintrånget som förändringarna av lagstiftningen på brottsbekämpningsområdet medför. Regeringen bör därför tillsätta en utredning med uppdrag att göra en översyn av åtgärderna och deras samlade effekter för den personliga integriteten. Av samma skäl behövs en kartläggning av hur övervakningen i arbetslivet har förändrats under de senaste åren.

  C. Vi är medvetna om att den regulatoriska bördan och osäkerheten upplevs vara hämmande för just konkurrenskraft och tillväxt. Röster har därför rests om en översyn av dataskyddsförordningen, i synnerhet från näringslivet. Men även många kommuner och statliga myndigheter uttrycker att det finns en osäkerhet som leder till en försiktig och mycket strikt tillämpning som motverkar innovation. IMY ser därför ett behov av en **översyn av dataskyddsförordningen**, i syfte att säkerställa att regleringen uppfattas som legitim och ger ett robust integritetsskydd där riskerna är som störst. IMY efterlyser också ett **mer snabbrörligt lagstiftningsarbete** för att ta om hand de regleringsbehov som uppkommer med anledning av teknikutvecklingen, digitaliseringen och det digitala årtiondet.

1. IMY:s bedömning och slutsatser

Rätten till personlig integritet innebär att alla människor har rätt till ett privatliv, en sfär där det går att ha privata tankar och kommunicera förtroligt med andra utan att bli kartlagd, spårad eller övervakad. Rätten till personlig integritet är en grundläggande rättighet, men den är inte absolut. Den kan begränsas om det är motiverat av till exempel viktiga allmänna intressen som brottsbekämpning eller andra fri- och rättigheter som yttrandefriheten.

Vår personliga integritet påverkas mycket av samhällets digitalisering och den snabba teknikutvecklingen, men även av samhällsförändringar som ökad gängkriminalitet och ett försämrat säkerhetspolitiskt omvärldsläge. Den ökande insamlingen av data om våra beteenden och rörelsemönster, både på nätet och i den fysiska världen, skapar stora risker ur ett integritetsskyddsperspektiv. Med hjälp av de digitala spår som vi lämnar efter oss kan man lätt skapa en fullständig bild av våra intressen, åsikter och kontakter, våra rörelsemönster, ekonomiska förhållanden, vanor och beteenden samt om vår hälsa. Få saker är så privata att de är dolda för en algoritm.

Vi lever i en tid av snabb teknisk utveckling där det görs stora framsteg inom avancerad teknik. Teknikutveckling kan vara svaret på många av vår samtids stora utmaningar, som hur vi ska behålla och utveckla välfärden, hur vi ska säkerställa ett säkert och tryggt samhälle och hur vi ska hantera klimatförändringarna. För att den digitala omställningen ska vara hållbar måste den dock ske på ett lagligt och etiskt sätt. För vår egen och för kommande generationers skull är det viktigt att vi inte bygger ett samhälle som innebär att vår privata sfär försvinner. I ett digitalt samhälle är självbestämmande centralt för den personliga integriteten, det vill säga att kunna kontrollera eller få insyn i uppgifter som rör en själv, vem som använder uppgifterna och varför.

1.1. IMY:s bedömning

- Integritetsskyddet i Sverige de senaste fyra åren är under förändring och påverkas av många olika motstående krafter, vilket innebär att det både **stärks och urholkas samtidigt**.

- På ett övergripande plan är en av de största riskerna för integritetsskyddet fortfarande att många verksamheter har **brister i sitt grundläggande dataskyddsarbete**, vilket gör att gapet mellan teknikutvecklingen och integritetsskyddet fortsätter att öka.

- Omvärldsläget har lett till fler och mer omfattande cyberattacker. Skyddet av informationstillgångar och förmågan att stå emot riktade angrepp är centralt både för enskilda verksamheter och för samhällsviktiga funktioner. **Data- och integritetsskyddsfrågorna behöver tydligare kopplas ihop med informations- och cybersäkerhetsområdena**. Områdenas krav på tekniska och organisatoriska säkerhetsåtgärder kan tillsammans verka för att stärka robusthet och resiliens i samhället.

- **Ny lagstiftning, både i EU och Sverige, påverkar integritetsskyddet**. Viss lagstiftning skyddar och främjar integritet, medan annan möjliggör utökad övervakning och omfattande personuppgiftsbehandling. I Sverige har det samhälleliga samtalet präglats av frågan om hur den organiserade brottsligheten ska bekämpas och av diskussioner om hur en effektiv brottsbekämpning kan balanseras i förhållande till integritetsskyddet. Utvecklingen går mot att de brottsbekämpande myndigheterna ges möjlighet att använda teknik i större omfattning och mer effektivt, till exempel genom utökad kamerabevakning, ökad användning av biometri och DNA samt stöd av AI i det brottsbekämpande arbetet.

- På EU-nivå har det digitala årtiondet sedan 2020 producerat många omfattande rättsakter som ska skapa förutsättningar för en inre marknad av data som respekterar de grundläggande värderingar som EU bygger på. Det byggs upp ett omfattande och komplext regelverk som bland annat fokuserar på säkerhet, konkurrenskraft och rättigheter. Många upplever en stor, och ibland innovationshämmande, regelbörda. **Behovet av vägledning är stort**, både i fråga om enskilda regler och helheten.

1.2. Slutsatser

A. Främja integritetsvänlig teknikutveckling

Det finns många sätt att öka integritetsskyddet i samhället utan att det hämmar utveckling eller effektivitet. IMY är övertygad om att det är möjligt – och att det är den enda framkomliga vägen – att hela samhället arbetar för integritetsvänlig innovation och en hållbar digital framtid där våra barns och barnbarns rätt och möjlighet att ha ett privatliv skyddas. Det tjänar vi alla på.

A.1. IMY anser, liksom AI-kommissionen[1], att Sverige bör satsa på forskning och utveckling av integritetsstärkande tekniker (privacy enhancing techniques, PET). IMY rekommenderar att regeringen stärker finansieringen av forskning och utveckling av integritetshöjande teknik. IMY:s bedömning är att Sverige genom att stödja forskning inom dessa områden kan stärka konkurrenskraften och bidra till en säkrare digital miljö både i Sverige och globalt.

A.2. Behovet av vägledning om integritetsvänlig utveckling är mycket stort. Regulatorisk osäkerhet har en hämmande effekt på innovation och investeringar, och därmed även på konkurrenskraften. Det är särskilt utmanande när det gäller ny teknik, eftersom det ofta saknas praxis att luta sig emot. Det är viktigt att berörda myndigheter ger samordnad vägledning för att främja innovation och utveckling. Det gemensamma målet bör vara att genom nära samverkan och med hög grad av transparens underlätta för andra att göra rätt. Vägledningen behöver tas fram i dialog med berörda aktörer och branscher för att säkerställa att den möter de behov som finns. Det finns ett särskilt stort behov av vägledning när det gäller rättsakterna i det digitala årtiondet.

B. Skapa kunskap och bättre beslutsunderlag om integritetsskydd

I en tid av exponentiell teknikutveckling, omfattande lagstiftningsaktivitet och stort informationsflöde är det svårt att se helhetsbilder och ta stora perspektiv på komplexa frågor. IMY önskar därför att det tas ett helhetsgrepp om integritetsfrågor på områden där utvecklingen är omfattande och snabb. På så sätt skapas bättre förutsättningar för regering och riksdag att fatta beslut på kunskapsbaserad grund.

B.1. IMY anser, liksom Lagrådet[2] och Justitiekanslern[3], att det är svårt att se de samlade integritetsintrången som förändringarna av lagstiftningen på brottsbekämpningsområdet medför. Regeringen bör tillsätta en utredning med uppdrag att göra en översyn av åtgärderna och deras samlade effekter för den personliga integriteten. En sådan översyn är också viktig för att utvärdera om åtgärderna gett det förväntade resultatet och om det integritetsintrång de medför fortfarande kan motiveras.

B.2. Regeringen bör tillsätta en utredning med uppdraget att kartlägga, analysera och beskriva hur övervakningen i arbetslivet har förändrats under de senaste åren. Utredningen bör om det är lämpligt ges uppdraget att lämna författningsförslag och föreslå andra åtgärder som utredningen bedömer behövs för att motverka arbetsgivares användning av oproportionerliga övervakningsåtgärder.

1. AI-kommissionens Färdplan för Sverige
2. Lagrådets protokoll från sammanträde 2024-10-18
3. Justitiekanslern remissyttrande (2024/4010) i DS 2024:11 om bland annat biometrisk fjärridentifiering i realtid och ANPR-bevakning

C. Tiden är mogen för en översyn av dataskyddsförordningen

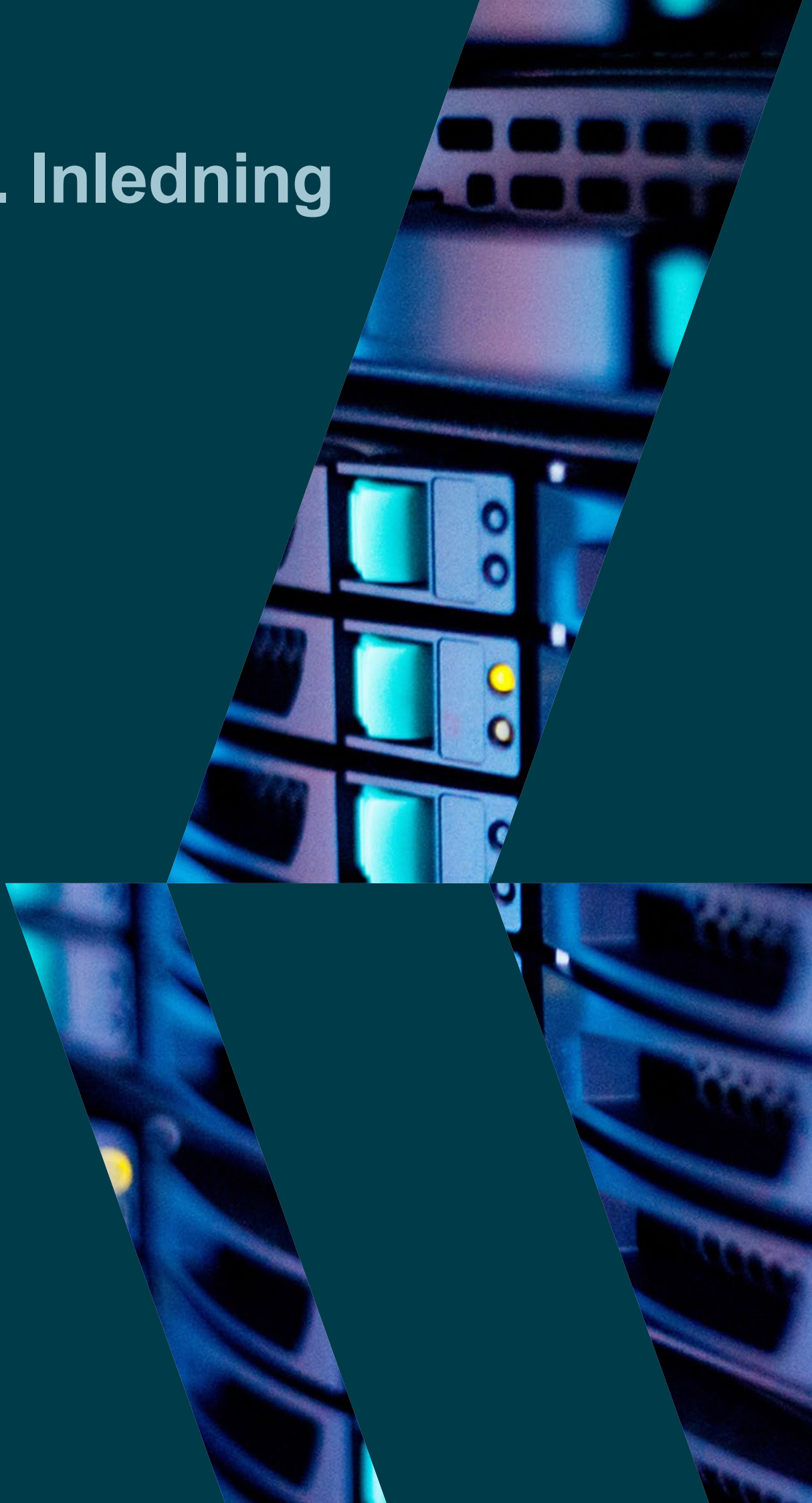
Många lagar är präglade av den samtid då de formulerades. I många fall är det inget problem, men i vissa fall skapar det onödiga hinder för användningen av ny teknik. Ambitionen bör vara att skapa teknikneutral lagstiftning som håller över tid. Teknikutvecklingen och det stora behovet av data är utmanande för det tidskrävande lagstiftningsarbetet. IMY anser dock att det går att skapa bättre förutsättningar för ett kontinuerligt lagstiftningsarbete för att ändra, uppdatera, avskaffa eller skapa nya regler som bättre passar samtidens behov.

C.1. Vi är medvetna om att den regulatoriska bördan och osäkerheten upplevs vara hämmande för konkurrenskraft och tillväxt. Röster har därför rests om en översyn av dataskyddsförordningen, i synnerhet från näringslivet. Men även många kommuner och statliga myndigheter uttrycker att det finns en osäkerhet som leder till en försiktig och mycket strikt tillämpning som motverkar innovation.

Det finns en utbredd uppfattning att dataskyddsförordningen är svår att tillämpa och att den skapar en stor administrativ börda, även när integritetsriskerna är små. Detta kan leda till att regleringen förlorar i legitimitet, vilket på sikt kan försvaga integritetsskyddet. IMY anser därför att tiden är mogen för att göra en översyn av dataskyddsförordningen i syfte att säkerställa ett effektivt och balanserat skydd av den personliga integriteten samt att regleringen uppfattas som legitim och ger ett robust integritetsskydd där riskerna är som störst.

C.2. De bestämmelser som reglerar myndigheternas personuppgiftsbehandling, de så kallade registerförfattningarna, behöver ses över. En del av regleringen kan behöva läggas på lägre författningsnivå. Eftersom en förordning kan ändras inom betydligt kortare tidsramar ger detta förutsättningar för ett mer snabbrörligt författningsarbete så att regleringen kan anpassas efter de behov som uppkommer. Ett sådant snabbrörligt författningsarbete förutsätter att Regeringskansliet har rätt resurser och kompetens för att snabbt och löpande kunna hantera de regleringsbehov som uppkommer med anledning av teknikutvecklingen, digitaliseringen och EU:s digitala årtionde.

2. Inledning



IMY har fått i uppdrag av regeringen att följa, analysera och beskriva utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik. Vart fjärde år ska IMY lämna en redovisning av utvecklingen på området till regeringen.[4]

Vi lämnade vår förra redovisning i januari 2021. I denna rapport beskriver vi de stora dragen i utvecklingen omkring integritetsskydd och teknik de senaste fyra åren. I vissa fall tar beskrivningen avstamp i samhällsfenomen, i andra fall är utgångspunkten teknik och dess användning. Rapporten gör inte anspråk på att utgöra en fullständig redogörelse för allt som hänt på teknikområdet sedan 2020. Vi tar istället fasta på konsekvenser och påverkan på integritetsområdet och gör nedslag på vissa områden. Det innebär att de tekniska beskrivningarna kan uppfattas som förenklade och summariska.

Integritetsskydd och ny teknik påverkas av varandra och av händelser och trender i samhället. I vissa fall är det aktuella frågor eller trender som driver fram teknisk utveckling, både vad gäller utveckling av ny teknik och ny användning av befintlig teknik. I andra fall kan ny teknik användas för att lösa problem eller för att effektivisera befintliga arbetssätt.

Under perioden 2020–2024 är det på samhällsnivå framför allt pandemin och det stora skiftet i svensk kriminalpolitik som har påverkat integriteten. Pandemin drev på utvecklingen av digitala möten och hybridarbete. För många har det inneburit en ökad frihet, men utvecklingen har också inneburit ökade möjligheter för arbetsgivare att övervaka sina anställda. Vad gäller brottsbekämpning ser vi hur teknik används för att öka eller effektivisera bevakning och utredning. Det finns också en ökad vilja att använda biometriska data, till exempel ansiktsbilder eller DNA.

Flera uppmärksammade cyberattacker har skett. Det nutida samhällets sårbarhet för cyberattacker diskuteras allt mer i takt med att vi blir mer och mer uppkopplade. Det får olika konsekvenser för den personliga integriteten. Uppgifterna kan säljas, spridas, stjälas eller försvinna.

Teknikutvecklingen är snabb, särskilt på AI-området. Användningen av olika tekniker innebär att insamlingen av personuppgifter ökar, datadelning förenklas, användning av uppkopplad teknik ökar och AI införs i många verksamheter.

På EU-nivå har fokus legat på det som kallas det digitala årtiondet, vilket syftar till att skapa fritt flöde för data inom EU och ställa om till en datadriven ekonomi. För att uppnå det har EU-kommissionen tagit fram omfattande ny lagstiftning på dataområdet, vilket har och kommer att påverka verksamheter som behandlar personuppgifter och enskilda lång tid framöver.

4. 2 § andra stycket förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten

3. Teknikutveckling

All teknik skapar både möjligheter och utmaningar. IMY:s bedömning är att det går att kombinera innovation och ny teknik med ett starkt integritetsskydd.

IMY har en löpande omvärldsbevakning om teknikutveckling och integritet. Det finns flera teknikområden som haft stor påverkan för den personliga integriteten 2020–2024. Att ge en beskrivning som skulle göra anspråk på att vara heltäckande är dock inte möjligt eller ens meningsfullt. Utifrån graden av integritetspåverkan väljer vi i rapporten att göra nedslag på följande områden: AI, webbskrapning, biometriska data och integritetshöjande teknik.

3.1. Artificiell intelligens

AI kan definieras på många olika sätt. Med AI avser IMY i denna rapport ett system (till exempel bestående av algoritmer och modeller) som hittar samband i data och utifrån dessa samband utför en handling, exempelvis drar slutsatser, genererar en bild, text eller tar fram ett scenario. För att hitta dessa samband krävs ofta stora datamängder. AI är därmed en dataintensiv teknik. Riskerna med AI ur ett integritetsperspektiv varierar och är beroende av vilken data den använder, hur den tränas, utvecklas och används.

AI skapar också möjligheter för oss att skydda personuppgifter på nya sätt, till exempel genom att skapa produkter och nya metoder för att lagra och dela personuppgifter på ett säkrare sätt.

3.1.1. Generativ AI

Ursprungligen användes generativ AI som ett samlingsnamn för den typ av modeller som utifrån statistisk sannolikhet använder sitt eget utfall för att åstadkomma nästa utfall, till exempel när en modell genererar text genom att ange det mest sannolika kommande ordet efter ett tidigare. Numera avses ofta även modeller som skapar ljud, bild och video. Några av de mer kända just nu är de stora språkmodellerna såsom ChatGPT, Gemini, Llama och Claude. De stora språkmodellerna fick ett betydande genomslag i november 2022. Modellerna är tränade på stora textmängder och möjliggör för användaren att interagera med modellen via chatt. Utöver dessa har också AI-modeller som genererar bilder fått stort genomslag, exempelvis Midjourney, Flux och DALL E. Dessa modeller tillhör också gruppen generativ AI, men till skillnad från de stora språkmodellerna är de text-till-bild-modeller.

Det finns flera integritetsrisker kopplade till stora språkmodeller.

- **Hallucinationer** är ett begrepp som beskriver fenomenet där en AI-modell genererar ett svar som vi kan anse felaktigt eller orimligt. En AI-modell kan lämna ett svar som den bedömt vara sannolikt utifrån den data som den tränats på. Det innebär att modellen kan förstärka stereotyper och felaktigt anklaga personer för exempelvis brott.

- Träning innebär också risk för **bias** (snedvridning) om träningsdatan inte är representativ för den population den ska avse. En modell som tränat på fördomsfulla data blir en fördomsfull modell.

- Det är viktigt att inte ha en övertro till AI-modellen och de svar som den ger, och det är nödvändigt att det finns en **mänsklig kontrollfunktion** (human-in-the-loop). Verksamheter som använder AI behöver en tydlig ansvarsstruktur och uppföljningsprocess. Ingen AI-modell kommer att fungera felfritt hela tiden. Med tiden kan modellen inge en falsk trygghet. Det är därför viktigt att medarbetare som arbetar med stöd av AI-modeller har kunskap om hur modellen fungerar och om dess förmågor och begränsningar för att undvika en övertro till modellens kapacitet.

- Det finns även integritetsrisker kopplat till **träningen av stora språkmodeller**. Att träna en AI-modell är generellt sett dataintensivt och träningen kan därmed innebära att stora mängder personuppgifter behandlas. Det kan vara svårt för den som tränar AI-modellen att veta vilka personuppgifter som finns i datan och vilka uppgifter som går att utvinna ur den. Detta gör det svårt att på ett effektivt sätt informera enskilda om att deras personuppgifter behandlas. AI har dessutom stor förmåga att återskapa information som den tränats på. Det innebär att modellen också kan läcka personuppgifter vid användning.

- Som med många produkter finns alltid en risk att användaren **använder produkten eller tjänsten på ett felaktigt sätt** eller på ett sätt som produkten inte är tänkt att användas till.

- Allt eftersom språkmodellerna blir bättre blir **interaktionen med dem mer lik den vi har med människor**. Det kan inbjuda till att använda modellerna till exempel som terapeut, för medicinsk rådgivning eller för tekniskt stöd. Denna typ av användning medför risker. En person kan dela stora mängder känsliga uppgifter om sig själv och andra. Det kan vara svårt för individen att förstå vilka konsekvenser det kan få. Råden som ges av en AI-modell är inte heller kvalitetssäkrade eller evidensbaserade.

- En **deepfake är en syntetisk framställning** av till exempel en person, i video-, bild- eller ljud-format, där personen framstår som äkta men i själva verket är syntetiskt genererad. Deepfakes används både för att sprida falsk information och för att göra underhållning. Samma teknik kan användas för olika typer av bedrägerier. Tekniken kan också användas för att skada en persons anseende eller relationer. Ett exempel på långtgående konsekvenser är ökningen av deepfakes bland barn och unga, eller när bilder från sociala medier används för att skapa AI-genererade videor med sexuellt innehåll.

3.1.2. Exempel på andra typer av AI-modeller

Det finns många andra AI-system än de stora språkmodellerna, till exempel AI som effektiviserar verksamhet eller tar över farliga arbetsmoment. Det illustrerar hur AI används i kombination med annan teknik för att fortsätta den automatisering som pågått sedan den industriella revolutionen började. Exempel på det är företaget Amazon som utökade sin automatisering med hjälp av AI-robotar och ersatte cirka 100 000 tjänster med 750 000 robotar.[5] I Sverige används robotar till exempel i gruvor för att utföra arbeten som är farliga för människor.[6]

AI används även inom forskning för att stötta med beräkningskraft och svara på komplexa frågor. Ett exempel på det är AlphaFold och Alpha Proteo från Google deepmind, vars modeller simulerar vissa biologiska processer. Modellerna används framför allt av forskare inom medicinsk forskning. Med hjälp av modellerna har forskarna lyckats förutspå hur protein viks, ett problem som forskare försökt lösa i över 50 år och som ger förbättrade möjligheter att ta fram nya och bättre läkemedel.[7]

3.1.3. AI-modeller som används för övervakning

Övervakning med hjälp av AI kan ske på många olika sätt. Med data från övervakningen kan olika AI-drivna analyser genomföras. Övervakning tar olika former och har olika syften, till exempel att bedöma anställdas produktivitet eller monitorera en patient på intensiven. Utvecklingen inom AI har gjort övervakningen effektivare, i vissa fall mer lättillgänglig, och har gjort det möjligt att övervaka sådant som tidigare varit väldigt svårt att mäta.

AI och övervakning är ett komplicerat område och vad som kan upplevas som ett stort integritetsintrång för någon kan vara ett värdefullt hjälpmedel för någon annan. Övervakning kan till exempel möjliggöra för personer med behov av tillsyn att bo ensamma eller förbättra övervakning av patienters hälsodata på intensiven och därmed möjliggöra bättre och effektivare vård.

5. www.tbsnews.net/world/global-economy/amazon-advances-automation-over-750000-robots-replacing-100000-jobs-888656 (2024-12-11)
6. www.svt.se/nyheter/lokalt/norrbotten/sa-ska-robotar-och-dronare-radda-liv-svenska-gruvor (2024-12-11)
7. www.nobelprize.org/uploads/2024/11/popular-chemistryprize2024-swedish.pdf (2024-12-11)

Det finns olika exempel på AI-modeller som används för övervakning:

- På biometriska data för ansiktsigenkänning
- På data från kamerabevakning i brottsbekämpande verksamhet
- Vid avlyssning eller i kombination med andra hemliga tvångsmedel
- För att övervaka medarbetares produktivitet eller lojalitet
- Inom hälsa, vård och omsorg, till exempel genom ”smarta klockor” eller annan teknik som övervakar brukare i hemmet
- Fordon som varnar förare som är trötta eller AI som tar över kontrollen och svänger tillbaka bilen om föraren börjar köra av vägen
- Social profilering för till exempel marknadsföring eller anpassade shopping-upplevelser

3.2. Webbskrapning

Webbskrapning är ett sätt att samla in data från webbplatser, istället för att hämta in information från till exempel en databas. Omfattningen av webbskrapning varierar, i vissa fall används det för att inhämta begränsad information från endast en webbplats, i andra fall kan det handla om att stora delar av hela internet skrapas på data.

Vid webbskrapning finns ingen kontroll av vilken data som samlas in eller i vilken mån den innehåller personuppgifter. Webbskrapning sker ofta utan att webbplatsinnehavaren eller den enskilde vars personuppgifter samlas in känner till det.

Webbskrapning är i sig ingen ny teknik utan har funnits nästan lika länge som internet. Det finns flera olika skäl till att personer och företag använder sig av webbskrapning, till exempel att informationen användaren vill ha inte finns tillgänglig på annat sätt. Att information inte finns allmänt tillgänglig kan bero på olika saker, till exempel att det inte är lönsamt för informationsägaren att göra den tillgänglig.

Utvecklingen inom AI är beroende av tillgång till data, vilket driver efterfrågan på webb-skrapning. Viss webbskrapning är mer problematisk ur integritetssynpunkt, till exempel när webbskrapning används för att kartlägga personer eller för att träna ansiktsigen-känningsmodeller.

3.3. Ökad användning av biometriska data

Med biometriska uppgifter menas personuppgifter som samlats in genom en särskild teknisk behandling som rör någons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av den personen.

Det finns många olika typer av biometriska data och de grupperas på olika sätt. Ett sätt är i grupperna fysiologiska och beteendemässiga. Ett exempel på fysiologiska biometriska data är fingeravtryck och ett exempel på beteendemässiga biometriska data är hur en person går.

Behandlingen av biometriska data innebär särskilda integritetsrisker eftersom de är svåra eller omöjliga att byta ut. Det är svårt för enskilda att förstå hur uppgifterna används och konsekvenserna av att man delar med sig av dem. Det kan till exempel vara svårt att föreställa sig vilka uppgifter som går att utläsa utifrån till synes harmlös insamling av olika biometriska data. Till exempel kan data som vid insamlingstillfället saknade prediktivt värde några år senare visa sig vara en indikator på sjukdom.

Insamlingen av biometriska data skiljer sig åt både i fråga om hur den samlas in och hur den avgränsas. Användningen av övervakningskameror, framför allt när de kombineras med teknik för ansiktsigenkänning, är en teknik som utgör en potentiellt stor risk utifrån ett integritetsskyddsperspektiv. Det beror bland annat på att det är svårt att kontrollera vilka som övervakas och på att övervakningen ofta omfattar ett stort antal människor.

Integritetsriskerna kopplade till biometriska data är höga, men nyttan kan i vissa sammanhang vara betydande. Till exempel kan ansiktsigenkänning vara ett kraftfullt verktyg inom det brottsbekämpande området. Biometriska data är också viktiga inom exempelvis viss medicinsk forskning. Biometriska data används dessutom för att förbättra autentisering och identifiering, i syfte att öka säkerheten. Behovet av mer avancerad biometrisk autentisering har drivits på eftersom äldre typer av autentisering inte längre är lika effektiva.

Konsekvenserna av exempelvis cyberattacker, missbruk eller överträdelser är högre än för andra, mindre känsliga data. Det är därför viktigt att hantera biometriska data med försiktighet och en hög nivå av säkerhet.

3.4. Integritetshöjande teknik

Integritetshöjande teknik är ett samlingsbegrepp för teknik eller metoder som stärker integritetsskyddet. De olika teknikerna har olika styrkor och svagheter och ingen teknik innebär ett fullständigt skydd. Allt eftersom behovet att dela personuppgifter ökar så tilltar efterfrågan på integritetshöjande teknik. Tekniken kan komplettera befintligt skydd eller minska riskerna så att de blir färre eller mindre allvarliga.

Behoven och de potentiella tillämpningsområdena för integritetshöjande teknik är många och det finns flera olika typer av integritetshöjande teknik. Vissa är enklare och billigare, medan andra är mer avancerade och dyrare. Vilken teknik eller metod som ska användas måste avgöras från fall till fall med beaktande av de risker som finns.

En särskild fråga som uppkommer vi användning av nya tekniker och där det finns en stor efterfrågan på vägledning är utrymmet för att bedöma den data som används som anonymiserad och vilka tekniker som kan användas för att uppnå anonymisering. IMY är medveten om behovet av att detta klarläggs. Europeiska dataskyddsstyrelsen (EDPB) arbetar med att ta fram vägledningar om anonymisering och pseudonymisering.

Även om integritetshöjande teknik är ett viktigt verktyg som skapar förutsättningar för ett starkare integritetsskydd är detta inte tillräckligt för att säkerställa ett bra dataskydd. Även organisatoriska åtgärder, som exempelvis rutiner och utbildning, är av stor betydelse eftersom skyddet i praktiken ofta är beroende av den mänskliga faktorn.

3.4.1. Tekniker som ger ökat skydd genom att modifiera data

Vissa integritetshöjande tekniker fokuserar på att modifiera data på ett sätt som gör det svårare att identifiera uppgifter om den enskilde eller på att skapa nya data som inte är personuppgifter.

- **Syntetiska data** innebär att användaren genererar ny, syntetisk (konstgjord) data utifrån faktiska data. Med hjälp av syntetiska data går det att analysera en population och behålla detaljerade uppgifter om dem eftersom personerna inte finns i verkligheten och därmed inte omfattas av dataskyddsregleringen. Eftersom poängen med att använda syntetiska data ofta är att undvika att använda originaldata är det ibland inte möjligt att säkerställa att den på ett meningsfullt sätt överensstämmer med originalet. Det gör att resultaten av analyserna gjorda på datan i vissa fall är mindre värdefulla och ibland direkt felaktiga. Det kan vara svårt att säkerställa att den syntetiska datamängden inte innehåller några av de ursprungliga personuppgifterna eller att en fiktiv person kan ha blivit identisk med en faktisk person.

- **Differentiell integritet**, mer känt som differential privacy, avser metoder som använder sig av exempelvis brus för att försvåra identifieringen av enskilda i en datamängd. Brus kan läggas in för att göra enskilda datapunkter mer svårtolkade. Differentiell integritet påminner i flera fall om syntetiska data.

- Att **generalisera data** innebär att specifika uppgifter görs mer generella, till exempel att en persons ålder ändras till att personen ingår i en viss åldersgrupp. Värdet på informationen minskar ofta i samband med att detaljeringsgraden minskar. I vissa fall innebär informationsförlusten efter generaliseringen att datan saknar värde för en viss typ av analys.

3.4.2. Krypteringsverktyg

Ett annat sätt att höja integritetsskyddet är att använda kryptering. Olika typer av kryptering kan användas för olika ändamål. Det finns kryptering som kan användas för att skydda uppgifter när de överförs eller lagras. Då är det primära syftet att skydda uppgifterna från obehöriga.

Det finns också annan typ av kryptering, till exempel så kallad homomorfisk kryptering, som kan användas för att skydda uppgifterna även från behöriga. Denna typ av kryptering möjliggör för användaren att göra dataanalys trots att användaren inte kan förstå de enskilda datapunkterna eftersom datan är krypterad. Homomorfisk kryptering skulle kunna skapa nya möjligheter att analysera exempelvis känsliga personuppgifter genom att integritetsintrånget minskas. Denna typ av kryptering är än så länge resurskrävande och kräver särskild kunskap hos såväl den som ska kryptera som den som ska analysera datan. Det återstår att se om denna typ av kryptering kommer få bred spridning eller om det enbart kommer användas i särskilda fall.

Även om uppgifter blivit krypterade finns en risk att någon bryter krypteringen. Därför är det viktigt att personuppgifter som blivit krypterade fortfarande hanteras på ett säkert sätt och inte kommer obehöriga till del.

3.4.3. Federerad och distribuerad analys och edge

En federerad och distribuerad analys är en metod där data inte samlas centralt för att där genomföra personuppgiftsbehandlingen, utan att analysen istället sker där datan finns och att enbart lärdomarna från analysen samlas centralt. Ur integritetssynpunkt finns två huvudsakliga fördelar med det. Den ena är att data inte behöver delas. Den andra är att data inte behöver samlas på ett ställe för att analyseras. IMY har hanterat ett användarfall med federerad maskininlärning i en regulatorisk sandlåda.[8]

Det finns en liknande teknik som kallas edge (kant) och avser den utrustning som finns längst från it-systemets centrala servrar, det vill säga i utkanten av systemet. Edge beskriver var i nätverket något befinner sig. Ett exempel är edge computing, vilket betyder att behandlingen sker i till exempel sen användares telefon istället för i en central server.

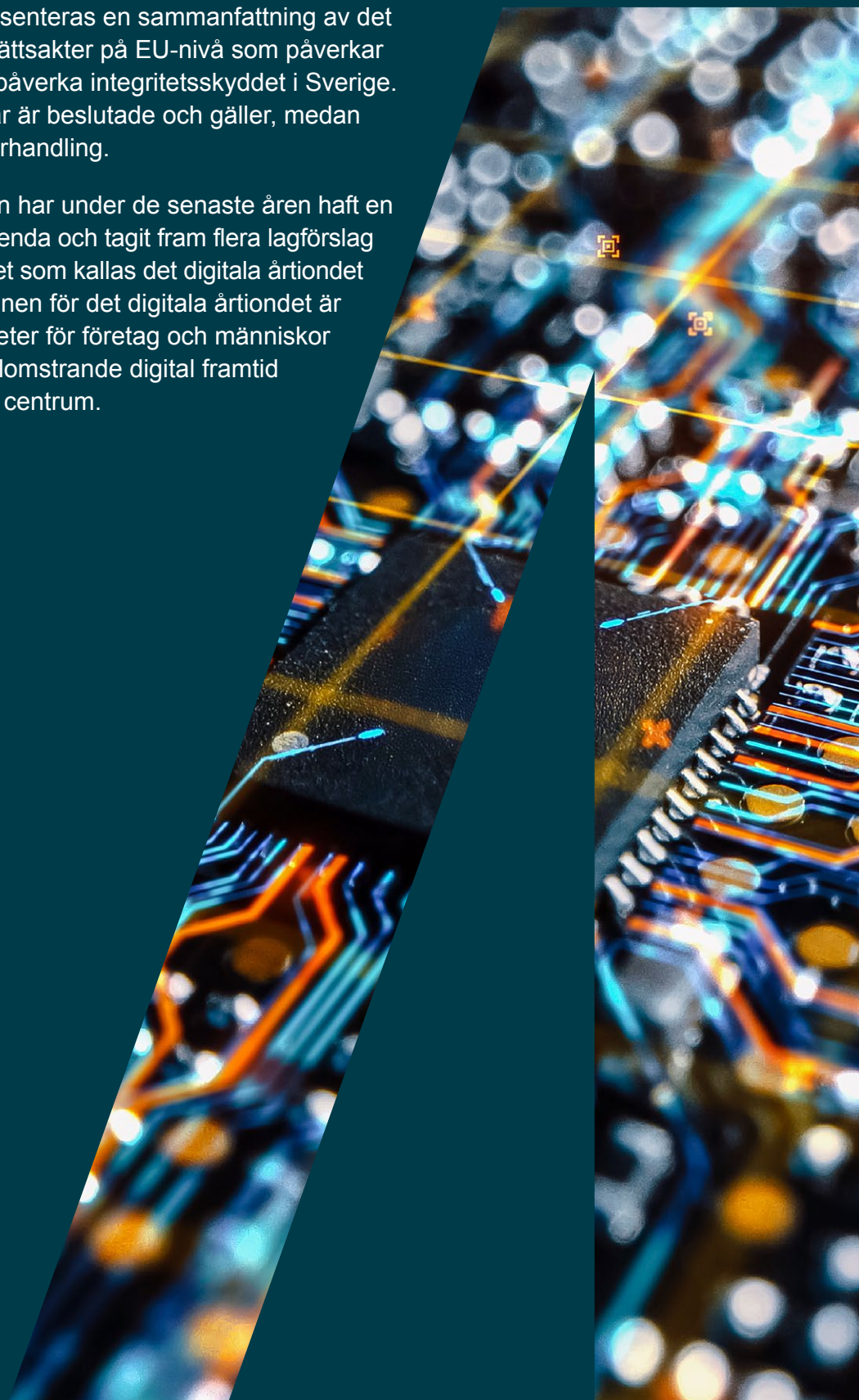
Fördelarna med båda teknikerna är ur ett integritetsperspektiv snarlika. Om person-uppgifter behandlas direkt i en sensor eller i en användares telefon istället för centralt är det fördelaktigt från integritetsperspektiv, eftersom mängden data som delas minskar. Det ställer dock höga krav på säkerhet även i edge-enheterna.

8. Slutrapport om IMY:s pilotprojekt med regulatorisk testverksamhet om dataskydd, IMY-2023-2602

4. EU:s digitala årtionde

I detta avsnitt presenteras en sammanfattning av det arbete med nya rättsakter på EU-nivå som påverkar eller kommer att påverka integritetsskyddet i Sverige. Vissa förordningar är beslutade och gäller, medan andra är under förhandling.

EU-kommissionen har under de senaste åren haft en offensiv reformagenda och tagit fram flera lagförslag inom ramen för det som kallas det digitala årtiondet 2020–2030. Visionen för det digitala årtiondet är att skapa möjligheter för företag och människor i en hållbar och blomstrande digital framtid med människan i centrum.



Visionen kommer från EU:s datastrategi, där målet är att skapa ett gemensamt europeiskt dataområde – en inre marknad för data. På det europeiska dataområdet ska data kunna delas och användas likt varor på den inre marknaden. EU-kommissionen använder framför allt två styrmedel för att utveckla dataområdet: lagstiftning och EU-budgeten. Eftersom ett stort fokus i arbetet ligger på lagstiftning kommer resultatet att bli ett, till stor del, nytt rättsligt landskap på det digitala området. För en mer fullständig beskrivning av initiativ inom det digitala årtiondet, hänvisar IMY till EU-kommissionens sammanställning.[9]

4.1. Dataskyddsförordningen

Dataskyddsförordningen (GDPR) har två syften: att skydda enskildas grundläggande rättigheter och friheter vid behandling av personuppgifter och att harmonisera regelverket på EU:s inre marknad för att säkerställa ett fritt flöde av personuppgifter inom unionen. Dataskyddsförordningen antogs 2016 och började tillämpas i maj 2018.

Dataskyddsförordningen gäller som en bottenplatta för den reglering som tas fram i det digitala årtiondet. Detta innebär att dataskyddsförordningen kommer att tillämpas parallellt med exempelvis AI-förordningen.

Enligt dataskyddsförordningen ska EU-kommissionen vart fjärde år överlämna en rapport till Europaparlamentet och rådet angående tillämpningen av förordningen. I rapporten från 2024[10] konstaterar EU-kommissionen att det råder enighet bland intressenter, dataskyddsmyndigheter och medlemsstater om att dataskyddsförordningen, trots vissa utmaningar, har ökat skyddet för den personliga integriteten och förbättrat verksamheters kunskap om dataskydd.

Europeiska dataskyddsstyrelsen (EDPB) och de nationella tillsynsmyndigheterna rekommenderas att intensifiera arbetet med att vägleda små och medelstora företag. EU-kommissionen konstaterar att det fortfarande görs olika tolkningar av dataskyddsförordningen. De nationella dataskyddsmyndigheterna uppmanas verka för att nationella riktlinjer och tillämpningen av dataskyddsförordningen på nationell nivå är förenliga med EDPB:s riktlinjer och rättspraxis från EU.

I Sverige har det under lång tid funnits kritik mot EU:s regleringsmodell för dataskydd, som innebär en detaljerad reglering av behandlingen från insamling till radering. Redan i samband med införandet av personuppgiftslagen uppmanade riksdagen regeringen att inom EU med kraft verka för att få till stånd en mer missbruksinriktad reglering, det vill säga en reglering som tar sikte på missbruk av personuppgifter.[11] Sverige har dock inte haft framgång med att förändra den EU-rättsliga regleringsmodellen.

Dataskyddsförordningen bygger på en riskbaserad ansats som innebär att kraven ökar när risken är högre. Det finns dock en utbredd uppfattning att dataskyddsförordningen är svår att tillämpa och att den skapar en stor administrativ börda, även när integritetsriskerna är små.

IMY anser att tiden är mogen för att göra en översyn av dataskyddsförordningen i syfte att säkerställa ett effektivt och balanserat skydd av den personliga integriteten. Det behöver också säkerställas att regleringen inte sätter upp omotiverade hinder för utvecklingen och användningen av ny teknik.

9. EU-kommissionen, 2024, Report on the state of the digital decade 2024
10. COM(2024) 357 final
11. Bet. 1998/99:KU15, rskr. 1998/99:147

IMY ser också ett behov av att se över den svenska kompletterande regleringen av myndigheternas personuppgiftsbehandling, de så kallade registerförfattningarna. En del av regleringen kan behöva läggas i förordning i stället för i lag. Detta skulle ge förutsättningar för ett mer snabbrörligt författningsarbete som gör att regleringen kan anpassas efter de behov som uppkommer, eftersom en förordning kan ändras inom betydligt kortare tidsramar. Ett sådant snabbrörligt författningsarbete förutsätter att Regeringskansliet har rätt resurser och kompetens för att snabbt och löpande kunna hantera de regleringsbehov som uppkommer med anledning av teknikutvecklingen, digitaliseringen och EU:s digitala årtionde.

4.2. Dataförvaltningsförordningen

Dataförvaltningsförordningen syfte är att öka transparensen, tillgängliggöra data samt skapa verktyg för att möjliggöra datadelning. I förordningen finns både verktyg för att skapa en tryggare datadelning och för att skapa förutsättningar för konkurrensneutral datadelning, med målet att främja konkurrens och innovation.

Målen är att öka datadelning mellan företag och göra data från offentlig sektor mer tillgänglig. Förordningen är en av de större rättsakter som ska stödja inrättandet och utvecklandet av de gemensamma europeiska dataområdena.

4.3. Dataförordningen

Dataförordningen syftar till att sätta människan i centrum och till att data ska kunna flöda inom EU och mellan sektorer. Det innebär att data inte ska kunna låsas in och ägas av enskilda aktörer. Ambitionen är istället att individen ska ges större kontroll över data och hur de används.

Det övergripande syftet med dataförordningen är att säkerställa att värdet av data fördelas rättvist bland aktörerna i dataekonomin samt att främja åtkomsten till och användningen av data.

4.4. AI-förordningen

Syftet med AI-förordningen är att förbättra den inre marknadens funktion samt att skapa ett regelverk för AI inom EU som säkerställer att användningen och utvecklingen av AI går i linje med EU:s värderingar. Målet är att skapa en trygg och etiskt hållbar miljö för AI-innovation, samtidigt som man skyddar medborgarnas rättigheter och friheter.

AI-förordningen delar in AI i olika riskgrupper utifrån dess användningsområden. Vissa AI-användningsområden anses medföra oacceptabel risk och förbjuds därför. Det gäller till exempel när AI används till manipulation, social poängsättning eller webbskrapning för att skapa databaser för ansiktsigenkänning. Nästa risknivå är hög risk, vilket innebär att särskilda krav ställs upp. Hög risk-AI är till exempel AI-användning inför livsavgörande beslut, exempelvis för studier och anställning. Här finns krav i form av kontroll av efterlevnad och registrering hos en ansvarig myndighet. De AI-system som anses innebära liten eller ingen risk får användas utan restriktioner, med vissa undantag. Exempel på begränsad risk är chatbottar och minimal risk är exempelvis spamfilter.

I AI-förordningen ställs olika krav beroende på vilken roll och vilket ansvar en aktör har i AI-systemets värdekedja, om man till exempel är utvecklare eller tillhandahållare. Ett system för tillsyn, styrning och kontroll av efterlevnad ska införas både på nationell nivå och på EU-nivå. Dessutom finns krav på att så kallade regulatoriska sandlådor ska inrättas i syfte att främja innovation och effektivisera regelefterlevnad.

4.5. Gemensamma europeiska dataområden

EU bryter ner det gemensamma dataområdet i 14 mindre dataområden, bland annat energi, finans och medier. Inom varje område kommer det att finnas regelverk och infrastruktur för att dela data. Uppbyggnaden av de gemensamma europeiska dataområdena kommer att vara kostsam. Även om EU-kommissionen ger ekonomiskt stöd till utvecklingen kommer omställningen att kräva att medlemsstaterna gör omfattande investeringar, inte minst för att uppnå interoperabilitet mellan olika system.

4.5.1. Det europeiska hälsodataområdet

Ett av de första att utvecklas är det europeiska hälsodataområdet (EHDS). EHDS regleras i en förordning som är indelad i två delar, primäranvändning och sekundäranvändning. Primäranvändningen syftar till ökad interoperabilitet inom varje medlemsland och mellan länder i EU. Ett av syftena med förordningen är att underlätta för gränsöverskridande vård inom EU genom att underlätta uppgiftsutbyte över landsgränser. Sekundäranvändningen syftar till att hälsouppgifter ska kunna användas för bland annat innovation och forskning.

EHDS ger en rad rättigheter för enskilda, bland annat rätten för enskilda att få tillgång till sina hälsodata och att lägga till eller rätta information i sin journal.

4.6. Interoperabilitetsförordningar och -direktiv

Interoperabilitet betyder att olika system kan utbyta data med varandra, och kan liknas vid att två personer talar samma språk. Interoperabilitet är därför en grundförutsättning för omställningen till en datadriven ekonomi och en inre marknad för data. EU-kommissionen har lagt fram flera lagförslag som syftar till att öka interoperabiliteten inom EU.

- **Interoperabilitetsförordningarna gräns och polis**
  För att skapa interoperabilitet mellan olika stora it-system som används inom EU för att hantera bland annat migration, gränskontroll och brottsbekämpning inom EU har EU-kommissionen lämnat förslag på två förordningar: interoperabilitetsförordningen gräns och interoperabilitetsförordningen polis. Förordningarna syftar bland annat till att skapa en europeisk gemensam sökportal, en gemensam europeisk matchningstjänst, en detektor för multipla identiteter samt en gemensam databas för identitetsuppgifter.

- **Prüm II-förordningen**
  Syftet med Prüm-förordningen är att underlätta automatiskt utbyte mellan brottsbekämpande myndigheter av DNA-uppgifter, fingeravtrycksuppgifter och uppgifter ur fordonsregister för att förebygga, upptäcka och utreda brott. Det gör det möjligt för polisen och andra behöriga myndigheter att söka i en eller flera EU-länders nationella databaser om en person förekommer eller inte. Prüm II-förordningen utvidgar och effektiviserar utbytet.

- **Förordningen om ett interoperabelt Europa**
  Målet med förordningen är att främja interoperabilitet mellan nätverk och informationssystem som används i offentlig sektor inom EU. Det ska stärka utvecklingen av en infrastruktur för interoperabla, gränsöverskridande digitala offentliga tjänster. Förordningen ska skapa en struktur för interoperabilitetsstyrning och ett ekosystem av gemensamma interoperabilitetslösningar för EU:s offentliga sektor.

4.7. Övriga rättsakter med påverkan på den personliga integriteten

- EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (**NIS2-direktivet**) syftar till att uppnå en hög gemensam cybersäkerhetsnivå. Utöver detta direktiv finns även EU:s **cyberresiliensförordning** som reglerar cybersäkerhet kopplat till maskin- och programvara.

- EU:s **direktiv om kritiska entiteters resiliens** (CER-direktivet) syftar till att medlemsstaterna ska säkerställa förmågan hos samhällsviktig verksamhet att förebygga, motstå och hantera störningar eller avbrott i verksamheten, vilket inkluderar bland annat digital infrastruktur där stora mängder personuppgifter behandlas.

- **Förordningen om digitala tjänster** (DSA-förordningen) syftar till att motverka olaglig och skadlig verksamhet på internet samt till att begränsa spridningen av desinformation. Den ska bidra till att öka säkerheten för användarna, upprätthålla skyddet för grundläggande rättigheter och främja rättvisa och transparenta förhållanden för internetplattformar.

- **Förordningen om digitala marknaden** (DMA-förordningen) innehåller regler som digitala plattformsföretag med stor marknadsmakt måste följa i syfte att göra den digitala sektorn mer rättvis och skapa bättre förutsättningar för små och medelstora företag att konkurrera på den marknaden.

- **eIDAS-förordningen** och **EUDI-förordningen** syftar till att underlätta för säkra gränsöverskridande transaktioner genom att inrätta en ram för digital identitet och autentisering. Ett av målen med förordningen är att den ska främja arbetet med att ta fram sömlösa digitala tjänster inom EU.

- Förslaget **CBE-direktivet** syftar till att underlätta gränsöverskridande informationsutbyte om trafikrelaterade brott, bland annat kommunikationen mellan medlemsstaterna i frågor som rör gränsöverskridande utredningar och verkställighet av påföljder. Förslaget bygger på interoperabilitet mellan medlemsstaternas informationssystem.

- **CSAM-förordningen** syftar till att förebygga och bekämpa sexuella övergrepp mot barn. Förslaget innebär att leverantörer som tillhandahåller kommunikations- och molnlagringstjänster ska kunna bli ålagda att spåra hela eller delar av sina tjänster för att söka efter material med sexuella övergrepp mot barn och grooming.

4.8. Tekniska lösningar och metodik inom det digitala årtiondet

Inom ramen för det digitala årtiondet har EU-kommissionen lagt fram förslag på olika tekniska lösningar och arbetssätt som på olika sätt bidrar till att nå målet om ett mer digitaliserat Europa. I denna rapport lyfter IMY tre exempel på lösningar, digital plånbok, säkra behandlingsmiljöer och sandlådor.

4.8.1. Europeisk digital identitetsplånbok

En stor del i den digitala omställningen är att möjliggöra för individer att styrka sin identitet med hjälp av digitala verktyg. Svenska exempel på sådana lösningar är BankID och Freja eID. För att möjliggöra detta håller EU-kommissionen tillsammans med medlemsstaterna på att utveckla en europeisk digital identitetsplånbok. Den europeiska digitala identitetsplånboken ska inte förväxlas med andra digitala plånböcker, som snarare påminner om digitala bankkort.

Målet är att plånboken ska kunna innehålla exempelvis körkort och examensbevis, men skulle teoretiskt också kunna innehålla behörighet kopplat till personens arbetsplats, tågbiljetter eller annan identitetsknuten information.

Ett av syftena med EU:s digitala plånbok är att stärka den personliga integriteten. En digital plånbok gör det möjligt att identifiera sig eller styrka information genom att lämna ifrån sig endast den information som krävs för det specifika ändamålet. Till exempel skulle en digital plånbok kunna styrka att en person är över 18 år, utan att personen i fråga behöver visa en ID-handling som innehåller mer information än ålder. Beroende på den slutliga utformningen av plånboken finns ökad risk för profilering och att plånboken lämnar för mycket information eller att motparten begär mer information än vad som är nödvändigt.

Vilket genomslag EU:s digitala plånbok kommer att få är svårt att säga, men det är tydligt att det finns en önskan och ett behov av att digitalt kunna styrka vissa uppgifter. EU-kommissionen har som mål att en europeisk digital plånbok ska vara tillgänglig för medlemsstaterna 2025–2026.

4.8.2. Säkra behandlingsmiljöer

Begreppet säker behandlingsmiljö kan avse flera olika saker. I denna rapport avses de säkra behandlingsmiljöer som de avses i dataförvaltningsförordningen och de sektorsspecifika dataområdena. Ett sådant exempel är EHDS, där säkra behandlingsmiljöer är en central del.

Det är ännu inte klart hur de säkra behandlingsmiljöerna kommer att se ut och man kan anta att de kommer skilja sig åt mellan sektorerna. Syftet med de säkra behandlingsmiljöerna är att öka möjligheten att ge tillgång till data. Det kan betyda att fler aktörer kan få enklare tillgång till mer data om fler personer. I en säker behandlingsmiljö är det enklare att säkerställa vilka som får tillgång till vilka uppgifter och att kontrollera att uppgifterna behandlas såsom är överenskommet. Uppgifterna behöver inte spridas, och därmed inte heller samlas in och lagras på flera olika ställen.

4.8.3. Sandlådor

Sandlådor för att innovera, utveckla, träna och testa ny teknik förekommer i flera olika förordningar inom ramen för det digitala årtiondet. Sandlådor har till syfte att främja innovation och konkurrenskraft. I vissa sandlådor finns möjlighet till undantag från lagstiftning, men inte i alla.

Vissa sandlådor kallas för regulatoriska sandlådor, och där är främsta syftet att minska den regulatoriska osäkerheten. Det kan uppstå ett gap mellan den snabba teknikutvecklingen och arbetet med att stifta, tolka och tillämpa regelverk. I sandlådan kan innovatörer och behöriga myndigheter arbeta tillsammans för att tolka hur regelverk kan fungera i praktiken vad gäller innovativa produkter och tjänster.

IMY bedriver sedan 2022 en regulatorisk sandlåda om dataskydd, där vi ger vägledning om gråzonsfrågor i första hand relaterade till dataskyddsförordningen. Arbetet påbörjades inom ramen för det regeringsuppdrag om att ge vägledning till innovationssystemet som vi hade 2021–2023. Regeringsuppdraget var ett resultat av vår förra rapport om integritet och ny teknik. Vi var första myndighet i Sverige att prova arbetssättet.

Inom ramen för AI-förordningen ska regulatoriska sandlådor inrättas. IMY bedriver sedan 2024 tillsammans med eSam, Bolagsverket, Skatteverket och Arbetsförmedlingen ett pilotprojekt där arbetssätt för en sådan sandlåda tas fram. Arbetsmetoden har tagit avstamp i IMY:s erfarenheter av vår sandlåda om dataskydd.

5. Fokusområden

I detta avsnitt lyfter IMY fram fyra områden där vi bedömer att det skett stora förändringar kopplade till teknik och integritetsskydd under perioden 2020–2024.

5.1. Effektiv brottsbekämpning och integritet

Utvecklingen av den organiserade brottsligheten är en fråga som har präglat samhällsdebatten i Sverige i flera år. Kampen mot den organiserade brottsligheten har beskrivits som en av vår tids största utmaningar. Det finns tre delar i frågan om effektivare brottsbekämpning med direkt påverkan på integritetsskyddet i Sverige.

- **Ökad informationsdelning**
  Informationsdelning med syfte att förebygga och utreda brott ökar på flera sätt. Dels delas mer information om fler personer och företeelser, dels är fler aktörer inblandande i informationsdelningen. I allt större utsträckning medverkar aktörer, som inte tidigare haft brottsbekämpande uppdrag, i informationsdelning för brottsbekämpande ändamål. Den ökade informationsdelningen sker både inom Sverige och på EU-nivå, och till viss del i övriga internationella sammanhang. Informationsflödet blir mer och mer komplext och svåröverskådligt.

- **Mer kamerabevakning**
  Regleringen av kamerabevakning har i flera steg förändrats för att ge bättre möjligheter att använda bevakningskameror, inte minst inom brottsbekämpningen. Det finns en ambition att öka antalet kameror i det offentliga rummet. Dessutom finns en ambition att använda information från kameror på ett effektivare sätt till exempel med tekniker som ansiktsigenkänning och AI. Avsikten med förändringarna är att regleringen bättre ska svara mot behovet av att kamerabevaka i syfte att bekämpa brott och upprätthålla allmän ordning och säkerhet.

- **Nya verktyg**
  Den snabba tekniska utvecklingen i kombination med de kriminellas ökade förmåga att undanhålla information från myndigheterna kräver åtgärder för att bevara och utveckla de brottsbekämpande myndigheternas förmåga och effektivitet. Rättsväsendets förmåga och effektivitet ska stärkas genom mer resurser, nya verktyg och skärpta straff. Några exempel på verktyg är utökad upptagning och användning av biometri i brottsbekämpningen och utökade möjlighet att använda preventiva och hemliga tvångsmedel.

Balanspunkten mellan brottsbekämpningens effektivitet och den enskildes integritet har förflyttats genom de åtgärder som vidtagits för att ge de brottsbekämpande myndigheterna effektivare verktyg. Lagstiftningstakten på området är hög och sker ofta i flera utredningar som pågår parallellt. Det är därför svårt att få en helhetsbild av hur de åtgärder som vidtas påverkar integritetsskyddet i samhället i stort. Oftast är det också först när verktygen tillämpats en tid som det är möjligt att bedöma om den nytta de medför står i rimlig proportion till integritetsintrånget.

Det finns även en trend att frågor om brottsbekämpning inte utreds inom ramen för en traditionell utredning med expertmedverkan som redovisas i ett betänkande, en så kallad SOU. Det blir i stället allt vanligare att sådana utredningar omhändertas inom ramen för så kallade bokstavsutredningar utan expertmedverkan som resulterar i en departementspromemoria, en så kallad Ds.

Många av förslagen på åtgärder på brottsbekämpningsområdet är långtgående och kan försämra integritetsskyddet i det svenska samhället. Därför har IMY och flera andra instanser, till exempel Lagrådet[12] och Justitiekanslern[13], påtalat behovet av att det görs en samlad översyn av åtgärderna och deras effekter för den personliga integriteten. Det är angeläget för att man ska kunna få en helhetsbild av den samlade påverkan på integriteten. En sådan översyn är också viktig för att utvärdera om åtgärderna gett det förväntade resultatet och om det integritetsintrång som de medför kan motiveras.

12. Lagrådets protokoll från sammanträde 2024-10-18
13. Justitiekanslern remissyttrande (2024/4010) i DS 2024:11 om bland annat biometrisk fjärridentifiering i realtid och ANPR-bevakning

5.2. Övervakning i arbetslivet

Övervakning i arbetslivet är inget nytt, men ny teknik har skapat nya möjligheter till omfattande övervakning av anställda. Det är oklart hur omfattande övervakningen i Sverige är och det saknas kunskap om hur utvecklingen sett ut över tid.

Under perioden 2020–2024 var det framför allt pandemin som påverkade hur övervakningen i arbetslivet förändrades. Det finns indikationer på att viljan och det upplevda behovet av att övervaka ökade under pandemin, för att sedan ligga kvar på en högre nivå än tidigare. Denna typ av normalisering av övervakning är vanlig. I fallet med övervakning i arbetslivet återstår det att se om den övervakning som implementerades under pandemin kommer att fortsätta när allt fler återgår till att arbeta på kontoret.

Övervakning i arbetslivet kan delas in i tre huvudsakliga delar.

- Möjligheterna till **digital övervakning av anställda som arbetar i hybrida arbetssätt** har utvecklats och mycket teknik har också blivit enklare och billigare att använda. Pandemin gjorde att allt fler arbetade hemma, vilket begränsade möjligheten till traditionell fysisk övervakning. Behovet och viljan att övervaka anställda bidrog till utvecklingen av verktyg för att kunna övervaka sina anställda genom deras användning av framför allt sina datorer. Det blir vanligare att programvara har övervakning inbyggd som en grundläggande funktion.

- En annan typ av övervakning som ökat är övervakningen av anställda som arbetar inom transport och distribution, som till exempel taxi- och busschaufförer, bud och andra yrken där arbetsgivare och kunder med hjälp av GPS har möjlighet att **spåra den anställdas position i realtid**.

- Slutligen så finns behovet av **övervakning med kamera** i syfte att säkerställa säkerhet, kvalitet eller minska brottslighet. Det kan handla om medarbetare som filmas under hela sin arbetsdag, till exempel när en medarbetare sitter i en kassa eller packar mediciner.

Det kan vara svårt att som anställd utnyttja sina rättigheter i förhållande till sin arbetsgivare, eftersom man kan uppleva att det riskerar ens möjligheter på arbetsplatsen. Flera fackförbund vittnar om att övervakning upplevs som ett problem för många medlemmar, men att det är svårt att driva frågorna till exempel i domstol eftersom personen som berörs av övervakningen kan vara rädd för att en sådan process kan leda till negativa konsekvenser i det egna arbetslivet.[14]

14. www.unionen.se/opinion-kategori/integritet-i-arbetslivet (2024-12-11)
www.akavia.se/om-akavia/det-har-tycker-akavia/fragor-vi-driver/framtidens-arbetsmarknad/digital-overvakning-i-arbetslivet (2024-12-11)
tco.se/fakta-och-politik/arbetsmarknad/overvakningen-i-arbetslivet-okar-behovs-ny-lag (2024-12-11)

5.3. Ökad insamling och användning av hälsodata

Hälsodata avser här uppgifter om en persons hälsa, till exempel uppgifter om sjukdomar eller mätningar av puls och temperatur, och inkluderar biometri såsom DNA. Insamlingen av användningen av hälsodata fortsätter att öka.

Allt fler använder sig av teknik för att samla in stora mängder hälsodata om sig själva. Insamlingen sker på olika sätt, till exempel genom smarta klockor, appar, trycksensorer och värmemätare. Många använder också tjänster för att analysera genetiskt ursprung. Ser man till en genomsnittlig användare finns både information om personens matpreferenser, sömnvanor och levnadssätt i kombination med biometriska uppgifter. Datan delas mellan enheter och applikationer. Sammantaget skapas en nästan fullständig bild av personen och dennas personlighet.

Insamling av hälsodata kan ha positiva effekter. För medicinsk forskning är hälsodata viktigt, för att till exempel ta fram nya läkemedel eller bota sjukdomar. Förväntan på att data är tillgänglig driver krav på ökad interoperabilitet och digitala lösningar för att tillgängliggöra hälsodata. För enskilda kan personer med kroniska sjukdomar uppleva en ökad kontroll över sin sjukdom eller de med behov av tillsyn kan monitoreras på distans. Det finns också risker. En person kan tillgängliggöra data om sig själv på ett sätt som hon eller han inte förstår, är förberedd på eller skulle godkänna. Det kan också vara möjligt att extrahera nya data ur uppgifterna. Dessa slutsatser kan vara användbara och till nytta för individen, men kan också innebära integritetsrisker om de sprids till obehöriga eller används på ett felaktigt sätt.

En utmaning med den snabba utvecklingen på hälsodataområdet är möjligheten att skapa teknikneutral och långsiktig hållbar lagstiftning. Forskningen och utvecklingen kommer att skapa ny kunskap. Det kan innebära att data, som tidigare inte ansågs känsliga, med hjälp av ny kunskap kan bli en känslig uppgift.

5.4. Barn och ungas integritet

Många barn och ungdomar är redan i unga år avancerade användare av program och appar. Från åtta års ålder använder nästan alla barn internet dagligen. Internet är en självklar del av vardagen och det finns ingen tydlig gräns mellan tillvaron framför skärmen och det övriga livet. Det handlar om sociala medier, onlinespel, videodelningsappar och andra digitala plattformar som styrs av algoritmer som anpassar innehållet till användaren.[15]

I vissa fall kan det vara harmlöst att barn och unga använder digitala tjänster, exempelvis för att dela bilder med vänner och familj. Det finns dock situationer där det kan få långtgående negativa konsekvenser. Det kan handla om att de får dåliga förebilder eller felaktiga råd. I värsta fall kan det handla om vuxna som söker kontakt med barn och unga av sexuella skäl eller för att rekrytera dem att begå brott.

Personuppgifter om barn är särskilt skyddsvärda enligt dataskyddsförordningen. Det beror på att barn har svårare att ta in och bedöma riskerna med att dela med sig av sina personuppgifter och att förstå vilken rätt till skydd för sina uppgifter som de har. IMY föreslår att breda utbildningsinsatser genomförs för att öka kunskapen om personlig integritet hos barn och unga. Dessa bör ske i nära samverkan med skolor och ideella föreningar som riktar sig till barn och unga.

15. svenskarnaochinternet.se/app/uploads/2024/09/internetstiftelsen-svenskarna-och-internet-2024.pdf (2024-12-11)

IMY. Integritetsskydds myndigheten

Detta är Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten arbetar för att skydda medborgarnas alla personuppgifter, till exempel om hälsa och ekonomi, så att de hanteras korrekt och inte hamnar i orätta händer. Det är vi som granskar att företag, myndigheter och andra aktörer följer GDPR – dataskyddsförordningen. Vi utbildar och vägleder dem som behandlar personuppgifter. Vi vill se en hållbar och integritetsvänlig digitalisering. Vi är övertygade om att det går att värna medborgarnas trygghet och samhällets säkerhet, utan omotiverad kartläggning och övervakning. Tillsammans med övriga dataskyddsmyndigheter i EU arbetar vi för att medborgarnas personuppgifter ska ha samma skydd i hela unionen. Vi arbetar även för att kreditupplysning ska bedrivas på ett korrekt sätt. Vår vision är ett tryggt informationssamhälle, där vi tillsammans värnar den personliga integriteten.

Kontakta Integritetsskyddsmyndigheten

E-post: imy@imy.se
Webb: www.imy.se
Tel: 08-657 61 00
Postadress: Integritetsskyddsmyndigheten,
Box 8114, 104 20 Stockholm