Stockholms läns landsting

Landstingsrådsberedningen

SKRIVELSE
2016-10-19

LS 2016-0925

Landstingsstyrelsen

Yttrande över delbetänkandet Hur står det till med den personliga integriteten? (SOU 2016:41)

Föredragande landstingsråd: Torbjörn Rosdahl

Ärendebeskrivning

Justitiedepartementet har genom remiss bjudit in Stockholms läns landsting att lämna synpunkter på delbetänkandet Hur står det till med den personliga integriteten? (SOU 2016:41).

Förslag till beslut

Landstingsrådsberedningen föreslår landstingsstyrelsen besluta

att avge yttrande till Justitiedepartementet över slutbetänkandet Hur står det till med den personliga integriteten? (SOU 2016:41) i enlighet med landstingsdirektörens förslag till yttrande.

Landstingsrådsberedningens motivering

Integritetskommittén har i delbetänkandet identifierat och analyserat risker för den personliga integriteten på flera olika samhällsområden. Det som är förknippat med den högsta risken för den personliga integriteten handlar oftast om den stora insamling och hantering av uppgifter om enskilda.

Även den omfattande kartläggning av enskilda som sker när personer använder diverse appar eller sociala medier kan utgöra en hög risk för den personliga integriteten samtidigt uppmärksammas de stora fördelar som digitala tjänster medför för den enskilde. Mångfalden ställer därför krav på att det finns former för ändamålsenlig och säker informationsöverföring.

Dokumentationen inom hälso- och sjukvården och socialtjänsten är utan tvekan av mer integritetskänslig karaktär än information i många andra sammanhang bland landstingets verksamheter. Ibland kan det råda osäkerhet om vem som är ytterst ansvarig för de uppgifter som samlas in. Regelverk kan därför vara svåra att tolka för dem som är verksamma inom

området. Att uppgifter finns tillgängliga när de behövs för vården av en patient är en grundläggande förutsättningar för en ändamålsenlig informationshantering. En annan förutsättning är att de uppgifter som dokumenteras om patienter förvaras och hanteras på ett sådant sätt att obehöriga inte kan komma åt dem. Uppgifterna ska inte spridas på ett otillbörligt sätt utanför organisationen. Samtidigt är det viktigt att olika vårdgivare kan ha bästa tänkbara samarbete för att ge god vård till patienterna. Det är viktigt att regelsystemet inte försvårar informationsutbyte mellan dessa vårdgivare.

Den digitala utvecklingen är nödvändig men även behovet av att i största möjliga utsträckning ta tillvara den moderna informationsteknologins fördelar i arbetet med att förbättra effektivitet och kvalitet i landstingets verksamheter. Samtidigt måste förändringarna genomföras utan att riskerna för den personliga integriteten tillåts bli för stora.

Det är viktigt att lagstiftning och regelverk utvecklas i takt med samhällsutvecklingen och att det inte skapar onödiga hinder för den positiva utvecklingen av modern informationsteknologi.

Landstinget har under de senaste åren tagit ett antal initiativ för att förbättra informationssäkerheten. I syftet att säkerställa ett långsiktigt arbete har bland annat ett handlingsprogram med ett målsystem för informationssäkerhet tagits fram. Samtidigt arbetar landstinget kontinuerligt med förbättringar på beskrivna områden.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 3 oktober 2016
Förslag till yttrande
Sammanfattning av delbetänkandet Hur står det till med den personliga integriteten? (SOU 2016:41)

Torbjörn Rosdahl

Carl Rydingstam

Landstingsstyrelsens förvaltning
SLL Juridik och upphandling

TJÄNSTEUTLÅTANDE
2016-10-03

LS 2016-0925

Handläggare: Josef Driving

Ankom
Stockholms läns landsting
2016 -10- 13
Dnr LS 2016-0925
Rotel I

Landstingsstyrelsen

Yttrande över delbetänkandet Hur står det till med den personliga integriteten? (SOU 2016:41)

Ärendebeskrivning

Justitiedepartementet har genom remiss bjudit in Stockholms läns landsting att lämna synpunkter på delbetänkandet Hur står det till med den personliga integriteten? (SOU 2016:41).

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 3 oktober 2016
Förslag till yttrande
Sammanfattning av delbetänkandet Hur står det till med den personliga integriteten? (SOU 2016:41)

Förslag till beslut

Landstingsstyrelsen föreslås besluta

att avge yttrande till Justitiedepartementet över slutbetänkandet Hur står det till med den personliga integriteten? (SOU 2016:41) i enlighet med landstingsdirektörens förslag till yttrande.

Förvaltningens förslag och motivering

Sammanfattning
Integritetskommitténs uppdrag är att utifrån ett individperspektiv kartlägga och analysera risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik. I delbetänkandet presenterar kommittén en översiktlig beskrivning av faktiska och potentiella integritetsrisker som enskilda utsätts för på olika områden av samhällslivet. Kommittén föreslår bl.a. ett utvidgat uppdrag till Datainspektionen att följa och redovisa de legala förutsättningarna för integritetsskyddet, samt att regeringen ska lämna en årlig skrivelse till riksdagen med information om utvecklingen inom området.

Förvaltningen delar i stort kommitténs omvärldsanalys och slutsatser och tillstyrker förslagen på åtgärder i delbetänkandet.

Delbetänkandets innehåll
I delbetänkandet presenterar Integritetskommittén sin kartläggning av de faktiska och potentiella integritetsrisker som en medborgare kan utsättas för. En grundläggande slutsats är att den fredade zon som medborgare har rätt till minskar, samtidigt som insamlandet och vidareanvändningen av personuppgifter ökar. För att förbättra kunskapen om utvecklingen för den personliga integritetet föreslår kommittén att Datainspektionen varje år ska rapportera om den samlade utvecklingen till regeringen och riksdagen.

I delbetänkandet presenteras även ett stort antal områden och företeelser som kan innebära en risk för den personliga integriteten. Företeelserna har delats in i olika kategorier beroende på vilken risk de utgör för den personliga integriteten.

Bland det som bedöms ha en påtaglig risk för den personliga integriteten finns bland annat olika former av e-förvaltning inom och mellan myndigheter och vidareanvändning av offentlig information.

Det som är förknippat med den högsta risken för den personliga integriteten handlar oftast om den stora insamling och hantering av uppgifter om enskilda som stora delar av befolkningen genomgår. Bland dessa finns arbetsgivares möjligheter till övervakning av anställda, samt även informationshanteringen inom hälso- och sjukvård, inte minst frågor om rätt behörighet och åtkomstkontroller. Även den omfattande kartläggning av enskilda som sker när personer använder diverse appar eller sociala medier utgör en hög risk för den personliga integriteten samtidigt som kommittén är medveten om de stora fördelar som digitala tjänster medför för den enskilde. Kommittén pekar bl.a. på risken att oklara avtalsförhållanden gällande hur den insamlade information om individer kan delas samt om och hur insamlad hälsoinformation via appar kan säljas vidare i marknadsföringssyfte.

Kommittén ska slutredovisa sitt uppdrag senast den 1 juni 2017 och ska då presentera förslag till åtgärder som skulle kunna vidtas för att motverka de risker som identifierats.

Delbetänkandets innehåll på utvalda, för landstinget relevanta områden (betänkandets kapitelindelning inom parentes)

Arbetslivet (kapitel 8)
Karaktäristiskt för övervakning inom arbetslivet är att endast få system marknadsförs med det uttalade syftet att övervaka arbetstagarna. Vanligen är det angivna syftet ett annat, men tekniken gör det även möjligt att i detalj övervaka personalen. Som exempel nämns användning av positionerings-

teknik, in- och utpasseringssystem eller olika verktyg för övervakning och loggning av arbetstagarnas användning av arbetsgivarens IT-utrustning. Ny teknik i kombination med nya arbetssätt innebär även risk för en ökande och oönskad sammanblandning av arbetstagarnas privatliv och arbetsliv.

Hälso- och sjukvård och välfärdsteknik inom socialtjänst (kapitel 9)
Dokumentationen inom hälso- och sjukvården och socialtjänsten är utan tvekan av mer integritetskänslig karaktär än information i många andra sammanhang. Uppgifter som dokumenteras i vården hanteras även för andra syften än den hantering som behövs för att kunna ge den vård som behövs i det enskilda fallet. Exempelvis hamnar vissa uppgifter i kvalitetsregister med anknytning till hälso- och sjukvården. Vissa uppgifter måste även lämnas av vårdgivaren till något av Socialstyrelsens hälsodataregister. Utvecklingen med bl.a. ökande andel privata vårdgivare och apotek samt ökad specialisering har lett till att det ofta är fler aktörer än tidigare inblandade i vården av samma patient. Mångfalden ställer krav på att det finns former för ändamålsenlig och säker informationsöverföring.

Välfärdsteknik inom socialtjänsten kan bland annat handla om användning av olika digitala tjänster i form av trygghetslarm, tele- och videokommunikation, sensorer i hemmet, kognitiva hjälpmedel, ett mobilt arbetssätt och e-tjänster för trygghet, service och delaktighet.

Svensk sjukvårds-IT består idag av ett mycket stort antal system och tjänster som lagrar och distribuerar patientinformation. Ett område som är under utveckling är användningen av olika former av besluts- och kunskapsstöd i vårdarbetet.

Grundläggande förutsättningar för en ändamålsenlig informationshantering är bland annat att uppgifter finns tillgängliga när de behövs för vården av en patient. En annan förutsättning är att de uppgifter som dokumenteras om patienter förvaras och hanteras på ett sådant sätt att obehöriga inte kan komma åt dem, att uppgifter inte sprids utanför verksamheten, att de informationssystem som används i verksamheten är utformade på ett sådant sätt att integritetsskyddet tillgodoses, att användares behörighet till uppgifter anpassas och begränsad till de behov som användaren har samt att åtkomst till uppgifterna loggas och kontrolleras.

Datainspektionen har riktat kritik mot olika vårdgivare i ett antal ärenden på senare år. Kritiken har gällt bl.a. behörighetsstyrning, åtkomstkontroll, bristande information till patienter om s.k. sammanhållen journalföring samt patienters möjlighet att begära spärr av sina uppgifter. Kritiken har till

viss del lett till förbättringar, men utredningen konstaterar att det fortfarande förekommer brister hos flera vårdgivare.

Sammanfattningsvis konstaterar kommittén att risker uppstår i samband med informationshantering inom hälso- och sjukvården till följd av

- bristande ledning och ansvarstagande över informationssystemen och de personuppgifter som hanteras i dessa,
- komplexa miljöer med många olika system för hantering av information,
- brist på gemensamma lösningar, bl.a. gemensam infrastruktur,
- bristande regelefterlevnad,
- bristande kunskaper hos både personal och ledning samt
- bristande informationssäkerhet.

Utredningens slutsats är att det föreligger allvarliga risker för den personliga integriteten i samband med hantering av personuppgifter inom hälso- och sjukvården och i samband med socialtjänstens användning av välfärdsteknik.

Forskning och statistik (kapitel 10)
Kommittén bedömer att det föreligger allvarliga risker för den personliga integriteten i samband med hantering av integritetskänsliga person-uppgifter för forskningsändamål. Samtidigt konstaterar kommittén att resultaten av dessa verksamheter bidrar med viktiga värden inom en rad olika samhällsområden. Beträffande den statliga statistikframställningen föreligger viss risk för den personliga integriteten.

Sverige utmärker sig internationellt med sina stora och centraliserade myndighetsregister och statistikdatabaser som omfattar hela befolkningen samt genom de unika personnumren som används konsekvent och genomgående, vilket möjliggör sambearbetning av data från många olika källor. Inom forskningen rör det sig därför ofta om stora samlingar uppgifter som kan vara synnerligen integritetskänsliga. Forsknings-huvudmännen är många med varierande resurser och kunskap om integritetsskydd.

För vissa forskningsprojekt, t.ex. då forskningen omfattar behandling av känsliga personuppgifter, krävs godkännande av etikprövningsnämnd för att forskningen ska få utföras. Etikprövningsnämnderna tillåter ofta att s.k. registerforskning bedrivs utan att de enskilda ges någon information om att deras uppgifter används i forskningen och utan att deras samtycke behöver inhämtas.

Datainspektionens tillsyn har visat att det förekommer brister i bl.a. hur forskningshuvudmännen informerar de personer som ingår i forskningen om hur deras uppgifter kommer att användas och vilka rättigheter de har. Ibland kan det råda osäkerhet om vem som är ytterst ansvarig för de uppgifter som samlas in. Regelverket bedöms som svårt att överblicka och förstå för dem som är verksamma inom området.

E-förvaltning (kapitel 11)
Digitaliseringen i den offentliga förvaltningen har redan skapat betydande värden i form av bättre service till medborgarna och en effektivare förvaltning. Nyttoeffekterna av de olika företeelserna i e-förvaltningen varierar, liksom de risker för den personliga integriteten som företeelserna innebär. Inom såväl statlig som kommunal förvaltning hanteras ett stort antal uppgifter om enskilda som kan vara av mycket känslig art. Ofta har de enskilda inget inflytande över myndigheternas hantering vilket medför ett stort ansvar för att uppgifter bara behandlas om det är nödvändigt samt för att hanteringen är säker.

Teknikutvecklingen gör det möjligt att utveckla och effektivisera hanteringen, både genom att öka spridning och vidareanvändning av uppgifterna men även att bättre skydda uppgifterna. En generell iakttagelse som kommittén gör är att myndigheterna och regeringen fokuserar mer på att öka hanteringen av uppgifterna än på att förbättra skyddet för dem.

Molntjänster (kapitel 21.1)
Begreppet molntjänster används som gemensamt namn för tjänster som ersätter program och lagringsutrymme i användarens egen dator och i stället erbjuder motsvarande funktioner via internet. Fokus för avsnittet om molntjänster ligger främst på globala molntjänster som riktar sig till företag, myndigheter och organisationer, inte till privatpersoner.

Molntjänster erbjuder många fördelar, bl.a. en tydlig kostnad och kapacitet efter behov. Molntjänster har vissa fördelar även ur integritetsskyddsperspektiv, främst genom att säkerheten för personuppgifterna kan vara bättre hos en molntjänstleverantör än i den egna IT-miljön. Det förutsätter dock att den senare gjort en grundlig risk- och sårbarhetsanalys och ställt krav på säkerheten som motsvarar uppgifternas känslighet. Annars kan resultatet bli att känsliga uppgifter hanteras över internet med en säkerhet som är anpassad för uppgifter av mer trivial natur. De största integritetsriskerna med molntjänster hänger dock ihop med förlusten av insyn och kontroll, vilken kan innebära att en organisation i slutändan inte kan uppfylla sin skyldighet att se till att uppgifterna hanteras för rätt ändamål och på ett tillräckligt säkert sätt. Det

finns också en risk att uppgifterna hamnar i länder där lagstiftningen inte ger ett tillräckligt skydd. Kommittén anser att publika molntjänster, där flera leverantörer är inblandade, innebär en allvarlig risk för den personliga integriteten.

Informationssäkerhet och integritet (kapitel 22)
Det finns ett starkt samband mellan informationssäkerhet och integritet. En väl fungerande informationssäkerhet är en viktig grund för ett väl fungerande integritetsskydd. Eftersom den enskilda individen i de flesta fall har liten möjlighet att påverka hur de egna uppgifterna hanteras, vilar ett tungt ansvar på företag, organisationer och särskilt på myndigheter när det gäller att arbeta med riskbedömningar och skapa ett gott integritetsskydd.

Kommittén anser att det finns starka indikationer på väsentliga brister i informationssäkerheten hos offentliga organisationer med omfattande personuppgiftsbehandlingar, t.ex. kommuner. På den privata sektorn är frånvaron av aktuella undersökningar en brist i sig.

Överväganden
Integritetskommittén har i delbetänkandet gjort ett omfattande arbete när det gäller att identifiera och analysera risker för den personliga integriteten på en mängd samhällsområden.

Förvaltningen instämmer i kommitténs slutsatser i stort och pekar samtidigt på den digitala utvecklingen och behovet av att i största möjliga utsträckning ta tillvara den moderna informationsteknologins fördelar i arbetet med att förbättra effektivitet och kvalitet i landstingets verksamheter. Samtidigt måste förändringarna genomföras utan att riskerna för den personliga integriteten tillåts bli för stora. Detta kräver att informationssäkerhets- och integritetsfrågorna tas på allvar. För att minimera integritets- och informationssäkerhetsriskerna krävs kraftfulla och långsiktiga insatser i form av stärkt styrning och integrering av informationssäkerhetsarbetet i kärnverksamheterna.

Under de senaste åren har ett antal initiativ tagits för att förbättra informationssäkerheten inom landstinget. Bland annat har ett handlingsprogram med ett målsystem för informationssäkerhet tagits fram i syfte att säkerställa ett strukturerat och långsiktigt arbete inom området, insatser görs för att förbättra regelefterlevnad och flera initiativ har tagits för att upptäcka och hantera it-säkerhetsrelaterade hot och incidenter.

På hälso- och sjukvårdens område finns utmaningar, som beskrivs i delbetänkandet bl.a. när det gäller att få till stånd en effektiv och ändamålsenlig informationshantering, med bibehållande av ett gott

integritetsskydd. Även för kollektivtrafikens del finns viktiga avvägningar att göra, exempelvis när det gäller kameraövervakning och andra värdefulla åtgärder för att öka säkerheten som samtidigt innebär integritetsrisker.

Landstinget arbetar kontinuerligt med förbättringar på beskrivna områden. Utredningar och granskningar av Datainspektionen, Socialstyrelsen m.fl. har medfört en större medvetenhet i integritetsfrågor och förbättrad regelefterlevnad. Viktiga strategiska insatser, med potential att åstadkomma väsentliga förbättringar för det systematiska informationssäkerhetsarbetet pågår i landstinget, men mycket arbete återstår.

EU:s dataskyddsförordning träder ikraft 2018. Under det utredningsarbete som nu pågår för att anpassa den svenska lagstiftningen till förordningen är det viktigt att man i arbetet bidrar till nödvändiga förtydliganden.

Förvaltningen ser det som väsentligt att återaktualisera förslagen i betänkandet Rätt information på rätt plats i rätt tid (SOU 2014:23), som presenterades i april 2014 men ännu inte har lett till vidare lagstiftningsåtgärder, för att inte bromsa en nödvändig utveckling inom svensk hälso- och sjukvård. Förvaltningen efterlyser även statliga satsningar på utbildning och riktade anslag inom informationssäkerhetsområdet.

Ekonomiska konsekvenser av beslutet

Beslutet har inga ekonomiska konsekvenser.

Miljökonsekvenser av beslutet

I enlighet med landstingets Miljöpolitiska program 2012-2016 har hänsyn till miljön beaktats och slutsatsen är att det inte är relevant med en miljökonsekvensbedömning i detta ärende.

Anne Rundquist
Tillförordnad landstingsdirektör

Thomas Wedegren
Tillförordnad funktionsdirektör
SLL Juridik och upphandling

Landstingsstyrelsens förvaltning

YTTRANDE
2016-10-25

Diarienummer
LS 2016-0925

Justitiedepartementet
Ju2016/04398/L6

Yttrande över delbetänkandet Hur står det till med den personliga integriteten? (SOU 2016:41)

Justitiedepartementet har genom remiss bjudit in Stockholms läns landsting att lämna synpunkter på delbetänkandet Hur står det till med den personliga integriteten? (SOU 2016:41). Med anledning av remissen vill landstinget anföra följande.

Integritetskommittén har i delbetänkandet gjort ett omfattande och värdefullt arbete när det gäller att identifiera och analysera risker för den personliga integriteten på en mängd samhällsområden.

Stockholms läns landsting instämmer i kommitténs slutsatser i stort och tillstyrker förslaget om att ge ett utvidgat uppdrag till Datainspektionen, liksom förslaget om en årlig skrivelse till riksdagen med information om utvecklingen inom området.

Stockholms läns landsting står inför en stor förändringsprocess med behov av omfattande satsningar på bl.a. e-hälsa och IT. Behovet av att i största möjliga utsträckning ta tillvara den moderna informationsteknologins fördelar är stort. Samtidigt måste förändringarna genomföras utan att riskerna för den personliga integriteten tillåts bli för stora. Detta kräver att informationssäkerhets- och integritetsfrågorna tas på allvar.

På hälso- och sjukvårdens område finns utmaningar, t.ex. när det gäller att få till stånd en effektiv, ändamålsenlig och säker informationshantering, med bibehållande av ett gott integritetsskydd. Nya verktyg för uppföljning, verksamhetsutveckling och beslutsstöd i patientmötet ger goda förutsättningar för kvalitetsförbättringar.

Samtidigt försvåras värdefull utveckling inom hälso- och sjukvården av att lagstiftningen inte anpassats till de förändringar som skett på området under de senaste åren, med ökande antal privata vårdgivare och större inslag av s.k. nätverkssjukvård, där flera offentliga och privata vårdgivare samverkar kring vården av en patient. De sekretessgränser som därigenom uppstår betyder att samarbete mellan vårdens aktörer försvåras i en utsträckning som inte står i proportion till integritetsvinsterna. Utredningen Rätt information i Vård och Omsorg föreslog i april 2014 genom betänkandet Rätt information på rätt plats i rätt tid (SOU 2014:23) lösningar på vissa av dessa problem. Förslagen har dock ännu inte lett till vidare lagstiftningsåtgärder. Förvaltningen ser det som väsentligt att förslagen i betänkandet återaktualiseras, för att inte bromsa en nödvändig utveckling inom svensk hälso- och sjukvård.

Utveckling och förändringstryck skulle även kunna åstadkommas med statliga satsningar inom området, såsom exempelvis utbildning och anslag inom informationssäkerhetsområdet. Förslag i detta avseende skulle mottas positivt. Regelverket till skydd för den personliga integriteten är förhållandevis svåröverskådligt och i flera delar svårtillämpat. EU:s dataskyddsförordning träder ikraft 2018. Under det utredningsarbete som nu pågår för att anpassa den svenska lagstiftningen till förordningen är det viktigt att man i arbetet bidrar till nödvändiga förtydliganden.

Ankom
Stockholms läns landsting
2016 -07- 07
Dnr. LS 2016-0925

Sammanfattning

Inledning

För att kunna ta del av många fördelar med modern informationsteknik delar vi med oss av våra personuppgifter. Ibland betalar vi som vanligt, men ofta får vi betala för olika tjänster genom att dela med oss av uppgifter om oss själva och ibland också om våra vänner. Det är svårt för oss att förstå och ha en överblick över på vilket sätt våra personuppgifter samlas in, sprids och vidareanvänds. Det är i dag möjligt att behandla stora mängder uppgifter om oss på ett sätt som blir mycket närgånget. Sådana behandlingar görs inte bara av kommersiella företag utan också av myndigheter.

På vilket sätt påverkar användningen av modern teknik vår möjlighet att bestämma över vilka uppgifter om oss som andra ska få ta del av? Finns det någon möjlighet att upprätthålla en fredad sfär, som inte myndigheter, företag eller andra enskilda kan komma åt? Hur står det till med den personliga integriteten i det moderna informationssamhället?

Integritetskommitténs uppdrag är att utifrån ett individperspektiv kartlägga och analysera risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik. I detta delbetänkande presenterar vi en översiktlig beskrivning av faktiska och potentiella integritetsrisker som var och en av oss utsätts för.

Kommitténs riskbedömning

För att göra det möjligt att jämföra de risker för den personliga integriteten som är förknippade med olika företeelser i samhället har kommittén valt att beskriva riskerna utifrån tre nivåer; viss risk, påtaglig risk eller allvarlig risk för den personliga integriteten. En riskbedömning utgår dels från sannolikheten för att ett intrång inträffar, dels från effekterna eller konsekvenserna av intrånget. Mer om hur vi har arbetat med riskbedömningen redovisas i kapitel 2.

Företeelser som är förknippade med viss risk för den personliga integriteten

När det gäller företeelser som är förknippade med den lägsta graden av risk för den personliga integriteten handlar det ibland om företeelser som sannolikt inte så många av oss blir föremål för. Det kan också vara så att det inte är så många uppgifter som behandlas eller att det inte är så känsliga eller närgångna uppgifter. Det kan också vara så att det finns en bra och tydlig lagstiftning och att det inte har uppmärksammats särskilt stora tillämpningsproblem. Men dessa företeelser är ändå förknippade med risker för den personliga integriteten.

De företeelser som kommittén bedömt som förknippade med vissa risker för den personliga integriteten är:

- Hanteringen av personuppgifter inom elevhälsan (skolan)
- Skolfederation (skolan)
- Arbetsgivares granskningar av vad arbetstagare skriver på sociala medier (arbetsliv)
- Kompetensdatabaser och bakgrundskontroller inom arbetslivet
- När vårdgivare tillhandahåller både hälso- och sjukvård och personaladministrativa tjänster (arbetsliv)
- Statlig statistikverksamhet (forskning och statistik)
- Myndigheters användning av sociala medier (e-förvaltning)
- Kronofogdemyndighetens verksamhet

- Inkassobolagens verksamhet
- Personuppgiftsbehandling i domstolarnas verksamhetsregister, i samband med ljud- och bildupptagningar och i samband med informationsutbyte med andra myndigheter
- Tvångsmedel med stöd av 27 kap. rättegångsbalken (brottsbekämpning)[1]
- Polisens spaningsverksamhet på internet och utåtriktade verksamhet i sociala medier (brottsbekämpning)
- Polisens hantering av personuppgifter som överförs av flygbolag och polisens deltagande i internationellt samarbete (brottsbekämpning)
- Behandling av personuppgifter i den militära underrättelsetjänstens it-system[2]

Företeelser som är förknippade med påtaglig risk för den personliga integriteten

När det gäller företeelser som är förknippade med den högre graden av risk för den personliga integriteten handlar det ofta om företeelser som innefattar behandling av fler uppgifter om enskilda och om behandlingar som omfattar många av oss. De uppgifter som behandlas kan vara känsliga eller närgångna. Sådana företeelser är ofta reglerade, men har ibland brister i regelverket eller i tillämpningen av dessa. Kommittén har bedömt riskerna efter en sammanvägning av dessa faktorer.

- Kameraövervakning (i allmänhet och särskilt beträffande övervakning inomhus i skolan)
- Informationsdelning inom och mellan myndigheter (e-förvaltning)

[1] För de enskilda personer som blir föremål för åtgärden är intrånget i den personliga integriteten tveklöst mycket närgånget. Men ur ett riskperspektiv ska även sannolikheten för att någon blir föremål för åtgärden beaktas, liksom andra relevanta faktorer som ett fungerande regelverk och risken för oönskad spridning m.m. Kommittén bedömer därför att åtgärden utgör en viss risk för den personliga integriteten, det vill säga den lägre riskgraden.

[2] Se fotnot 1.

- Informationsutbyte med enskilda (e-förvaltning)
- Vidareanvändning av offentlig information enligt PSI-lagstiftningen (e-förvaltning)
- Oskyddad e-post
- Försäkringsföretagens verksamhet
- Kreditprövning och rådgivning samt rapporteringskrav (bank- och kreditmarknad)
- Domstolarnas utlämnande av uppgifter på medium för automatiserad behandling
- Spaningsmetoder som enbart regleras av polislagen (brottsbekämpning)
- Polisens behandling av personuppgifter i register (brottsbekämpning)
- Signalspaning (försvarsunderrättelseverksamhet och militär säkerhetstjänst)[3]
- Tekniker som involverar många och detaljerade biometriska uppgifter (biometri)

Företeelser som är förknippade med allvarlig risk för den personliga integriteten

När det gäller företeelser som är förknippade med den högsta graden av risk för den personliga integriteten handlar det ofta om företeelser som innefattar behandling av många uppgifter om enskilda och om behandlingar som omfattar stora delar av befolkningen. Det handlar också ofta om behandling av mycket känsliga eller närgångna personuppgifter. Sådana företeelser kan sakna reglering eller ha stora brister i regelverket eller i tillämpningen av dessa. Kommittén har bedömt riskerna efter en sammanvägning av dessa faktorer.

[3] För de enskilda personer som faktiskt blir föremål för granskning är intrånget i den personliga integriteten tveklöst mycket närgånget. Men ur ett riskperspektiv ska även sannolikheten för att någon blir föremål för åtgärden beaktas, liksom andra relevanta faktorer som ett fungerande regelverk och risken för oönskad spridning m.m. Kommittén bedömer därför att åtgärden utgör en påtaglig risk för den personliga integriteten, det vill säga den något högre riskgraden.

- Digitala lärplattformar och digitala läromedel (skolan)
- Vissa sociala medier (i allmänhet och särskilt beträffande användningen av sociala medier i skolans undervisning)
- Arbetsgivares positionering och annan övervakning och kontroll av arbetstagarnas aktiviteter och beteenden på arbetet
- Kameraövervakning på arbetsplatser
- Hälso- och sjukvård och välfärdstjänster inom socialtjänsten
- Viss forskning
- Myndigheter med kunddata i molnet (e-förvaltning)
- Medborgarprofilering och kontroller på internet (e-förvaltning)
- Brister i myndigheters informationssäkerhet (e-förvaltning)
- Konsumentområdet
- Försäkringsföretagens framtida verksamhet
- Användningen av kreditkort och andra digitala transaktioner (bank- och kreditmarknad)
- Kreditupplysningsföretagens verksamhet
- Lagring och vidarebearbetning av uppgifter som har samlats in med hjälp av kameraövervakning
- Publika molntjänster
- Big data

Informationssäkerhet och integritet

Vi har som enskilda personer ofta små möjligheter att påverka hur uppgifter om oss hanteras. Därför är det nödvändigt att de som hanterar våra personuppgifter tar sitt ansvar för säkerheten. Kommittén anser att det finns starka indikationer på allvarliga brister i informationssäkerheten i offentliga verksamheter. När det gäller den privata sektorn har kommittén inte tillräckligt underlag för att göra en generell bedömning. I kapitel 22 skriver vi mer om detta viktiga ämne.

Övervägande om behovet av ett integritetsskyddsråd

Vi bedömer att det saknas behov av ett nytt integritetsskyddsorgan som, på det sätt som Integritetsskyddskommittén ansåg kunde övervägas, skulle ha till huvuduppgift att verka för en säkrare avvägning av motstående intressen i lagstiftningen.

Förslag om ökad information till regering och riksdag

Kommittén lämnar förslag om att Datainspektionens uppdrag att följa och beskriva utvecklingen på it-området när det gäller frågor som rör personlig integritet och ny teknik, ska utvidgas till att även omfatta de legala förutsättningarna för integritetsskyddet och att myndigheten årligen ska lämna en redovisning om utvecklingen inom området till regeringen (kap. 24).

Vi föreslår även att regeringen i en årlig skrivelse till riksdagen ska informera om utvecklingen och det aktuella tillståndet när det gäller frågor som rör personlig integritet, informationsteknik och de legala förutsättningarna för integritetsskyddet.

Ett dygn med familjen Svenssons elektroniska spår

I del VI finns en vardaglig beskrivning av några integritetsrisker som en vanlig familj kan drabbas av under ett dygn. Syftet är att på ett lättillgängligt sätt redovisa hur modern teknik påverkar den personliga integriteten.

Sammanfattningsvis

I detta betänkande redogör kommittén för behandlingen av personuppgifter inom ett antal områden som en enskild person kommer i kontakt med i olika livsskeden och gör en riskbedömning av dessa. Vi beskriver därtill några vanliga generella företeelser, som har inverkan på den personliga integriteten. Vi drar också vissa slutsatser

beträffande den samlade effekten för en enskild person av all den insamling och lagring av personuppgifter, kartläggning och övervakning som han eller hon deltar i eller blir föremål för.

Den digitala utvecklingen innebär en genomgripande förändring av samhället och enskildas livsvillkor. Personuppgifter i digital form genereras och används i allt högre grad inom alla samhällsområden. Antalet aktörer ökar, användningsområdena ökar, lagringstiderna ökar, spridningen och utbytet mellan aktörerna ökar, vidareanvändningen hos respektive aktör ökar liksom spridningen över nationsgränserna. Vi ser också att vissa stora aktörer, som en följd av utvecklingen i stort och deras egna affärsstrategier, får tillgång till en allt större mängd personuppgifter och därmed har möjlighet att teckna en alltmer komplett bild av en enskild person. Ur den enskildes perspektiv innebär utvecklingen att kunskapen om hur uppgifterna hanteras, liksom möjligheten att påverka detta, hela tiden krymper i förhållande till den ökande hanteringen av personuppgifter i samhället.

I motsvarande mån begränsas även den enskildes möjlighet att genom ett verkligt fritt val bestämma hur uppgifter om honom eller henne ska hanteras. Integritetskommitténs generella slutsats är därför att den enskilde – parallellt med den digitala utvecklingen – utsätts för stegvisa försämringar av den personliga integriteten.

Självfallet innehåller den digitala utvecklingen en enorm nyttopotential, men i det här delbetänkandet har vi fokuserat på faktiska och potentiella risker.