Hur står det till med den personliga integriteten?

– en kartläggning av Integritetskommittén

Delbetänkande av Integritetskommittén

Stockholm 2016

STATENS OFFENTLIGA UTREDNINGAR

SOU 2016:41

Innehåll

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 kameröverväkning
- 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.