Remissvar – Så stärker vi den personliga integriteten (SOU 2017:52)

Internetstiftelsen i Sverige (IIS) är en oberoende allmännyttig organisation som verkar för positiv utveckling av internet i Sverige. Vi ansvarar för internets svenska toppdomän .se, med registrering av domännamn samt administration och teknisk drift av det nationella domännamnsregistret. Sedan september 2013 sköter IIS också drift och administration för toppdomänen .nu. En av IIS visioner är att vi vill ha ett internet för alla. Alla människor i Sverige ska ha samma rätt och möjlighet att utnyttja internets tjänster. Internet ska vara säkert, användarna ska känna sig trygga och kunna lita på tjänster på internet. Det är viktigt för IIS att medborgarnas rätt till integritet skyddas vid användning av informationsteknik. IIS har fått möjlighet att lämna remissvar på Integritetskommitténs slutbetänkande och lämnar följande synpunkter.

Allmänna synpunkter

Integritetskommittén har i sitt slutbetänkande, Så stärker vi den personliga integriteten, presenterat flertalet förslag på åtgärder för att minska risker för den personliga integriteten som identifierades under utredningsarbetet och som presenterades i delbetänkandet Hur står det till med den personliga integriteten? (SOU 2016:41).

IIS ställer sig positiv till slutbetänkandets slutsatser och förslag. Det är uppenbart att den personliga integriteten är en viktig fråga med tanke på de många utredningsuppdrag som regeringen har lagt ut för att hantera detta inom många olika politikområden. Därtill ställer den nya dataskyddsförordningen stora krav på alla verksamheter som hanterar personuppgifter i någon form.

Integritetskommitténs förslag innebär enligt IIS tydligare förhållningsregler och ökat stöd för hanteringen av personuppgifter. Förhoppningsvis kommer detta att leda till en säkrare hantering och därmed ett bättre skydd av den personliga integriteten för individen.

Detaljerade synpunkter

Skolan

IIS ställer sig bakom integritetskommitténs förslag att regeringen bör ge Skolverket i uppdrag att initiera och stödja utarbetandet av uppförandekoder för skolan. Vidare anser IIS att det är viktigt att regeringen skyndsamt utreder behovet av stärkt sekretesskydd för elevarbeten, eftersom elevernas digitala avtryck är avsevärt och kommer följa elever under hela deras digitala liv. IIS anser också att det är av största vikt att det är tydligt hur, samt för vad,

eventuellt tillgängliggörande och vidareanvändning av data från skolornas system ska uppmuntras så att det system och tjänster som utvecklas gynnar lärandet och skolans arbete.

Arbetslivet

IIS ställer sig bakom integritetskommitténs förslag att regeringen bör ge Arbetsmiljöverket i uppdrag att initiera och stödja utarbetandet av uppförandekoder för arbetslivet. Enligt IIS bör detta ske i samråd med Datainspektionen. Förutom de frågor som utredningen anser kan tas upp i uppförandekoder kan det också vara lämpligt att tillföra spårbarhet, det vill säga, vem som de facto har behörighet och befogenhet att hantera personinformation i olika situationer och att det framgår i loggar som arkiveras under lämplig tid.

Hälso- och sjukvård

Hälso- och sjukvården är den sektor där integritetskommittén konstaterat att allvarliga risker uppstår i samband med informationshantering till följd av allt från bristande ledning till bristande informationssäkerhet och regelefterlevnad. IIS anser att det här behövs omfattande utbildningsinsatser för att minska förekomsten av incidenter där anställda inom sektorn överträder sina befogenheter. Uppförandekoder bör vara gemensamma för hela sektorn, oavsett landsting eller huvudman. IIS uppmuntrar att den norska normen för informationssäkerhet används som en förebild i arbetet. Vi ställer oss också bakom de förslag som integritetskommittén lägger fram om att genomföra befintliga förslag från tidigare utredningar.

E-förvaltning

IIS stödjer helt och fullt förslaget om att den nya myndigheten med samlat ansvar för den offentliga förvaltningens digitalisering även får ansvar för att främja skyddet av den personliga integriteten och ge råd och rekommendationer om lösningar som nyttjar integritetsskyddande arbetssätt och teknik.

IIS förordar ett samordnat program för e-förvaltning bestående av skydd av personlig integritet, informationssäkerhet och säkerhetsskydd med hänsyn till rikets säkerhet. Som utredningen konstaterar finns det motsättningar mellan de myndigheter som driver digitaliseringen och de tillsynsansvariga myndigheterna, vilket ofta kan förklaras med bristande samordning och samverkan. Det kommer enligt IIS uppfattning att vara av yttersta vikt för att nå framgång i arbetet att det finns ett mycket väl fungerande samarbete mellan ansvariga myndigheter, allt från den myndighet som får det samordnade tillsynsansvaret till Konsumentverket, Skolverket, Datainspektionen med flera.

Beträffande molntjänster anser IIS att de åtgärder som vidtagits efter incidenten med Transportstyrelsen tyder på brådska och att det vore lämpligare att fördjupa utredningen som föreslagits från Statens Servicecenter och närmare analysera förutsättningarna för att inrätta en ”statens molntjänst” i enlighet med

förslagen i rapporten. De uppdrag som så här långt givits till Försäkringskassan respektive PTS är otydliga i sin formulering och riskerar att bidra till mer splittring än samordning.

Det kompetenscenter som föreslagits genom att utse en myndighet eller annan aktör för vägledning och kunskapsutbyte mellan myndigheter i frågor som rör anskaffning och användning av externa it-tjänster kan med fördel placeras hos den föreslagna Digitaliseringsmyndigheten, medan Statens Servicecenter kan göras operationellt ansvarigt enligt förslaget ovan.

IIS understryker vikten av integritetskommitténs förslag om att regeringen bör komplettera sina digitala strategier med en formulering om att Sverige ska bli världsledande på att skydda den personliga integriteten utan att minska takten i digitaliseringen. Att bli bäst i världen på att använda digitaliseringens möjligheter får aldrig ske på bekostnad av skyddet av den personliga integriteten. För det ändamålet bör regeringen också stödja aktuella och pågående strävanden inom EU att tillåta end-to-end-kryptering utan bakdörrar.[1]

Konsumentområdet

IIS tillstyrker utredningens förslag.

Försäkringsverksamhet

IIS stödjer utredningens förslag om att vidta de utredningsåtgärder som är nödvändiga för att genomföra en lagreglerad tystnadsplikt för försäkringsföretagen och deras anställda avseende personuppgifter.

Åtgärder inom några andra områden med allvarliga eller påtagliga risker

Bank- och kreditmarknad

IIS stödjer utredningens förslag om att låta utreda hur en säker ordning för utfärdande av fysiska legitimationer ska se ut och hur statens ansvar för den ska vara utformad. Vi ställer oss också bakom förslaget om att låta utreda möjligheten till en författningsreglerad rättighet för fysiska personer att vända sig till den som ger ut en kreditupplysningspublikation för att få uppgifter om sig själv strukna innan uppgifterna publiceras. Detta kan göras med utgångspunkt i förslag som redan ligger.

De brottsbekämpande myndigheternas verksamhet

IIS stödjer förslaget om att låta utreda en lagreglering av sådana integritetskänsliga spaningsmetoder som idag inte är reglerade eller har svag reglering.

---

[11] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0324+0+DOC+PDF+V0//SV

Informationssäkerhet

Sedan betänkandet lades fram har regeringen lagt fram en nationell strategi för informations- och cybersäkerhet. Strategin är i stora delar av karaktären vision, och saknar i vissa avseenden mätbara mål.

Om det är så att man ska ge MSB ökat mandat och ökat ansvar, och att de dessutom ska ges i uppgift att bedriva tillsyn över statliga myndigheters arbete med informationssäkerhet anser IIS att det kräver att MSB själva föregår med gott exempel och ser över sitt arbete med informationssäkerhet.

Krav på incidentrapportering som kommer inte bara av GDPR och NIS, utan också av reglering inom energibranschen och säkerhetskyddsförordningen skapar stor osäkerhet kring vad som ska rapporteras till vilken myndighet. Från statens sida vore det av stort värde om man inrättade en så kallad ”one stop shop” där incidentrapporter lämnas, oavsett vilket lagrum incidenten ska hänföras till. På så sätt går det förmodligen enklare för den rapporterande organisationen att hålla sig inom de tidsramar som krävs, och att det är en rapport som lämnas, även om incidenten träffar flera lagrum, vilket kanske inte är omöjligt.

Förslaget om att MSB ska få i uppdrag att beträffande myndigheter under regeringen följa upp vilka åtgärder myndigheterna vidtar för att följa kraven i MSB:S föreskrifter (MSBFS 2016:1) om statliga myndigheters informationssäkerhet kan tillgodoses genom att MSB upphandlar extern revision så som om det vore revision enligt den internationella standarden ISO 27001. Det är av stor vikt att säkerhetsarbetet bedrivs riskbaserat och systematiskt och på ett sätt som gör att man kan mäta framsteg. En gemensam modell för mätning av mognadsgrad för informationssäkerhet bör definieras för att man därefter ska kunna genomföra jämförelser (benchmarking) av var olika myndigheter och verksamheter befinner sig.

Uppförandekoder

IIS stödjer utredningens förslag om att de insatser som föreslås i betänkandets olika delar för att åstadkomma uppförandekoder också bör innehålla informationssäkerhetsåtgärder som ett framträdande inslag.

En nationell styrmodell

IIS anser att någon myndighet bör få i uppdrag att i samverkan med andra myndigheter utveckla, förvalta och vidareutveckla en styrmodell för statens informationssäkerhet, men att det inte med självklarhet ska ske hos MSB. Det skulle kunna vara en uppgift för den nya Digitaliseringsmyndigheten. Det viktiga är att det finns ett för myndigheterna gemensamt förhållningssätt till informationssäkerhetsfrågor, att man har en modell till stöd för benchmarking och att man genomför återkommande externa revisioner av myndigheternas ledningssystem som stöd i deras förbättringsarbete.

IIS saknar tekniska aspekter i beskrivningen av en samlad modell och vad denna ska innefatta. En grundskyddsnivå ska även innehålla krav på tekniska åtgärder, medan själva implementationen av dessa kan ske på många olika sätt.

Stockholm den 10 november 2017

Danny Aerts

Vd, Internetstiftelsen i Sverige