Finansdepartementet
Fi2018/01418/DF

Remissvar – Juridik som stöd för förvaltningens digitalisering (SOU 2018:25)

Stiftelsen för Internetinfrastruktur (Internetstiftelsen) 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 Internetstiftelsen också drift och administration för toppdomänen .nu.

Internetstiftelsens vision är att alla i Sverige vill, vågar och kan använda internet.

Internetstiftelsen har fått möjlighet att lämna remissvar och lämnar följande övergripande synpunkter.

Inledning

Internetstiftelsens bedömning är att utredningen har gjort ett grundligt och väl genomarbetat underlag som belyser relevanta delar för att stärka den digitala förvaltningen. Internetstiftelsen välkomnar betänkandet och ställer sig i allt väsentligt positivt till utredningens förslag.

Såsom utredningen konstaterar instämmer Internetstiftelsen i att insyn är av stor betydelse för att enskildas tillit till den digitala förvaltningen ska upprätthållas. Men att det även kan öppna upp för olika risker vilket innebär att stora krav behöver ställas på god informationssäkerhet.

Internetstiftelsen instämmer vidare i att värdegrunder såsom rättssäkerhet, skydd för personlig integritet och välavvägd sekretess för skyddsvärda uppgifter har en avgörande betydelse för allmänhetens förtroende för den offentliga verksamheten. Löpande bedömning av regleringen är dock viktigt för att tillse att utveckling och digitalisering som är önskvärd är möjlig. Att finna balansen är nödvändigt.

Synpunkter

Internetstiftelsen instämmer i att myndigheter ska vara skyldiga att tillhandahålla, och på lämpligt sätt anvisa, en eller flera digitala mottagningsfunktioner dit handlingar kan förmedlas, om det inte är olämpligt av säkerhets- eller andra skäl. Att bidra till förenklingar för den enskilde och stärka möjligheten till digitala lösningar är positivt, dock är det viktigt att poängtera behovet av att tillse att de digitala lösningarna säkerställer bland annat säkerheten och skyddet för den personliga integriteten. De digitala lösningarna måste tas fram med medborgarperspektivet snarare än verksamhetsperspektivet.

Internetstiftelsen instämmer i att det finns behov av att klargöra de rättsliga förutsättningarna för utkontraktering av it-drift och andra it-baserade funktioner från myndigheter till privata leverantörer. Detta eftersom det är tydligt att det föreligger oklarheter när det gäller de rättsliga förutsättningarna bland annat för att lämna ut sekretessreglerade uppgifter.

Internetstiftelsen instämmer vidare i att myndigheter i den offentliga förvaltningen bör tillhandahållas stöd i arbetet med att formulera juridiskt hållbara och affärsmässigt gynnsamma villkor i it-avtal samt stöd i framtagandet av personuppgiftsbiträdesavtal. Internetstiftelsen har inget att erinra mot att nämnda myndigheter får till uppgift att genomföra uppdraget.

Att skapa ett kompetenscenter för juridiska frågor inom digitaliseringsområdet är ett positivt förslag som kan bidra till att möjliggöra den digitala förvaltningen samtidigt som behovet av att tydliggöra de rättsliga förutsättningarna och minska osäkerheten hos myndigheter.

Särskilt om informationssäkerhet

Internetstiftelsen väljer att samla alla synpunkter rörande informationssäkerhet under en rubrik.

Först och främst vill Internetstiftelsen understryka att informationssäkerhet i detta sammanhang är ett bättre begrepp än cybersäkerhet. Även om cybersäkerhetsbegreppet är vanligt förekommande i en internationell kontext finns det inte någon samsyn på vad innebörden är. Internetstiftelsen anser att cybersäkerhetsbegreppet bör avgränsas till det behov av säkerhetsåtgärder som kommer av risken att drabbas av antagonistiska hot, medan informationssäkerhet mer handlar om det behov av säkerhet som kommer av informationshantering generellt, det vill säga både oavsiktliga och avsiktliga hot.

Internetstiftelsen välkomnar utredningens noggranna genomgång av behovet av informationssäkerhet inom den digitala förvaltningen. Det råder enligt Internetstiftelsen ingen tvekan om att god informationssäkerhet är nödvändig i förvaltningens digitalisering och att dessa frågor behöver belysas särskilt. En genomgående informationssäkerhet är en nödvändig förutsättning för att enskilda ska ha ett högt förtroende för den offentliga förvaltningen. Internetstiftelsen vill betona att det vilar ett tungt ansvar på offentlig förvaltnings ledningar och beslutsfattare, i rollerna som beställare av it-system som stöd för digitalisering i offentlig sektor, att göra informationssäkerhet till en integrerad del av verksamheten. Att med utgångspunkt i vad som är skyddsvärt, kunna identifiera hotbilden och analysera riskerna är naturliga inslag. Det är viktigt att inse att många risker har sitt ursprung i det faktum att riskaptiten inte är tydliggjord, att kravställningen brister eller att lösningar är undermåliga och ibland rentav dysfunktionella. Internetstiftelsen framförde redan i remissvaret på betänkandet Reboot – omstart för den digitala förvaltningen (SOU 2017:114) följande:

Enligt Internetstiftelsens uppfattning *måste informationssäkerhetsarbetet inom offentliga myndigheter styras på ett mer kraftfullt sätt och krav måste ställas på att det ska genomsyra samtliga digitaliseringsprocesser. För tio år sedan kunde inte i princip vem som helst slå ut elnätet i Sverige från var som helst i världen. För tio år sedan kunde inte i princip vem som helst slå ut de digitala systemen i Göteborgs hamn från var som helst i världen. För tio år sedan kunde inte vem som helst sätta ihop ett botnät av internetanslutna webbkameror och slå ut ett stort antal myndigheters namnserver- och webbtjänster samtidigt. Av dessa exempel har de två sistnämnda redan inträffat.*

Idag bygger digitaliseringen på att allt ska vara uppkopplat och sammankopplat samtidigt som vi saknar förmågan att applicera ett relevant skydd, eftersom var och en hanterar sin egen isolerade del (se ovan under En myndighet med samlat ansvar).
Internetstiftelsen har vid tidigare tillfällen kommenterat att informationssäkerhetsarbetet är uppdelat på för många olika och delvis överlappande ansvarsområden på både departements- och myndighetsnivå.

***Internetstiftelsen välkomnar** utredningens förslag om att regeringen behöver inleda ett arbete att samordna och strukturera reglering inom informationssäkerhetsområdet och att regeringen ger den nya digitaliseringsmyndigheten i uppdrag att ta fram och mäta nyckeltal för informationssäkerhetsrelaterade aspekter i syfte att följa informationssäkerhetsmognaden i förhållande till digitaliseringen.*

***Internetstiftelsen är också positiv till** att regeringen tar fram rättsliga krav som omfattar samtliga offentliga myndigheter att införa ett systematiskt och riskbaserat informationssäkerhetsarbete och i det sammanhanget ge MSB i uppdrag att utreda hur tillsyn över informationssäkerhetsområdet och förbättringar av kraven på incidentrapportering kan genomföras.*

***Internetstiftelsen delar uppfattningen** att det bör utredas ytterligare hur alla offentliga myndigheter kan omfattas av en för hela den offentliga förvaltningen gemensam reglering gällande tillsyn av informationssäkerhetsarbetet med tillhörande incidentrapportering. Samtidigt är det viktigt att konstatera att det inte rapporteras tillräckligt idag, men att öka kraven på tvingande rapportering, kommer det verkligen att hjälpa?*
*Erfarenheter från CERT-verksamhet i andra delar av världen visar att det finns en direkt korrelation mellan kvaliteten på rapporter som en CERT skapar och intresset för att bidra rapportering. Tyvärr upprepas kravet på tvingande rapportering som lösning när det finns oklarheter om huruvida det verkligen leder till önskat mål. Om vi tar flygsektorn som exempel har de som mål att varje typ av incident ska drabba **sektorn** endast en gång, inte **varje enskild aktör** en gång. Det är ett relevant mål som även borde omfatta IT- och cybersäkerhetsområdet.*

Hela remissvaret finns här https://www.iis.se/docs/Remissvar-IIS-reboot-2017-114.pdf

Enligt regeringen läggs årligen 45 miljarder kronor på it inom offentlig sektor[1] och det är enligt Internetstiftelsens mening nödvändigt att informationssäkerhetskraven är med från början i upphandlingsprocessen.

Internetstiftelsen delar utredningens uppfattning att ett mer sammanhållet arbete med informationssäkerhet i den offentliga förvaltningen har potential att effektivisera den digitala utvecklingen utan att säkerheten åsidosätts. Vi ställer oss dock lite tveksamma till att detta skulle kräva att det utformas en generell informationssäkerhetsreglering. Det kan finnas andra medel än reglering för att stärka informationssäkerheten i hela den offentliga förvaltningen, till exempel genom att ge ett mer uttalat och tydligt samordningsansvar och stödfunktion hos den nyligen etablerade Myndigheten för digital förvaltning.

Den reglering som finns idag är omfattande, har tillkommit vid olika tidpunkter, utifrån olikartad terminologi och utan strukturerat inbördes samband. Det är en försvårande omständighet för den

[1] http://www.regeringen.se/regeringens-politik/digitalisering/digital-forvaltning/

offentliga förvaltningen att myndigheter under regeringen har en typ av reglering, medan till exempel kommuner har en annan, och det existerar en tredje inom hälso- och sjukvården. Internetstiftelsen är positiv till den nu aktuella utredningens förslag att låta utreda förutsättningarna för att ta fram en kompletterande reglering om informationssäkerhet som omfattar hela den offentliga förvaltningen för att klargöra fakta om vad som behövs i form av reglering. Med tanke på att det redan finns en hel del reglering rörande informationssäkerhet som träffar olika aktörer och information, med delvis olika syften, spridd i olika föreskrifter kan det vara nyttigt att göra en sådan översyn. I synnerhet som det redan pågår ett antal utredningar och andra initiativ som syftar till att ytterligare stärka informationssäkerheten i den offentliga förvaltningen. **Internetstiftelsen tillstyrker** därför förslaget om en enad lagstiftning på området, i kombination med föreskriftsrätt som innebär att en grundskyddsnivå för informationssäkerhet ska gälla inom hela den offentliga sektorn.

Internetstiftelsen vill betona att medborgare, organisationer och företag måste kunna ställa berättigade krav både på öppenhet om hur den digitala förvaltningen arbetar med informationssäkerhet och att den digitala förvaltningen upprätthåller en hög säkerhet när myndigheternas informationsmängder bearbetas, lagras och kommuniceras. Idag saknas medborgarperspektivet till stor del. För att myndigheter dessutom ska kunna ha tillit till varandras informationssäkerhet behöver en gemensam grundskyddsnivå etableras och verifieras, i synnerhet om samverkan om informationsutbyten ska kunna komma till stånd. En sådan grundskyddsnivå behöver specificeras och specifikationerna måste förvaltas över tid. Det skulle till exempel kunna uppnås genom att Sverige genomför en motsvarighet till den norska Normen[2]. Med utgångspunkt i relevant lagstiftning (vilka krav som ställs) omsätts detta i specifikationer med funktionella krav (vad som krävs för att lagkraven ska uppfyllas) till specifika åtgärder hos varje enskild myndighet (hur man väljer att införa funktionella krav).

Internetstiftelsen anser att det krävs ett resonemang kring hur säkerhetsfunktioner ska utvecklas, införas, valideras, kontrolleras, följas upp och användas i det civila samhället i dag, det vill säga säkerhet som bygger på öppna standarder, öppen kod och en mångfald leverantörer. Det borde som Internetstiftelsen ser det vara självklart att sträva efter att all kommunikation ska skyddas med moderna metoder.

Uppföljning och kontroll är centralt för att regleringen ska bli effektiv. Krisberedskaps-förordningen och MSB:s föreskrifter gällande statliga myndigheters arbete med informationssäkerheten har varit gällande i över 10 år, men ändå är mognadsgraden och följsamheten gentemot dessa lagar och författningar i många fall påtagligt bristfällig. Att reglering i sig inte löser frågan är således uppenbart och bevisat. När frågan om kompetensförsörjningen har klarats ut krävs också en effektiv apparat för att säkerställa att gällande krav uppfylls. Att genomföra denna typ av kontroll genom en tillsynsmyndighet eller riksrevisionen är möjligen inte bästa vägen från resurs- och effektivitetssynpunkt. Inte heller kan det förväntas att en sådan uppföljning och kontroll blir så pass heltäckande att de efterfrågade resultaten uppnås. Alternativ som kan övervägas är krav i regleringen om interna revisioner, och att såväl revisionsplan som resultat av sådana revisioner löpande ska tillhandahållas ansvarig tillsynsmyndighet.

Det absolut största hindret för god säkerhet i den offentliga sektorn är kompetens-försörjning. Till detta hör den offentliga sektorns utmaningar att uppfylla de mål och krav som EU har börjat ställa

[2] https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet

på en ökad digitalisering av den offentliga sektorn. Det är orimligt att varje myndighet ska kunna hålla sig med den kompetens som krävs för att kunna avväga risker, utforma och införa effektiva åtgärder, kontrollera följsamhet på rättsliga krav och avtal. Därtill tillkommer svårigheterna att upphandla effektivt utifrån sådan avvägning av risk gentemot kostnader. Det ligger i sakens natur att det mellan en vald leverantör och myndigheten finns motstridiga intressen då ett avtal väl är ingått. En ny reglering på området måste därför även ta i beaktande hur kompetensförsörjningen ska säkerställas.

Det sätt på vilket sätt förvaltningen svarar upp mot kraven på informationssäkerhet måste bedömas i varje enskilt fall, men mot gemensamma specifikationer, grundskyddsnivån. Den bedömningen lämpar sig bäst för informationssäkerhetsstöd i form av exempelvis tredjepartsrevisioner, där någon utifrån granskar arbetet med informationssäkerhet. Ett sätt att få detta på plats är att ställa krav på att alla myndigheter är certifierade mot ISO 27001, Ledningssystem för informationssäkerhet.

Ett stort antal statliga utredningar har genom åren lämnat ett ännu större antal förslag som syftar till att stärka informationssäkerheten i den offentliga förvaltningen. Internetstiftelsens uppfattning är att få av dessa förslag har genomförts med någon tydlig utgångspunkt från välformulerade mål för regeringens ambitioner med myndigheternas informationssäkerhetsarbete. Det är en brist som måste hanteras.

Internetstiftelsen vill betona att regeringen som ett första steg behöver definiera mål för informationssäkerheten i den offentliga förvaltningen och bland annat ange vilket skydd som behövs, för vilka det behövs, hur måluppfyllelse ska mätas och hur informationssäkerhet ska definieras. Ett riskbaserat arbetssätt är både nödvändigt och önskvärt. Det som behövs är en modell som har förutsättningar att lyfta hela det civila Sveriges samhällsapparat säkerhetsmässigt. Det skulle enligt Internetstiftelsen kunna vara en del av den föreslagna utredningens uppgift att definiera.

Samordnad och säker IT-drift för statlig förvaltning
Regeringen har gett Försäkringskassan i uppdrag att åren 2017-2020 erbjuda vissa myndigheter en samordnad och säker IT-drift. En delrapport levererades november 2017 och en slutredovisning ska ske till regeringen senast den 18 december 2020. Hur regeringen kommit fram till slutsatsen att Försäkringskassan är den lämpligaste partnern för en samordnad och säker it-drift för lämpliga myndigheter är emellertid enligt Internetstiftelsen inte uppenbart.

Statens servicecenter fick redan den 28 januari 2016 i uppdrag av regeringen att analysera och föreslå vilka myndighetsfunktioner som kan vara lämpliga att bedriva samordnat inom staten och utanför storstadsområden. Uppdraget redovisades i april 2017 i rapporten En gemensam statlig molntjänst för myndigheternas it-drift. Förslaget innebär i korthet inrättandet av en gemensam statlig molntjänst för hela den statliga förvaltningen, baserad på maximalt tio datacenter (jämfört med dagens cirka 200) som ska leverera drift baserad på virtuella servrar och gemensamma verktyg baserade på öppna standarder. Analysen visar att en gemensam statlig molntjänst innebär kostnadsbesparingar, minskar miljöpåverkan, eliminerar behovet av separata upphandlingar för varje myndighet, ökar leverantörsoberoendet och kan erbjuda hög tillgänglighet vid varje enskilt tillfälle.

Enligt Internetstiftelsens uppfattning är förslaget från Statens servicecenter ett väl genomarbetat förslag. Rapporten har såvitt Internetstiftelsen vet inte resulterat i några ytterligare åtgärder, som till exempel fördjupad utredning inom vissa områden.

Internetstiftelsen lyfte redan i ett tidigare remissvar på betänkandet SOU 2017:23, Digital förvaltning, fram förslaget från Statens Servicecenter som ett förslag som bör övervägas, och vi anser fortfarande - liksom den nu aktuella utredningen - att regeringen skyndsamt och mer i detalj bör analysera förutsättningarna för en sådan molntjänst och om den är bäst lämpad att drivas i statligt ägande eller om det är något som marknaden kan bistå med, givet de legala, tekniska och säkerhetsmässiga förutsättningar som finns.

Stockholm den 3 oktober 2018

Danny Aerts
Vd, Stiftelsen för Internetinfrastruktur