

Stockholm den 18 september 2018

R-2018/0991

Till Finansdepartementet

Fi2018/01418/DF

Sveriges advokatsamfund har genom remiss den 23 maj 2018 beretts tillfälle att avge yttrande över Digitaliseringsutredningens betänkande Juridik som stöd för förvaltningens digitalisering (SOU 2018:25).

Sammanfattning

Utredningen lägger fram förslag som Advokatsamfundet ser som angelägna från bland annat integritets- och rättssäkerhetssynpunkt. På flera punkter saknas emellertid en genomlysning av gällande rätt, t.ex. av vad som får anses vara ett röjande och hur personuppgiftsansvarets fördelning ska kunna förenas med skyddet för privatlivet i myndigheters digitala tjänster. Dessutom förekommer allmänna uttalanden om ett osäkert rättsläge som, om de inte konkretiseras, kan onödigtvis hindra eller försena digitaliseringen. Förslagen bör i dessa delar beredas ytterligare.

God offentlighetsstruktur

Advokatsamfundet ifrågasätter placeringen av de föreslagna reglerna om information om digitala källor för ärendehandläggningen och om användningen av algoritmer och datorprogram (se förslagen i 4 kap. 3 och 3 a §§offentlighets- och sekretesslagen [2009:400]). Sådana regler rör ärendehandläggning och synes lämpligen höras hemma i förvaltningslagen (2017:900).

Digitala mottagningsfunktioner

Advokatsamfundet tillstyrker de förslag som nu på nytt läggs fram om regler i förvaltningslagen beträffande anvisning av digitala mottagningsfunktioner och när handlingar som förmedlats till anvisad digital mottagningsfunktion ska anses ha kommit in. De komplikationer från rättssäkerhetssynpunkt som det s.k. E-samverkansprogrammet (eSam) berört i ett rättsligt uttalande den 26 oktober 2017 om ankomstdag för elektroniska handlingar och en promemoria den 31 oktober 2017 om inkommande handlingar, skulle därmed i allt väsentligt bli undanröjda.

Beträffande inkommande finns dessutom särreglering för vissa förvaltningsområden. Dessa föreskrifter innebär vanligtvis att data som representerar handlingen ska ha nått en viss elektronisk ”plats”. Handlingen ska ha anlänt till en anvisad del av ett system eller ett mottagningsställe. Som exempel kan nämnas 111 kap. 7 § socialförsäkringsbalken, där det föreskrivs att handling kommit in när den har anlänt till den del av ett system för automatiserad behandling som anvisats som mottagningsställe. Ett annat exempel finns i 19 kap. 10 a § jordabalken, där det beträffande elektroniska dokument föreskrivs att de ska lämnas till ett mottagningsställe som inskrivningsmyndigheten har anvisat och att ansökan ska anses ha kommit in till inskrivningsmyndigheten när den har anlänt till ett sådant mottagningsställe. Denna särreglering bör utmönstras och ersättas av förslagen i det remitterade betänkandet.

Automatiserade beslut

Så som utredningen anfört är det betydelsefullt att, i enlighet med E-delegationens förslag i betänkandet Automatiserade beslut – färre regler ger tydligare reglering, utmönstra den särreglering av automatiserat beslutsfattande som alltså finns kvar vid sidan av 28 § förvaltningslagen. I samband härmed bör även kommunallagen (2017:725) anpassas för att tillåta automatiserade beslut.

Personuppgiftsansvar och behovet av skydd för privatlivet

Persondataskyddet behöver inte bara förenas med reglerna i dataskyddsförordningen. Europakonventionens skydd för hem och familj måste också beaktas. Det hade varit positivt om även denna reglering tagits upp i det remitterade betänkandet, utifrån principen att EU-rätten ska ses som en helhet där olika skyddsintressen får avvägas mot varandra.

Advokatsamfundet har redan i ett remissvar från april detta år över SOU 2017:114 beskrivit hur utvecklingen inom e-förvaltningen inverkat på skyddet för enskilda när de ska upprätta, granska och ge in handlingar med stöd av eget utrymme. I traditionell fysisk miljö har användaren sin bostad eller sitt arbetsrum där skydd ges mot insyn av utomstående. På samma sätt hanterade användaren inledningsvis utkast o.l. i sin egen dator utan uppkoppling via nät. Behandlingen utfördes därmed skyddat i den lokala miljö som användaren förfogar över. Myndigheterna har emellertid, som utredningen beskrivit,

valt att utveckla digitala tjänster så att användare skriver sina utkast på servrar som finns under myndigheters kontroll. Nya risker uppkommer därmed för den enskilde, särskilt som den beskrivna ”flytten” från användarens privata miljö till myndigheters och företags servrar enligt vad utredningen anfört ska drivas så långt att den enskilde inte längre anses vara personuppgiftsansvarig för den behandling som äger rum av dennes privata material. Skyddet enligt 2 kap. 6 § regeringsformen för användarnas integritet måste upprätthållas. Dessa frågor behöver genomlysas, lämpligen utan konstlade resonemang kring tekniska begränsningar rörande registerutdrag o.l.

En lösning kan visserligen övervägas i enlighet med dataskyddsförordningens regler om ett gemensamt personuppgiftsansvar och överenskommelser om ansvarets fördelning. Advokatsamfundet delar också utredningens bedömning att det även när personuppgiftsansvaret inte är gemensamt bör vara möjligt att fastställa fördelningen av personuppgiftsansvaret i t.ex. en överenskommelse. Till skillnad från fysisk miljö där skyddet för den rumsliga integriteten är starkt kvarstår emellertid att skyddet för privatlivet i motsvarande elektroniska miljö riskerar att inskränkas alltmer med den bedömning som utredningen gör.

Eget utrymme och ”rättslig osäkerhet”

Advokatsamfundet delar inte den bedömning som utredningen ger uttryck för beträffande ”rättslig osäkerhet” vid användning av eget utrymme. Av regeringens uttalanden i propositionen Utökad sekretesskydd i verksamhet för teknisk bearbetning och lagring (2016/17:198) framgår att eget utrymme, om det utformats på ändamålsenligt sätt, kan tillhandahållas inom ramen för undantaget från allmän handling i 2 kap. 10 § tryckfrihetsförordningen. Dess ”kärna” torde numera vara etablerad.

Ytterligare rättslig osäkerhet bör inte onödigtvis skapas kring denna för den digitala förvaltningen centrala rättsfigur, jfr hur eSam i en juridisk vägledning för verksamhetsutveckling inom e-förvaltning (avsnitt 2.6) redovisat krav som behöver vara uppfyllda när eget utrymme tillhandahålls.

Det är en annan sak att helt nya mer långtgående användningssätt i anknytning till eget utrymme eller bristfällig utformning av ett sådant kan föra med sig rättsverkningar som inte varit avsedda vid användning av ett sådant utrymme.

Informationssäkerhet

Utredningens genomgång av berörda regelverk och det informationssäkerhetsarbete som varje myndighet är skyldig att bedriva ger bilden av ett växande, svåröverblickbart och fragmenterat rättsområde. Ny teknik och eskalerande hot och risker driver fram nya krav och nya regler. Detta har lett till såväl överlappande regler som att det upplevs finnas luckor i regleringen. Sammantaget skapar detta en osäkerhet i den praktiska hanteringen som för med sig negativa effekter från bl.a. säkerhets-, verksamhets- och kostnads-synpunkt.

Det finns således ett behov av att klargöra dessa regler och förutsättningar inte bara vid outsourcing utan beträffande myndigheternas informationshantering i stort.

Advokatsamfundet har i flera tidigare remissvar pekat på dessa behov och vill på nytt betona vikten av samordnade åtgärder som kan säkerställa en sund utveckling inom området. Utredningen har emellertid inte funnit förutsättningar att nå framgång med att klargöra de gränsdragningsfrågor som aktualiseras. Enligt Advokatsamfundets mening är det dock inte tillräckligt att, så som utredningen förordat, noga följa hur praxis utvecklas inom området (s. 324).

Utkontraktering och en bestämmelse om tystnadsplikt

Advokatsamfundet motsätter sig inte en regel om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring. Det är emellertid olyckligt att utredningen har lämnat den centrala frågan om *när ett röjande ska anses ha skett* därhän och i stället genom uttalanden i betänkandet tillfört ytterligare bränsle till en osäkerhet om vad som är ett röjande. Denna rättsliga osäkerhet har Advokatsamfundet uppfattat som mera begränsad, så länge det inte är fråga om molntjänster. Används t.ex. en kryptografisk metod som är godkänd för ändamålet av behörig myndighet kan en överföring via nät av uppgifter som skyddas på detta sätt inte rimligen anses vara röjda för den tjänsteleverantör som tillhandahåller nät för överföringen.

Klargörs det i lagstiftningsärendet vad som är ett röjande och förenas detta med uttalanden om att anlidade tjänster inte ska vara sådana att uppgifter röjs annat än när detta inte går att komma ifrån (t.ex. för att utföraren ibland måste ta del av vissa uppgifter), kan en ändamålsenligt utformad tystnadsplikt bli ett värdefullt komplement. Skulle en reglering inte förenas med ett klargörande av röjandefrågan blir emellertid den praktiska konsekvensen att fokus riktas mot att se till att reglerna om tystnadsplikt blir tillämpliga – i stället för att i första hand säkerställa att personal hos tjänsteleverantören inte får del av uppgifter så att de anses röjda.

Advokatsamfundet vill också ifrågasätta om det föreslagna tillämpningsområdet för tystnadsplikten är ändamålsenligt utformat. Den föreslagna lagen om tystnadsplikt gäller enligt 1 § när en myndighet uppdrar åt en privat leverantör att behandla uppgifter för ”enbart teknisk bearbetning eller teknisk lagring för myndighetens räkning”. Avtal om utkontraktering innehåller ofta olika delar, där inslag kan finnas av insatser som inte är enbart tekniska. Anses i så fall bara dessa delar vara undantagna eller faller hela tystnadsplikten och hur förhåller sig det i författningsförslaget valda uttrycket till motsvarande uttryck i 2 kap. 10 § tryckfrihetsförordningen?

SVERIGES ADVOKATSAMFUND

Anne Ramberg