Juridik som stöd för förvaltningens digitalisering

Betänkande av Digitaliseringsrättsutredningen

Stockholm 2018

STATENS OFFENTLIGA UTREDNINGAR

SOU 2018:25

SOU och Ds kan köpas från Norstedts Juridiks kundservice.
Beställningsadress: Norstedts Juridik, Kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@nj.se
Webbadress: www.nj.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Norstedts Juridik AB
på uppdrag av Regeringskansliets förvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck: Elanders Sverige AB, Stockholm 2018

ISBN 978-91-38-24780-8
ISSN 0375-250X

Till statsrådet Ardalan Shekarabi

Regeringen beslutade vid regeringssammanträde den 24 november 2016 att uppdra åt en särskild utredare att kartlägga och analysera i vilken utsträckning det förekommer lagstiftning som i onödan försvårar digital utveckling och samverkan inom den offentliga förvaltningen. Utredaren ska lämna förslag till de författningsändringar som bedöms ha störst potential att stödja den fortsatta digitaliseringen av den offentliga förvaltningen. Utredaren ska vidare bl.a. lämna förslag till hur en utvidgad rapportering av hela den offentliga förvaltningens löpande arbete med it och digitalisering kan utformas samt hur aktörerna inom förvaltningen som helhet kan samverka kring behovet av ny eller ändrad lagstiftning för att främja digitaliseringen (dir. 2016:98).

Som särskild utredare förordnades den 24 november 2016 professor Cecilia Magnusson Sjöberg.

Som sekreterare anställdes den 6 februari 2017 juristen Sara Markstedt, med förordnande fr.o.m. den 11 september 2017 som huvudsekreterare i utredningen. Som utredningssekreterare anställdes juristen Ingela Alverfors den 20 februari 2017 och hovrättsassessorn Anja Nordfeldt den 1 oktober 2017.

Som experter att biträda utredningen förordnades den 7 mars 2017 teknikchefen Daniel Akenine, Microsoft, verksamhetsutvecklaren Markus Bill, Försäkringskassan, juristen Sylvia Bylund, Tullverket, tidigare kanslirådet vid Justitiedepartementet, Kerstin Bynander, juristen Johan Bålman, eSamverkansprogrammets kansli vid Pensionsmyndigheten, juristen Malgorzata Drewniak, Lantmäteriet, departementssekreteraren Veronica Eckerby, Finansdepartementet, juristen Ylva Ehn, Socialstyrelsen, vice VD policy & kommunikation Anders Ekholm, Institutet för framtidsstudier, departementssekreteraren Nils Fjelkegård, Finansdepartementet, stadsjuristen Lena Grapp,

Uppsala kommun, stabsjuristen Désirée Veschetti Holmgren, Riksarkivet, chefsjuristen Gustaf Johnssén, Statens servicecenter, rättssakkunniga Helene Karlsson, Finansdepartementet, verksjuristen Linn Kempe, Bolagsverket, tidigare Chief Information Officer vid Kungliga biblioteket Peter Krantz, departementssekreteraren Lotta Lewin Pihlblad, Näringsdepartementet, tidigare verksjuristen vid Centrala studiestödsnämnden, numer Statens tjänstepensionsverk, Johan Lindeberg, juristen Manolis Nymark, Inera AB, förbundsjuristen Pål Resare, Sveriges Kommuner och Landsting, tidigare kanslirådet vid Justitiedepartementet, Maria Sertcanli, informationssäkerhetsspecialisten Kristina Starkerud, Myndigheten för samhällsskydd och beredskap, enhetschefen Katarina Tullstedt, Datainspektionen, verksamhetsutvecklaren Magnus Wallström, Skatteverket och avdelningschefen och chefsjuristen Mikael Westberg, Pensionsmyndigheten. Samma dag förordnades som expert kanslirådet Anders Hektor, Näringsdepartementet, som på grund av andra uppgifter inte haft möjlighet att delta i utredningens arbete. Maria Sertcanli och Kerstin Bynander entledigades från sina uppdrag den 2 oktober 2017 och samma dag förordnades rättssakkunniga Tove Axelsson, Justitiedepartementet, att vara expert i utredningen.

Utredningen redogör för uppdraget med användande av vi-form även om det inte funnits fullständig samsyn i alla delar.

Utredningen som har tagit sig namnet Digitaliseringsrättsutredningen (Fi 2016:13), överlämnar härmed betänkandet *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25).

Stockholm i mars 2018.

Cecilia Magnusson Sjöberg

/Sara Markstedt
Ingela Alverfors
Anja Nordfeldt

Innehåll

Bilagor

Sammanfattning

Inledning

Digitaliseringen beskrivs som vår tids starkaste förändringsfaktor. Tecken på detta är tillgången till smarta mobiltelefoner och stora datamängder samt utvecklingen inom artificiell intelligens (AI) och sakernas internet. Denna utveckling påverkar den grundläggande verksamheten inom den offentliga förvaltningen inbegripet dess möjligheter att tillhandahålla service till privatpersoner och företag.

Den snabba teknik- och samhällsutvecklingen kräver ett proaktivt arbete med att rättsligt analysera hur den offentliga förvaltningen påverkas av digitaliseringen och vice versa. Vi ser att det finns och kommer att finnas fortsatt behov av att anpassa lagstiftningen för att kunna stödja utvecklingen. I betänkandet utgår vi från de politiska mål och den inriktning som riksdag och regering givit och behandlar frågor om hur rättsliga utmaningar kan hanteras samtidigt som förvaltningens digitalisering främjas.

Värdegrunder i den digitala förvaltningen

De centrala värden som under lång tid burit upp den svenska förvaltningen behöver fortsatt vara en bas för den digitaliserade verksamheten. Det är givetvis angeläget att även det digitala samhället genomsyras av ett demokratiskt synsätt och att alla ska känna en grundtrygghet i den digitala förvaltningen.

För att enskildas tillit till den digitala förvaltningen ska upprätthållas är öppenhet i myndigheternas verksamhet genom möjlighet till insyn fortsatt av stor betydelse. En transparent förvaltning med ordning och reda på uppgifter och informationssamlingar är därtill en nödvändig förutsättning för att den offentliga förvaltningens

datamängder ska kunna vidareutnyttjas på ett sätt som skapar både ekonomiska och i övrigt samhällsnyttiga värden.

En allt mer digitaliserad förvaltning kan samtidigt innebära att samhället öppnar upp för olika risker. God informationssäkerhet är därför nödvändig i den digitala förvaltningen. Att krav på rättssäkerhet i grundlag och förvaltningslagstiftning följs och att dessa värden kan stärkas i den digitala förvaltningen utgör ytterligare centrala aspekter för den framtida utvecklingen. Frågor om vad som ur integritetssynpunkt kan anses tillåtet, såväl när det gäller dataskyddsreglering som sekretessreglering, är också centrala.

För att säkerställa en fortsatt trygg digital förvaltning, som också är innovativ och effektiv, har utredningen beaktat och utgått från de värden som här kort presenterats.

Kartläggning av hindrande eller hämmande lagstiftning

Vårt uppdrag är att i ett brett perspektiv kartlägga lagstiftning som i onödan försvårar digitalisering och digital samverkan inom den offentliga förvaltningen. Vi har träffat representanter för myndigheter och andra berörda aktörer vid 28 särskilda s.k. kartläggningsmöten. Vid urvalet av de verksamheter vi besökt har ansatsen varit att inhämta information ur ett brett perspektiv. I syfte att bl.a. få synpunkter från den privata sektorn har vi vidare anordnat en hearing och även sökt kunskap vid andra aktiviteter, t.ex. deltagande i olika nätverksträffar. I betänkandet presenteras den övergripande bilden av kartläggningsresultatet.

Bland områden där hindrande eller hämmande lagstiftning uppmärksammats särskilt under kartläggningen kan nämnas digital kommunikation med enskilda, frågor om elektroniska identiteter, underskrifter och annan koppling till person, frågor om grunddata, informationsförsörjning och informationsutbyten liksom frågor om digitalisering av ärendeprocesser och automation i förvaltningen. Därtill redovisar vi vårt kartläggningsresultat gällande öppenhet i den digitala förvaltningen, bl.a. vad avser rättsliga frågeställningar som rör öppna data. Kartläggningsresultat visar också på flera frågor om upphandling, utkontraktering och it-avtal. Frågor som rör myndig-

hetssamverkan, kompetens och stöd liksom samverkan kring författningsändringar har också förts fram under kartläggningen vilket redovisas i betänkandet.

En reflektion över kartläggningsresultatet är att lagstiftningen i vidsträckt bemärkelse omfattande lag, förordning eller föreskrift, kan hindra eller hämma digital utveckling inom förvaltningen på flera sätt; genom uppenbara rättsliga hinder, rättslig osäkerhet eller genom avsaknad av reglering.

Automation i förvaltningen

I betänkandet analyseras om gällande rätt nu och framöver möjliggör en tillräckligt god offentlighetsstruktur för att säkerställa insyn i hur förvaltningens verksamhet bedrivs. Detta gäller särskilt vid automatiserade förfaranden när algoritmer med anknytande datorprogram får en allt mer framträdande roll i myndigheters verksamhet. Frågeställningen bottnar i att beslutsfattande och urvalsförfaranden för kontroll m.m. i ökad grad sker helt eller delvis automatiserat med stöd av nya tekniker i stället för av mänskliga handläggare som kan svara på frågor om hur verksamheten bedrivs. Vi bedömer att en anpassning bör göras i den reglering som säkerställer insynsmöjligheter när vissa sådana automatiserade förfaranden används, i syfte att undanröja en rättslig osäkerhet som nu hindrar eller hämmar digitaliseringen samtidigt som offentlighetsprincipen säkerställs och rättssäkerheten stärks.

Vi föreslår närmare bestämt att det ska regleras i författning att en myndighet ska se till att kunna lämna information om hur myndigheten vid handläggning av mål eller ärenden använder algoritmer eller datorprogram som, helt eller delvis, påverkar automatiserade urval eller beslut. Bestämmelsen föreslås införas i 4 kap. offentlighets- och sekretesslagen (2009:400).

Vi lämnar också förslag som främjar inhämtande av beslutsunderlag på annat sätt än direkt från enskilda samtidigt som förvaltningen säkerställer ordning och reda på beslutsunderlag. Uppgifter som utgör underlag i ett mål eller ärende ska som huvudregel tillföras handlingarna i det målet eller ärendet, även när underlaget kommer från databaser eller andra digitala källor. En myndighet behöver dock inte tillföra underlaget om det finns särskilda skäl mot

det, men föreslås då behöva se till att information kan lämnas om vilken eller vilka databaser eller andra digitala källor som innehåller ett underlag för handläggningen. Förslaget innebär en anpassning av 4 kap. 3 § offentlighets- och sekretesslagen.

De föreslagna bestämmelserna ska inte påverka tillämpningen av sekretessregleringen.

Vi föreslår också organiserat arbete för att framgent säkerställa rättssäkra förfaranden när förvaltningen använder artificiell intelligens med maskininlärda algoritmer samtidigt som såväl innovation som samverkan främjas.

Digital kommunikation

I vårt uppdrag ska vi särskilt analysera och föreslå vilket författningsstöd som krävs för att tillvarata den fulla potentialen i regeringens satsning Digitalt först. Det handlar om att möjliggöra en övergång från traditionella ärendeflöden till digitala informationsutbyten mellan den offentliga förvaltningen och individer eller privata aktörer.

Vi föreslår en ny och anpassad reglering om digital kommunikation i förvaltningslagen (2017:900). Syftet är att stärka kraven på att förvaltningen ska vara digitalt tillgänglig på det sätt som allmänheten förväntar sig, samtidigt som tilliten till digitala förfaranden stärks med klara regler om hur sådan kommunikation förväntas gå till.

Förslagen innehåller en ny huvudregel om att myndigheter ska vara skyldiga att tillhandahålla, och på lämpligt sätt anvisa, en eller flera digitala mottagningsfunktioner dit handlingar kan förmedlas. För att säkerställa en lämplig balans mellan intressen av bl.a. effektivitet och säkerhet föreslås att huvudregeln inte tillämpas om det är olämpligt av säkerhetsskäl eller av andra skäl. Ytterligare anpassningar i fråga om förvaltningens kommunikation föreslås också för att skapa tillit till förvaltningens digitala förfaranden. Det gäller reglering om ankomstdag för handlingar som förmedlas digitalt till förvaltningen och om underrättelser om ankomst.

Vi föreslår också en ny huvudregel om att förvaltningens kommunikation till enskilda ska vara digital, om det inte är olämpligt av säkerhetsskäl eller av andra skäl. Enskilda ska också kunna meddela

att de inte önskar ta emot skriftliga underrättelser eller andra handlingar från myndigheten i digital form.

För att stärka de rättsliga förutsättningarna för tillhandahållande av digitala tjänster där ärenden t.ex. kan inledas föreslår vi också att en myndighet bör ges i uppdrag att ta fram allmänna råd eller annat stödmaterial som avser utformningen av sådana tjänster.

Informationssäkerhet

Förvaltningens digitalisering kan inte diskuteras utan att frågor om informationssäkerhet belyses särskilt. Det kan konstateras att reglering beträffande informationssäkerhet som träffar olika aktörer och information, med delvis olika syften, finns spridd i olika föreskrifter. För närvarande pågår också ett antal utredningar och andra initiativ som syftar till att stärka informationssäkerheten ytterligare i den offentliga förvaltningen. Vi ser också en tydlig utveckling, både på EU-nivå och nationellt, att i allt större utsträckning ställa rättsliga krav på informationssäkerhet. Här kan exempelvis nämnas NIS-direktivet[1] och dataskyddsförordningens[2] uttalade krav på säkerhet och förslaget till en reformerad säkerhetsskyddslag.[3]

Ett mer sammanhållet arbete med informationssäkerhet i den offentliga förvaltningen har potential att effektivisera den digitala utvecklingen utan att säkerheten åsidosätts. Det gäller inte minst när myndigheter samarbetar i gemensamma utvecklingsarbeten som innefattar informationsutbyten. Mot den bakgrunden bedömer vi att det även efter genomförandet av bl.a. NIS-direktivet och ikraftträdandet av en ny säkerhetsskyddslag, kommer att vara angeläget att utforma en generell informationssäkerhetsreglering som omfattar hela förvaltningen, dvs. också kommuner och landsting.

I syfte att stärka informationssäkerheten i hela den offentliga förvaltningen föreslår vi därför att regeringen låter utreda förutsättningarna för att ta fram en kompletterande reglering om informationssäkerhet som omfattar hela den offentliga förvaltningen.

---

[1] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.
[2] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[3] *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag*, prop. 2017/18:89.

Tystnadsplikt för privata leverantörer

Ur olika perspektiv står frågor om samverkan i fokus för vårt uppdrag. Samverkan i förhållande till privata leverantörer av it-drift och andra it-baserade funktioner har också kommit att utkristallisera sig som ett centralt område. En förklaring till detta är att myndigheter inte alltid har möjlighet att med egna resurser effektivt utveckla de digitala förfaranden som används eller kommer att behöva användas för fortsatt digitalisering i förvaltningen.

Frågan om sekretessregleringen utgör hinder för att i vissa fall lämna ut uppgifter som omfattas av sekretess till privata leverantörer i samband med utkontraktering har diskuterats sedan en tid. Diskussionen har lyfts fram även under vår kartläggning, eftersom osäkerheten kring rättsliga förutsättningar för att utkontraktera särskilt it-drift och andra it-baserade funktioner kan hindra eller hämma digitaliseringen i den offentliga sektorn. En myndighets utlämnande av sekretessreglerade uppgifter vid utkontraktering måste baseras på klara och tydliga regler och skyddet för uppgifter som omfattas av sekretess behöver vara starkt.

Vi föreslår därför en i lag reglerad tystnadsplikt för uppgifter som omfattas av sekretess och som lämnas ut till en privat leverantör i samband med utkontraktering när det är fråga om enbart teknisk bearbetning eller lagring. Tystnadsplikten ska gälla för anställda och uppdragstagare hos en privat leverantör som tekniskt bearbetar eller lagrar uppgifter för en myndighets räkning. Bestämmelsen om tystnadsplikt föreslås införas i en ny lag som ska benämnas lag om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring. Lagen, som är subsidiär i förhållande till säkerhetsskyddslagstiftningen, ska tillämpas när myndigheter, eller vissa organ eller verksamheter som trätt i stället för en myndighet, uppdrar åt en privat leverantör att behandla uppgifter för enbart teknisk bearbetning eller lagring för myndighetens, organets eller verksamhetens räkning. Den föreslagna bestämmelsen om tystnadsplikt är straffsanktionerad.

Vi föreslår också en ny sekretessbrytande bestämmelse för att myndigheter i samband med utkontraktering av enbart teknisk bearbetning eller lagring ska kunna lämna ut sekretessbelagda uppgifter till privata eller offentliga leverantörer. Ett sådant sekretessgenombrott får emellertid bara ske om uppgiften behövs för att

leverantören ska kunna utföra uppdraget. En uppgift får inte heller lämnas ut om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut eller det av andra skäl är olämpligt. Bestämmelsen föreslås införas i 10 kap. offentlighets- och sekretesslagen.

It-avtal

Mot bakgrund av vår kartläggning har vi funnit anledning att också belysa förvaltningens it-avtal med anknytande personuppgiftsbiträdesavtal. I syfte att skapa bättre förutsättningar för att hantera rättsliga utmaningar med anledning av den fortsatta digitaliseringen bedömer vi att myndigheter allmänt sett bör tillhandahållas utökat stöd i arbetet med att formulera juridiskt hållbara och affärsmässigt gynnsamma villkor i it-avtal.

Vi föreslår därför att den nya Myndigheten för digital förvaltning får i uppdrag att främja den offentliga förvaltningens digitala investeringar genom att stödja myndigheters inköps- och avtalsprocesser och bidra till spridning av goda exempel i fråga om it-avtal.

Vidare föreslår vi ett särskilt uppdrag till vissa myndigheter om ett gemensamt organiserat arbete med att utforma standardavtalsklausuler för personuppgiftsbiträdesavtal. Förslaget gäller sådana personuppgiftsbiträdesavtal som tecknas mellan en myndighet och en privat leverantör i fråga om myndigheters köp av it-drift eller andra it-baserade funktioner.

Rättsutveckling för den digitala förvaltningen

Åtgärder och ställningstaganden från såväl riksdag som regering pekar mot att förvaltningens arbete med digitalisering nu ska genomdrivas med ökat fokus. De förslag till författningsändringar och andra åtgärder som vi lämnar i detta betänkande för att ge en stabil och förvaltningsgemensam bas där juridiken stödjer fortsatt digitalisering kommer inte att vara tillräckliga för att möta de kommande årens behov av förändringar i lagstiftningen. Det finns ett väsentligt större förändringsbehov i lagstiftningen än vad vi inom ramen för denna utredning har haft i uppdrag att ta omhand.

Våra analyser i flera av de frågeställningar som förts fram under kartläggningen redovisas i betänkandet. Fortsatta rättsliga överväganden och ställningstaganden kommer emellertid att behöva göras för att möjliggöra eller stödja digitaliseringen av förvaltningen, samtidigt som teknikutvecklingen fortsätter.

Det kommer att krävas prioriteringar och avvägningar kring hur de rättsliga resurserna används på bästa sätt för att så resurseffektivt som möjligt åstadkomma den rättsutveckling som önskas. Vi bedömer att formerna för samordning av arbetet med författningsändringar kan förbättras så att ändringar kan åstadkommas i rätt tid och i lämplig omfattning för att inte hindra eller hämma önskad digital utveckling inom förvaltningen.

Vi föreslår därför att regeringen tillsätter ett rättsligt beredningsorgan i form av en kommitté eller särskild utredare som under de närmast kommande åren får i uppdrag att löpande ta fram beredningsunderlag för anpassning av gällande rätt vid ärendehandläggning som stöds av såväl befintliga som nya former för digital informationsförsörjning.

I förlängningen ser vi behov av ytterligare insatser för att säkerställa att Sverige kan ligga i framkant vad gäller rättsliga förutsättningar för digitalisering. Här kan den nya Myndigheten för digital förvaltning få en roll att spela. Vi lämnar i denna del inte något förslag, med anledning av att myndigheten för närvarande är under bildande, men bedömer att regeringen bör överväga att i den nya myndigheten också inrätta en funktion med juridisk expertis.

Rapportering av arbete med it och digitalisering

I vårt uppdrag ska vi vidare analysera och lämna förslag på hur en utvidgad rapportering av hela den offentliga förvaltningens löpande arbete med it och digitalisering kan åstadkommas och utformas. It-kostnader utgör det andra största utgiftsslaget i statsförvaltningens verksamhetskostnader och uppgår till uppskattningsvis mellan 25 och 30 miljarder kronor per år. För kommuner, landsting och regioner saknas motsvarande uppgifter om it-kostnadernas storlek.

En rapportering av den offentliga förvaltningens löpande arbete med it och digitalisering syftar enligt vår uppfattning bl.a. till att skapa förutsättningar för bättre uppföljning, styrning, samordning

och kostnadskontroll av hela den offentliga förvaltningens digitala utveckling. Det krävs en god kontroll över de kostnader som digitaliseringen för med sig och en styrning mot digitalisering av de förfaranden där störst mervärde kan skapas.

Vi har mot den bakgrunden bedömt att den offentliga förvaltningen i författning bör åläggas en skyldighet att lämna uppgifter om it-kostnader. Vi har också bedömt att regelverket kring den officiella statistiken kan utgöra en lämplig rättslig infrastruktur för en sådan uppgiftsskyldighet.

Vi föreslår att det i förordningen (2001:100) om den officiella statistiken föreskrivs att kommuner, landsting och kommunalförbund ska lämna uppgifter om it-kostnader för den officiella statistiken. Vi föreslår vidare att Myndigheten för digital förvaltning ska vara ansvarig myndighet för den officiella statistiken för statistikområdet it-kostnader, och att it-kostnader ska vara ett statistikområde under ämnesområdet offentlig ekonomi. Statliga myndigheters uppgiftsskyldighet är redan i dag mer vidsträckt och det krävs ingen ytterligare reglering för att även uppgifter om it-kostnader ska kunna samlas in från dessa myndigheter. Det framgår av befintlig reglering att det ankommer på varje statistikansvarig myndighet att hitta metoder som kan minska uppgiftslämnarbördan. Vi föreslår vidare att regeringen i förordning med instruktion för Myndigheten för digital förvaltning ska utfärda nödvändiga föreskrifter för uppdraget.

Summary

Using the law to support digitalisation of public administration

The Inquiry's remit has focused on *the legal considerations for public administration that is digitally interoperable*. The remit included surveying and analysing the extent to which there is legislation that unnecessarily obstructs digital transformation and interoperability in public administration.

The remit also included presenting proposals for the *legislative amendments* considered to offer the greatest potential to support continued digitalisation of public administration. We also present certain *other measures* aimed at creating better conditions for handling legal challenges resulting from the digitalisation of public administration.

We present proposed amendments to *Chapter 4 of the Public Access to Information and Secrecy Act (2009:400)* aimed at making it easier for public authorities to maintain *a good structure for public access to information* in certain automated procedures, while safeguarding the principle of public access to official documents and strengthening legal certainty. This means ensuring the ability to provide *insight* into certain automated procedures when algorithms or computer programmes are used in connection with selection or decision-making processes. The Inquiry also presents proposals that promote the possibilities for public administration *to collect decision-making data* by means other than directly from individuals, at the same time as public administration safeguards good order regarding decision-making data collected or read from digital sources.

We also present proposals for continued organised work to ensure legally certain procedures when public administration uses *AI*

systems with machine learning algorithms, while promoting both innovation and interoperability.

In our report, we further propose introducing new and adapted regulations on *digital communication* in the Administrative Procedure Act (2017:900). The aim is to strengthen requirements on public administration to meet the public's expectations of digital accessibility, at the same time as clear rules on how this communication is expected to take place strengthen confidence in digital procedures. The proposals contain a new general rule stipulating that public authorities will be required to provide and, in an appropriate manner, allocate one or more *digital reception functions* to which documents can be delivered. Certain exceptions to the general rule are proposed to guarantee a good balance between the interests of e.g. efficiency and security. Additional adjustments are also proposed when it comes to communication by public administration in order to create confidence in public administration's digital procedures concerning adjustment of rules on the *date of arrival* for documents sent digitally to a public administration body and on *notifications*. To strengthen the legal conditions for the provision of digital services where cases can be opened, we have also proposed tasking a public authority with drafting *general advice or other support material* regarding the design of such services. We also propose a new general rule stating that public administration *communications to individuals must be digital*.

Digital administration must be legally certain as well as being secure in other aspects. Therefore, in addition to the proposals presented above, the Inquiry also presents some proposals aimed at creating a stable legal basis for the continued development of a digital administration that is interoperable both internally and in relation to private actors. We propose that the Government appoint an inquiry to examine the need to strengthen regulations on *information security* for public administration as a whole. We also propose *a new act on confidentiality when outsourcing to private suppliers* who handle public authority information solely for technical processing or storage purposes. In addition, we propose *a new provision that overrides secrecy* in *Chapter 10 of the Public Access to Information and Secrecy Act* to allow public authorities to provide certain classified information to private or public suppliers in connection with outsourcing of technical processing or storage. Furthermore, we propose strengthening the conditions for handling legal challenges resulting from digitalisation

by means of the Government tasking certain public authorities with providing increased support in authorities' *IT agreement processes* and with regard to personal data processor agreements.

Measures and positions from both the Riksdag and the Government indicate that even greater focus will now be given to digitalisation work carried out by public administration. Our remit also included presenting proposals on how all actors in public administration can collaborate on the need for new or amended legislation to promote digitalisation. We propose that the Government appoint a *legal preparatory body* that, over the next few years, is tasked with regularly providing preparatory material for adapting current legislation on digitalisation of case processing in public administration, supported by digital information exchanges and new forms of digital information supply.

In addition, the Inquiry was tasked with providing proposals on possible designs for augmented reporting of the entire public administration's regular work on IT and digitalisation. In this part of its remit, the Inquiry proposes that, in the Official Statistics Ordinance (2001:100), an obligation be imposed on public administration to provide information on *IT costs*.

1 Författningsförslag

1.1 Förslag till lag (2019:000) om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring

Härigenom föreskrivs följande.

Lagens tillämpningsområde

1 § Denna lag gäller när en myndighet uppdrar åt en privat leverantör att behandla uppgifter för enbart teknisk bearbetning eller teknisk lagring för myndighetens räkning.

2 § Vid tillämpningen av denna lag ska följande organ och verksamheter jämställas med en myndighet

1. aktiebolag, handelsbolag, ekonomiska föreningar och stiftelser där kommuner, landsting eller kommunalförbund utövar ett rättsligt bestämmande inflytande enligt 2 kap. 3 § offentlighets- och sekretesslagen (2009:400),
2. de organ som anges i bilagan till offentlighets- och sekretesslagen beträffande den verksamhet som anges där, eller
3. en yrkesmässigt bedriven enskild verksamhet som till någon del är offentligt finansierad och som anges i 2 § första stycket lag (2017:151) om meddelarskydd i vissa enskilda verksamheter.

3 § Om det i säkerhetsskyddslagen (2018:000) eller i säkerhetsskyddsförordningen (1996:633) finns bestämmelser som avviker från denna lag ska de bestämmelserna gälla.

Tystnadsplikt

4 § Den som på grund av anställning eller uppdrag hos en privat leverantör tekniskt bearbetar eller tekniskt lagrar uppgifter för en myndighets räkning, får inte obehörigen röja eller utnyttja dessa uppgifter.

I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Denna lag träder i kraft den 1 juli 2019.

1.2 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att 4 kap. 3 § och rubriken före 4 kap. 3 § ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 4 kap. 3 a § och 10 kap. 2 a §, och en ny rubrik före 10 kap. 2 a § av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	4 kap.
Överföring av upptagning för automatiserad behandling i läsbar form i vissa fall	***God offentlighetsstruktur vid vissa automatiserade förfaranden***
	3 §
Om en myndighet för handläggning av ett mål eller ärende använder sig av *en upptagning för automatiserad behandling*, ska *upptagningen* tillföras handlingarna i målet eller ärendet i läsbar form, *om det inte finns särskilda skäl mot det*.	Om en myndighet för handläggning av ett mål eller ärende använder sig av *ett underlag i en databas eller annan digital källa*, ska *underlaget* tillföras handlingarna i målet eller ärendet i läsbar form. *En myndighet behöver inte tillföra underlaget till handlingarna i målet eller ärendet enligt första meningen om det finns särskilda skäl mot det.*
	När en myndighet tillämpar första stycket andra meningen ska myndigheten se till att information kan lämnas om vilken eller vilka databaser eller andra digitala källor som innehåller ett underlag för handläggningen av målet eller ärendet.

3 a §

En myndighet ska se till att information kan lämnas om hur myndigheten vid handläggning av mål eller ärenden använder algoritmer eller datorprogram som, helt eller delvis, påverkar utfallet eller beslutet vid automatiserade urval eller beslut.

10 kap.

Teknisk bearbetning och lagring

2 a §

Sekretess hindrar inte att en uppgift lämnas ut till en enskild eller till en annan myndighet som utför uppdrag för enbart teknisk bearbetning eller teknisk lagring för den utlämnande myndighetens räkning, om uppgiften behövs för att utföra uppdraget.

En uppgift ska inte lämnas ut om

1. övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut, eller

2. det av andra skäl är olämpligt.

Denna lag träder i kraft den 1 juli 2019.

1.3 Förslag till lag om ändring i förvaltningslagen (2017:900)

Härigenom föreskrivs i fråga om förvaltningslagen (2017:900)

dels att 22, 25 och 33 §§ ska ha följande lydelse,

dels att det ska införas tre nya paragrafer, 7 a, 8 a, och 22 a §§, två nya rubriker före 8 a § och en ny rubrik före 22 a § av följande lydelse.

Lydelse enligt SFS 2017:900	*Föreslagen lydelse*
	7 a §
	En myndighet ska tillhandahålla och på lämpligt sätt anvisa en eller flera digitala mottagningsfunktioner dit handlingar kan förmedlas, om det inte är olämpligt av säkerhetsskäl eller av andra skäl.
	Digital kommunikation
	Hur handlingar översänds till enskilda
	8 a §
	En myndighets skriftliga underrättelser eller andra handlingar till enskilda ska förmedlas digitalt, om det inte är olämpligt av säkerhetsskäl eller av andra skäl.
	Enskilda kan meddela att de inte önskar ta emot skriftliga underrättelser eller andra handlingar från myndigheten digitalt.

22 §

En handling har kommit in till en myndighet den dag som handlingen når myndigheten eller en behörig befattningshavare.

Om en handling genom en postförsändelse eller en avi om en betald postförsändelse som innehåller handlingen har nått en myndighet eller behörig befattningshavare en viss dag, ska handlingen dock anses ha kommit in närmast föregående arbetsdag, om det inte framstår som osannolikt att handlingen eller avin redan den föregående arbetsdagen skilts av för myndigheten på ett postkontor.

En handling som finns i en myndighets postlåda när myndigheten tömmer den första gången en viss dag ska anses ha kommit in närmast föregående arbetsdag.

En handling som förmedlats till en anvisad digital mottagningsfunktion ska anses ha kommit in när den tagits emot där.

Underrättelse om ankomst

22 a §

När en handling har anlänt till en anvisad digital mottagningsfunktion ska myndigheten digitalt förmedla underrättelse till avsändaren om detta.

Myndigheten behöver inte förmedla underrättelse till avsändaren enligt första stycket om

1. det på annat sätt framgår för avsändaren att handlingen har tagits emot,

2. handlingen utan onödigt dröjsmål besvaras med ett helt eller delvis automatiserat beslut, eller

3. det är olämpligt.

25 §

Innan en myndighet fattar ett beslut i ett ärende ska den, om det inte är uppenbart obehövligt, underrätta den som är part om allt material av betydelse för beslutet och ge parten tillfälle att inom en bestämd tid yttra sig över materialet. Myndigheten får dock avstå från sådan kommunikation, om

1. ärendet gäller anställning av någon och det inte är fråga om prövning i högre instans efter överklagande,

2. det kan befaras att det annars skulle bli avsevärt svårare att genomföra beslutet, eller

3. ett väsentligt allmänt eller enskilt intresse kräver att beslutet meddelas omedelbart.

Myndigheten bestämmer *hur underrättelse ska ske*. Underrättelse får ske genom delgivning.	Myndigheten bestämmer *om underrättelse ska ske muntligen eller skriftligen*. Underrättelse får ske genom delgivning.

Underrättelseskyldigheten gäller med de begränsningar som följer av 10 kap. 3 § offentlighets- och sekretesslagen (2009:400).

33 §

En myndighet som meddelar ett beslut i ett ärende ska så snart som möjligt underrätta den som är part om det fullständiga innehållet i beslutet, om det inte är uppenbart obehövligt.

Om parten får överklaga beslutet ska han eller hon även underrättas om hur det går till. Myndigheten ska samtidigt upplysa parten om avvikande meningar som har antecknats enligt 30 § eller enligt särskilda bestämmelser i någon annan författning. En underrättelse om hur man överklagar ska innehålla information om vilka krav som ställs på överklagandets form och innehåll och vad som gäller i fråga om ingivande och överklagandetid.

Myndigheten bestämmer *hur underrättelsen ska ske*. En underrättelse ska dock alltid vara skriftlig om en part begär det. Underrättelse får ske genom delgivning.	Myndigheten bestämmer *om underrättelse ska ske muntligen eller skriftligen.* En underrättelse ska dock alltid vara skriftlig om en part begär det. Underrättelse får ske genom delgivning.

Denna lag träder i kraft den 1 juli 2019.

1.4 Förslag till förordning om ändring i förordningen (2001:100) om den officiella statistiken

Härigenom föreskrivs i fråga om förordningen (2001:100) om den officiella statistiken att 5 c och 5 d §§ och bilagan ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
5 c §[1]	
Kommuner och landsting ska för den officiella statistiken lämna de uppgifter som avses i 5 § 1–7, samt uppgifter om	
1. preliminära och definitiva årliga bokslut,	
2. budget och plan för resultat- och balansräkning enligt 5 kap. 1 och 2 §§ lagen (1997:614) om kommunal redovisning,	
3. utfall av kommunernas och landstingens resultaträkning för räkenskapsårets första tertial samt årsprognoser för innevarande år vid utgången av samma tertial,	
4. kommun- och landstingsägda företag, *och*	4. kommun- och landstingsägda företag,
5. alternativa utförare av kommun- och landstingsfinansierad verksamhet.	5. alternativa utförare av kommun- och landstingsfinansierad verksamhet, *och*
	6. it-kostnader.
Kommuner och landsting ska för den officiella statistiken dessutom lämna kvartalsvisa uppgifter om intäkter och kostnader, finansiella tillgångar och skulder, balansräkningsposter, investeringsutgifter samt kvartalsvisa årsprognoser för dessa.	
5 d §[2]	
Kommunalförbund ska för den officiella statistiken lämna de uppgifter som avses i 5 § 1–7 *och* uppgifter från de årliga boksluten.	Kommunalförbund ska för den officiella statistiken lämna de uppgifter som avses i 5 § 1–7, uppgifter från de årliga boksluten *och uppgifter om it-kostnader.*
Kommunalförbund ska för den officiella statistiken dessutom lämna kvartalsvisa uppgifter om intäkter och kostnader, finansiella	

[1] Senaste lydelse 2013:946.
[2] Senaste lydelse 2013:946.

tillgångar och skulder, balansräkningsposter, investeringsutgifter samt kvartalsvisa årsprognoser för dessa.

Nuvarande lydelse

Bilaga[3]

Den officiella statistiken
De statistikansvariga myndigheterna
Arbetsmiljöverket
Brottsförebyggande rådet
Centrala studiestödsnämnden
Domstolsverket
Ekonomistyrningsverket
Finansinspektionen
Försäkringskassan
Havs- och vattenmyndigheten
Kemikalieinspektionen
Konjunkturinstitutet
Kungliga biblioteket
Medlingsinstitutet
Myndigheten för familjerätt och föräldraskapsstöd
Myndigheten för kulturanalys
Myndigheten för tillväxtpolitiska utvärderingar och analyser
Naturvårdsverket
Pensionsmyndigheten
Riksgäldskontoret
Skogsstyrelsen
Socialstyrelsen
Statens energimyndighet
Statens jordbruksverk
Statens skolverk
Statistiska centralbyrån
Sveriges lantbruksuniversitet
Tillväxtverket
Trafikanalys
Universitetskanslersämbetet

[3] Senaste lydelse 2018:35.

Officiell statistik och vilka myndigheter som ansvarar för respektive område

Officiell statistik	Ansvarig myndighet
OFFENTLIG EKONOMI	
Finanser för den kommunala sektorn	SCB
Statlig upplåning och statsskuld	Riksgäldskontoret
Beskattning	SCB
Utfallet av statsbudgeten	Ekonomistyrningsverket
PRISER OCH KONSUMTION	

Föreslagen lydelse

Bilaga

Den officiella statistiken

De statistikansvariga myndigheterna

Arbetsmiljöverket
Brottsförebyggande rådet
Centrala studiestödsnämnden
Domstolsverket
Ekonomistyrningsverket
Finansinspektionen
Försäkringskassan
Havs- och vattenmyndigheten
Kemikalieinspektionen
Konjunkturinstitutet
Kungliga biblioteket
Medlingsinstitutet
Myndigheten för digital förvaltning
Myndigheten för familjerätt och föräldraskapsstöd
Myndigheten för kulturanalys
Myndigheten för tillväxtpolitiska utvärderingar och analyser

Naturvårdsverket
Pensionsmyndigheten
Riksgäldskontoret
Skogsstyrelsen
Socialstyrelsen
Statens energimyndighet
Statens jordbruksverk
Statens skolverk
Statistiska centralbyrån
Sveriges lantbruksuniversitet
Tillväxtverket
Trafikanalys
Universitetskanslersämbetet

Officiell statistik och vilka myndigheter som ansvarar för respektive område

Officiell statistik	Ansvarig myndighet
OFFENTLIG EKONOMI	
Finanser för den kommunala sektorn	SCB
Statlig upplåning och statsskuld	Riksgäldskontoret
Beskattning	SCB
Utfallet av statsbudgeten	Ekonomistyrningsverket
It-kostnader	*Myndigheten för digital förvaltning*
PRISER OCH KONSUMTION	

Denna förordning träder i kraft den 1 januari 2019.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Regeringen beslutade den 24 november 2016 att ge en särskild utredare i uppdrag att kartlägga och analysera i vilken utsträckning det förekommer lagstiftning som i onödan försvårar digital utveckling och samverkan inom den offentliga förvaltningen (se bilaga 1). Av utredningsdirektiven framgår bl.a. att utredaren ska lämna förslag till de författningsändringar som bedöms ha störst potential att stödja den fortsatta digitaliseringen av den offentliga förvaltningen. Utredaren ska vidare lämna förslag till hur en utvidgad rapportering av hela den offentliga förvaltningens löpande arbete med användning av it och digitalisering kan utformas samt hur aktörerna inom förvaltningen som helhet kan samverka kring behovet av ny eller ändrad lagstiftning för att främja digitaliseringen.

Det kan noteras att uppdraget att kartlägga och lämna författningsförslag omfattar hela den offentliga förvaltningen och all den förvaltningsgemensamma lagstiftningen förutom grundlag och därtill inte heller författningar på personuppgiftsområdet. Begränsningen gäller emellertid bara i förhållande till de författningsförslag som lämnas. I utredningsarbetet har vi därför inte sett oss förhindrade att inkludera såväl grundlagsområdet som personuppgiftsområdet i kartläggningen och efterföljande analys.

Vårt omfattande uppdrag i kombination med den begränsade tid vi har haft till förfogande har gjort det nödvändigt med vissa prioriteringar av vilka frågor vi ska ta oss an. Mot denna bakgrund har vi valt att lägga fokus på förvaltningsgemensam lagstiftning och rättsfrågor som enligt vår bedömning har bäst förutsättningar att ge störst effekt för att stödja hela den offentliga förvaltningens digitalisering. Därtill har vi också prioriterat att lyfta fram vissa områden,

såsom informationssäkerhet och it-avtal, som också spelar en avgörande roll för att den offentliga sektorn ska fortsätta sin utveckling i riktning mot en trygg, innovativ och effektiv digital förvaltning.

2.2 Utredningens arbete

Vi har varit angelägna om att bedriva ett utåtriktat utredningsarbete för att få ett så brett och djupt underlag som möjligt. Det gäller både underlag om användning och utveckling av it i den offentliga sektorn och underlag kring vilken lagstiftning som kan anses försvåra digitalisering inklusive digital samverkan inom förvaltningen.

Vi har genomfört totalt 28 kartläggningsmöten där vi har träffat företrädare för både statliga och kommunala myndigheter liksom privata aktörer med en nära koppling till den offentliga sektorn (se vidare kapitel 5.1.2 om vår metod i kartläggningsarbetet och vilka aktörer som deltagit). Vi har därutöver bl.a. haft ett särskilt möte med Kammarkollegiet och ett antal möten med privata företag som erbjuder tjänster med ny digital teknik. I syfte att bl.a. inhämta synpunkter från den privata sektorn har vi vidare anordnat en hearing där ett hundratal representanter från privat och offentlig sektor deltog. Därtill har vi deltagit på konferenser och i olika nätverk och arbetsgrupper.

Vi har haft tre sammanträden med expertgruppen. Dessutom har vi haft särskilda fördjupningsmöten i avgränsade frågor med vissa experter och även andra specialister inom olika områden.

Det har inte uttryckligen ingått i vårt uppdrag att göra en internationell utblick. Vi har trots det, i viss utsträckning, tagit del av information om främst våra grannländers (Danmark, Finland, Norge och Estland) digitala utveckling inom ramen för offentlig förvaltning. Vi har därtill deltagit på seminarier med internationellt fokus.

Vi har enligt våra utredningsdirektiv haft att samråda med Datainspektionen, Myndigheten för samhällsskydd och beredskap och Sveriges Kommuner och Landsting. Vi har under arbetets gång haft separata möten med dessa aktörer och samråden har även fullgjorts genom att dessa tre aktörer varit representerade i utredningens expertgrupp. Viss kontakt har förevarit med Försvarsmakten. Parallellt

med vårt uppdrag har flera andra utredningar behandlat frågor med nära anknytning till vårt arbete. Här kan särskilt nämnas Utredningen om effektiv styrning av nationella digitala tjänster[1] som vi har träffat vid flera tillfällen. Vi har även haft kontakt med Expertgruppen för digitala investeringar,[2] Delegationen för korrekta utbetalningar,[3] Utredningen om vissa säkerhetsskyddsfrågor,[4] Delegationen för unga och nyanlända till arbete,[5] Tillitsdelegationen[6] och Utredningen om inrättande av en myndighet för digitalisering av den offentliga sektorn.[7]

2.3 Betänkandets disposition

I betänkandets inledande kapitel 3 och 4 redogörs för framväxten av, och värdegrunder i, den digitala förvaltningen. I kapitel 5 och 6 ges en översiktlig presentation av kartläggningen följt av några inledande reflektioner.

Kapitel 7 tar sitt avstamp i pågående och kommande automation i förvaltningen. I kapitlet behandlas bl.a. frågor om god offentlighetsstruktur vid vissa automatiserade förfaranden, rättssäkerhet vid förvaltningens användning av AI-system med maskininlärda algoritmer och automationsanpassad lagstiftning.

Kapitel 8 handlar om digital kommunikation, både när det gäller tillgänglighet till förvaltningen och sättet för förvaltningens kommunikation till enskilda.

I kapitel 9 redogörs för vikten av god informationssäkerhet för att trygga den fortsatta utvecklingen av en digital förvaltning. Kapitel 10 handlar om en författningsreglerad tystnadsplikt för privata leverantörer vid utkontraktering av teknisk bearbetning och lagring. I kapitel 11 redogörs för hur bl.a. myndigheters utkontraktering föranleder behov av att teckna juridiskt hållbara och affärsmässigt gynnsamma it-avtal.

Kapitel 12 omhändertar vissa frågor där vi av olika anledningar inte har haft möjlighet att göra djupare analyser eller lämna konkreta

[1] Fi N 2016:01.
[2] Fi 2017:04.
[3] Fi 2016:07.
[4] Ju 2017:08.
[5] A 2014:06.
[6] Fi 2016:03.
[7] Fi 2017:09.

förslag. I samma kapitel lämnas också förslag på hur det fortsatta arbetet med nödvändiga författningsändringar ska bedrivas för att sådana ändringar ska kunna åstadkommas i lämplig tid och omfattning.

I kapitel 13 lämnas förslag på hur den offentliga förvaltningen ska rapportera om sitt arbete med it och digitalisering.

I de avslutande kapitlen 14–16 återfinns konsekvensbedömningar, förslag på ikraftträdande avseende de författningsförslag som lämnas och författningskommentar.

3 Framväxten av den digitala förvaltningen

3.1 Tillbakablick

Vårt uppdrag är i huvudsak rättsligt inriktat. För att sätta in vårt arbete i en bredare kontext ser vi emellertid skäl att här kort presentera hur framför allt styrningen av den digitala förvaltningen har växt fram.

Svenska myndigheter har använt it för att utveckla sin verksamhet sedan 1950-talet. Myndigheterna byggde tidigt upp olika typer av dataregister som blev centrala i deras kärnverksamhet, bl.a. med anledning av att välfärdsstatens socialförsäkringsprogram förutsatte en väl utvecklad registerföring. Frågor om hur datordriften i statsförvaltningen och i den kommunala förvaltningen borde samordnas och organiseras har också sedan lång tid tillbaka varit föremål för diskussion.[1]

Under 1980-talet skapade regeringen ett rationaliseringstryck på myndigheterna som en konsekvens av en debatt kring den stora staten och det höga skattetrycket. Därigenom hamnade bl.a. ADB (automatisk databehandling) i fokus som ett verktyg för att öka myndigheternas produktivitet och effektivitet. Den politiska utmaningen var att förvaltningen skulle leverera mer för mindre. Under denna period i utvecklingen hade medborgaren huvudsakligen rollen som skattebetalare.[2] Denna utveckling kan beskrivas som den första generationen av den datoriserade förvaltningen.

[1] Se bl.a. Datasamordningskommitténs betänkande *ADB och samordning – samordning av ADB-verksamheten inom den offentliga förvaltningen* (SOU 1976:58) och Knutsson, *Från räknesnurra till dataplatta – 60 år med kommunal IT* 1954–2014, Institutet för informationsteknologi, 2015.

[2] E-delegationens betänkande *Strategi för myndigheternas arbete med e-förvaltning* (SOU 2009:86), s. 33.

En andra fas i utvecklingen av myndigheternas digitala verksamhet inleddes när internet och webben växte fram under 1990-talet. Myndigheterna hade redan då en relativt hög teknikmognad och e-tjänster blev ett sätt att underlätta kontakten utåt, men även ett sätt att effektivisera informationsutbytet mellan myndigheter.

Regeringen lade år 2000 fast en strategi för att skapa s.k. 24-timmarsmyndigheter.[3] Syftet var att myndigheterna skulle öka tjänsteutbudets effektivitet och tillgänglighet. Medborgaren betraktades nu i allt större utsträckning som kund och utmaningen låg i att leverera användarcentrerade och interaktiva e-tjänster.[4] Myndigheternas service och information skulle finnas på webben på tider och platser som passade individen. Utvecklingen under denna period dominerades av omfattande centrala initiativ med gemensamma lösningar för hela förvaltningen. Många länder hade t.ex. byggt upp nationella medborgarportaler. I Sverige fanns också sedan en tid tillbaka Sverige.se med avsikten att fungera som medborgarnas ingångsdörr till förvaltningens samlade tjänsteutbud. De stora centrala initiativen visade sig emellertid vid den tiden vara en relativt svårframkomlig väg. I stället växte sektorsvisa samverkansprojekt fram som ett sätt att driva utvecklingen framåt i Sverige med tätare samarbeten mellan myndigheter utan att för den skull kräva alltför stora samlade initiativ.[5]

Sverige kom under denna period ut väl i olika internationella jämförelser om förvaltningsutvecklingen. Svensk e-förvaltning var den bästa i världen år 2008 enligt FN och tog därmed för första gången över förstaplatsen från USA. I The Economist's ranking klättrade Sverige från en tredje plats till en andra plats mellan åren 2008 och 2009, medan Danmark tog förstaplatsen.[6]

Allt mer frekvent förde dock myndigheterna fram krav på en tydligare styrning, finansiering och koordinering av e-förvaltningsarbeten liksom behovet av ökade möjligheter till samverkan med

[3] *Ett informationssamhälle för alla*, prop. 1999/2000:86.
[4] SOU 2009:86 s. 33.
[5] Bland annat initiativ som Nationell IT-strategi för vård och omsorg, Geodatarådet, RIF-rådet, Verksamt.se, TIFOS (en utökning av tillhandahållandet av folkbokföringsuppgifter i samhället), Minpension.se, Elegitimation.se och Krisinformation.se. Se t.ex. Verva *69 Myndigheter redovisar 915 strategiska insatser för utveckling av e-förvaltningen. Analys och sammanställning* (2008:14).
[6] SOU 2009:86 s. 34.

tredje part. Det fanns också indikationer på att det inte var tillräckligt många som använde de e-tjänster som myndigheterna tog fram för att det skulle vara möjligt att realisera förväntade besparingar.[7]

Regeringen aviserade i budgetpropositionen för år 2007 att den avsåg att stärka styrningen och snabba på utvecklingen av e-förvaltningen.[8] I mars 2008 tillsatte regeringen en särskild statssekreterargrupp för strategiska frågor inom e-förvaltning. Under denna grupps ledning arbetade man fram en handlingsplan för e-förvaltning.[9] I handlingsplanen lades vissa principiella utgångspunkter för e-förvaltningsarbetet fast.

Stabsutredningen föreslog vid ungefär samma tid att dåvarande stabsmyndighet Verket för förvaltningsutveckling (Verva) skulle avvecklas.[10] I stället skulle en delegation för e-förvaltning tillsättas för att i nära samverkan med Regeringskansliet driva arbetet med e-förvaltning. Verva avvecklades den 31 december 2008 och i mars 2009 fattade regeringen beslut om direktiv till E-delegationen. Delegationen arbetade under åren 2009–2015 med den förvaltningsgemensamma utvecklingen för att skapa förutsättningar att nå regeringens övergripande mål för e-förvaltningen och lämnade ett flertal betänkanden.[11] Under den tidsperioden inrättades också E-legitimationsnämnden.

Efter E-delegationen fortsatte myndigheterna som ingick i delegationen och Sveriges Kommuner och Landsting (SKL) att driva frågor om digital samverkan i ett egeninitierat samarbete, E-samverkansprogrammet (eSam).[12] Efterhand har fler myndigheter anslutit sig och för närvarande ingår 25 medlemmar i eSam.

Regeringen har efter E-delegationen tillsatt ett råd för digitaliseringen av det offentliga Sverige. Rådet består av 11 ledamöter som representerar myndigheter, kommuner och landsting. Regeringen har också under senare år beslutat om ett antal olika uppdrag på digitaliseringsområdet till statliga myndigheter.[13]

---

[7] A.a.
[8] *Budgetpropositionen för 2007*, prop. 2006/07:1.
[9] Handlingsplan för e-förvaltning (Fi2008/491).
[10] Stabsutredningens betänkande *Ett stabsstöd i tiden* (SOU 2008:22).
[11] Se E-delegationens slutbetänkande *En förvaltning som håller ihop* (SOU 2015:66) med däri gjorda hänvisningar till delegationens delbetänkanden.
[12] Se vidare www.esamverka.se
[13] Se bl.a. Utredningen om effektiv styrning av nationella digitala tjänsters delbetänkande *digitalforvaltning.nu* (SOU 2017:23), s. 74.

På senare tid har Sverige halkat efter andra länder i internationella jämförelser på digitaliseringens område, särskilt när det gäller digitaliseringen av den offentliga sektorn. Digitaliseringskommissionen har framfört att digitaliseringen av det offentliga är Sveriges akilleshäl. Kommissionen beskrev att placeringen inom detta område var märkbart sämre än inom andra områden, och att det över tid var möjligt att se en negativ trend i hur Sverige placerar sig på området e-förvaltning. Sammanhållna ärendekedjor, transparens i ärendeprocesser och användare i fokus angavs som exempel på aspekter som mäts i indexen där Sverige inte presterar lika bra som andra jämförbara länder, däribland våra nordiska grannländer.[14] Enligt Utredningen om effektiv styrning av nationella digitala tjänster är den främsta orsaken till detta ett medvetet val att delegera ansvaret för digitaliseringen av den offentliga förvaltningen till myndigheterna. Att arbetet hos myndigheterna varit framgångsrikt i många avseenden kompenserar enligt den utredningen inte för de begränsningar som delegeringen inneburit. Regeringen har också enligt den utredningen avstått från att använda de styrinstrument som står till buds, t.ex. genom att inte förtydliga vilka uppdrag som myndigheterna har när det gäller digitalisering. Utredningen föreslog mot den bakgrunden bl.a. att ansvaret för digitaliseringen skulle samlas hos en myndighet.[15]

I budgetpropositionen för år 2018 föreslog regeringen att en ny myndighet med uppgift att samordna och stödja den förvaltningsövergripande digitaliseringen skulle inrättas.[16] Regeringen har också, i uppdraget till organisationskommittén, anfört att den nya myndigheten medför förbättrade förutsättningar för en säker, effektiv och innovativ verksamhetsutveckling som utgår från användarnas behov. Den nya myndigheten ska placeras i Sundsvall och ska inleda sin verksamhet den 1 september 2018. Myndigheten övertar uppgifter från E-legitimationsnämnden, Ekonomistyrningsverket, Skatteverket, Post- och telestyrelsen, Riksarkivet och Tillväxtverket.[17]

Den senaste tidens initiativ från regeringen markerar en tydlig förändring av inriktningen av politiken för den digitala förvaltningen, på ett sätt som i flera avseenden innebär en omprövning av

[14] *För digitalisering i tiden* (SOU 2016:89), s. 54.
[15] SOU 2017:23 s. 89 f.
[16] *Budgetpropositionen för år 2018*, prop. 2017/18:1, utg.omr. 2 s. 99 f.
[17] Inrättande av en myndighet för digitalisering av den offentliga sektorn (dir. 2017:117).

tidigare ställningstaganden. Utredningen om effektiv styrning av nationella digitala tjänster har därför beskrivit det som att nu pågår en omstart av politiken för digitalisering inom den offentliga sektorn.[18]

3.2 Internationell utblick

Vi har inte haft i uppdrag att göra någon särskild internationell utblick i vårt arbete. Ett uppdrag inom området för digitalisering kan emellertid knappast utföras utan viss orientering om andra länders förutsättningar och arbeten. Vi har därför, främst med de nordiska länderna i åtanke men även i en global kontext, översiktligt studerat framför allt de rättsliga förutsättningarna för en digital förvaltning. De snäva tidsramarna för vårt arbete har dock inte medgett några mer omfattande internationella kontakter, men som framgått i kapitel 2 har vi tagit del av information om främst våra grannländers (Danmark, Finland, Norge och Estland) digitala utveckling inom ramen för offentlig förvaltning. Vi har bl.a. träffat den pågående norska förvaltningslagsutredningen och deltagit vid ett seminarium om Estlands nationella digitala plattform X-Road. Vi har vidare haft möjlighet att ta del av olika författningar från Danmark, Finland och Norge, bl.a. tack vare kontakter som Utredningen om effektiv styrning av nationella digitala tjänster haft med dessa länder.[19]

Vi redovisar inte här på ett sammanhållet sätt utredningens ovan beskrivna begränsade internationella utblick utan återkommer i det följande till vissa internationella referenser vid våra överväganden, där vi funnit det vara relevant.

3.3 Rättsliga förutsättningar

Den i kapitel 3.1 beskrivna tillbakablicken över framväxten av den digitala förvaltningen utgår främst från hur styrningen av densamma fungerat och vilka organisationsformer som har förekommit. Under den beskrivna tidsperioden har också ett omfattande utrednings- och lagstiftningsarbete ägt rum med relevans för utvecklingen av den digitala förvaltningen. Vi sammanfattar inte här alla de tidigare arbeten som är relevanta för utredningen, utan återkommer i det

[18] *reboot- omstart för den digitala förvaltningen* (SOU 2017:114), s. 73 f.
[19] Se även bl.a. SOU 2017:23.

följande till några av de tidigare (och pågående) arbetena i sina respektive sammanhang.

Det kan här noteras att tidigare utredningsarbeten i hög grad har varit begränsade i så måtto att utredningarna har varit avgränsade till vissa specifika lagstiftningsområden. Det har alltså inte förut, på motsvarande sätt som för denna utredning, gjorts något utredningsarbete som i ett bredare perspektiv tagit sikte på bl.a. kartläggning och analys av all lagstiftning på området för digitalisering i den samverkande offentliga förvaltningen. Vi redovisar därför utförligt det som framkommit i utredningens kartläggning om hindrande eller hämmande lagstiftning i kapitel 5. Först finns dock anledning att kort presentera några rättsområden som är centrala för den digitala förvaltningen, se kapitel 4.

4 Värdegrunder i den digitala förvaltningen

4.1 Rättsliga utgångspunkter för en fortsatt trygg, innovativ och effektiv digital förvaltning

Möjligheterna i den digitala förvaltningen är stora. Många myndigheter gör mycket och har också kommit långt i sitt arbete med att genom digitala lösningar ge privatpersoner och företag tillgång till enklare och mer sammanhängande tjänster. På så vis minskar bl.a. behovet av uppgiftslämnande och myndigheternas verksamheter kan allmänt sett effektiviseras. I takt med utvecklingen av ny teknik och nya arbetssätt skapas också mervärden genom nya möjligheter till uppföljning, styrning, forskning och kunskap. Samtidigt behöver de centrala värden som under lång tid burit upp den svenska förvaltningen fortsatt vara en bas för den digitala förvaltningen. Det är angeläget att även det digitala samhället genomsyras av ett demokratiskt synsätt och att alla känner en grundtrygghet i den digitala samhällsutvecklingen.

För att enskildas tillit till den digitala förvaltningen ska kunna upprätthållas är inledningsvis transparens i myndigheternas verksamhet genom möjlighet till insyn fortfarande av grundläggande betydelse. En öppen förvaltning med ordning och reda på uppgifter och informationssamlingar är därtill en nödvändig förutsättning för att den offentliga förvaltningens uppgifter ska kunna vidareutnyttjas på ett sätt som skapar både ekonomiska och samhällsnyttiga värden.

God informationssäkerhet är en annan faktor som är nödvändig i den digitala förvaltningen. Att krav på rättssäkerhet i grundlag och förvaltningslagstiftning följs och att dessa värden kan stärkas i den digitala förvaltningen utgör ytterligare centrala aspekter för den framtida utvecklingen. Frågor om vad som ur integritetssynpunkt

kan anses tillåtet, såväl när det gäller dataskyddsreglering som sekretessreglering, är också centrala.

Det som beskrivs i det följande gör inte anspråk på att ge någon heltäckande bild av rättsläget, utan ska tjäna som en kort presentation av centrala rättsliga områden för förståelsen av utredningens bedömningar och förslag. För att främja läsbarheten hänvisar vi i denna introducerande framställning inte till konkreta lagrum, de återkommer vi till i våra fördjupade analyser i kapitel 7–13. Genom att beakta och utgå från de värden som här kort presenteras är det enligt utredningen möjligt att säkerställa en fortsatt trygg digital förvaltning, som också är innovativ och effektiv.

4.2 God offentlighetsstruktur är en nödvändig grund

Öppenhet är en central värdegrund för den svenska förvaltningen. Bakom den grundläggande rätten till insyn i myndigheters verksamhet ligger offentlighetsprincipen. Offentlighetsprincipen har kommit till uttryck på olika sätt i svensk lagstiftning. I tryckfrihetsförordningen stadgas rätten att ta del av allmänna handlingar, även kallad handlingsoffentligheten. Huvudprinciper om rätt till meddelarfrihet för bl.a. offentliganställda tjänstemän och om offentlighet vid domstolsförhandlingar och beslutande församlingars sammanträden är andra uttryck för offentlighetsprincipen.

Syftet med rätten att ta del av allmänna handlingar är rent generellt att främja ett fritt meningsutbyte och en allsidig upplysning. På det sättet markeras att det är fråga om en del av den medborgerliga yttrande- och informationsfriheten, som också utgör en av förutsättningarna för den fria demokratiska åsiktsbildningen. Rätten att ta del av allmänna handlingar har också kommit att fungera som ett viktigt medel för kontroll av offentliga organs verksamhet. Allmänheten får möjlighet att kontrollera handläggningsrutiner, ambitioner och effektivitet. Vetskapen om att en granskning kan utföras anses som en garanti för att myndigheter utför sina uppgifter korrekt. Offentlighetsprincipen har därtill under årens lopp i betydande utsträckning kommit att ligga till grund för uttag av allmänna handlingar för kommersiella ändamål.

Det som ovan beskrivits om syftena med rätten att ta del av allmänna handlingar gäller också i den digitala förvaltningen och måste

ses som en förutsättning för att medborgarna ska fortsätta att sätta sin tillit till det offentliga. Att allmänheten fortsatt ges goda möjligheter till insyn i den digitala förvaltningen är alltså fundamentalt. I det sammanhanget bör också framhållas att transparens gentemot enskilda är en grundpelare i den reformerade EU-rätten om dataskydd, liksom att möjligheter till partsinsyn regleras för att garantera en rättssäker förvaltning. Som närmare redovisas nedan finns dock begränsningar i insynsrätten genom att allmänna handlingar kan omfattas av sekretess.

Här lämnas inte någon fullständig presentation av vad som anses utgöra en allmän handling som omfattas av handlingsoffentligheten enligt tryckfrihetsförordningen (se vidare kapitel 7.6.3). Helt kort kan konstateras att ett antal kriterier måste uppfyllas för att uppgifter i digital miljö ska klassificeras dels som en handling, dels som en allmän sådan. I många fall måste ganska svåra rättsliga överväganden göras för att avgöra om, och i så fall när, ett visst elektroniskt material är att anse som en allmän handling. Handlingsoffentligheten innebär dock som utgångspunkt att myndigheters egna möjligheter till kontroll, sökning och sammanställning av uppgifter i allmänna handlingar ska motsvaras av allmänhetens möjligheter till insyn.

Myndigheter ska ta hänsyn till handlingsoffentligheten när de organiserar sina allmänna handlingar. Utan en god offentlighetsstruktur även i den digitala förvaltningen blir allmänhetens möjligheter till insyn i praktiken kraftigt beskuren. Det är därför nödvändigt att myndigheter även i digitala miljöer håller ordning och reda bland sina informationsmängder. Vissa krav måste också ställas när det gäller dels diarieföring och annan registrering, dels dokumentation av åtgärder. Författningsreglering kring diarieföring och beskrivning av myndighetens allmänna handlingar finns i offentlighets- och sekretesslagstiftningen. För arkiverade handlingar innehåller arkivlagstiftningen därtill vissa bestämmelser om förteckningar som ska föras. Krav på dokumentation för att möjliggöra transparens gentemot enskilda finns dessutom i dataskyddsregleringen. I förvaltningslagstiftningen finns andra krav på dokumentation som syftar till att garantera rättssäkra förfaranden. Det kan konstateras att bilden över författningskrav för säkerställande av att den digitala förvaltningen håller ordning och reda i sina informationsmängder inte är lättöverskådlig.

Förutom de ovan nämnda syftena med rätten att ta del av allmänna handlingar har den offentliga förvaltningen också en central roll i samhällets informationsförsörjning i vidare mening. Att den offentliga förvaltningen försörjer samhället i stort med information är i sig inte någonting nytt. Allt mer framhålls dock vikten av att de uppgifter som myndigheter samlar in och producerar digitalt också tillgängliggörs digitalt som öppna data för att nå en större samhällsnytta. Detta gäller särskilt med tanke på att myndigheterna i den offentliga förvaltningen står för en stor del av produktionen av den datamängd som hela det digitala samhället bygger på, och att mängden av information som produceras ökar i allt snabbare takt. Det handlar om uppgifter som rör bl.a. ekonomi, geografi, lantbruk, meterologi, skog, trafik, turism och vetenskap och som kommer från till exempel register, sensorer eller rapporter. All information som samlas in, produceras och lagras i offentlig förvaltning har både ekonomiska och samhällsnyttiga värden för människor och företag. Att ta till vara på dessa värden, genom innovationer eller med kända medel, bidrar till att öka tillväxten i samhället. Innovationer som bygger på myndigheters informationsmängder kan i förlängningen också användas av det offentliga och i sin tur leda till en än mer effektiv och rättssäker förvaltning genom användande av ny teknik för exempelvis automatiserade beslutsprocesser eller bättre utformade välfärdstjänster.

Öppenhet i den digitala förvaltningen är alltså en helt central värdegrund även för frågan om samhällets informationsförsörjning, och i förlängningen hela samhällets utveckling. En nödvändig faktor för att upprätthålla den transparensen är att även i den digitala förvaltningen åstadkomma en god offentlighetsstruktur med ordning och reda bland förvaltningens informationsmängder. Med en god offentlighetsstruktur som grund kan den tekniska utvecklingen också tas till vara på ett sätt som därtill stärker förvaltningens öppenhet. I förlängningen kommer en sådan transparens också att vara av grundläggande betydelse för den demokratiska förankringen av den offentliga och digitala förvaltningens verksamhet.

4.3 God informationssäkerhet behövs för att möta nya risker

Privatpersoner och företag har, utöver krav på öppenhet, också befogade krav på att den digitala förvaltningen upprätthåller en hög säkerhet när myndigheternas informationsmängder bearbetas, lagras och kommuniceras. Även myndigheter emellan krävs en viss form av tillit till varandras informationssäkerhet för att exempelvis samverkan om informationsutbyten ska kunna komma till stånd.

En allt mer digitaliserad förvaltning kan innebära att samhället öppnar upp för olika risker. Om myndigheter brister i hanteringen av eller säkerheten för information kan det få omfattande konsekvenser, såväl för samhället i stort som för enskilda. Den it-relaterade hotbilden (attacker, it-brott, spionage och kränkningar m.m.) står också under snabb utveckling. För att privata och offentliga utövare ska fortsätta att sätta sin tillit till den digitala förvaltningen krävs förtroende för att myndigheter vid varje tidpunkt har förmåga att hantera information på ett säkert sätt och att möta rådande hotbild.

Med informationssäkerhet förstås företrädesvis en strävan efter att skydda information så att den alltid finns när den behövs, att det går att lita på att den är korrekt och inte manipulerad eller förstörd, att endast behöriga personer får ta del av informationen och att det går att följa hur och när informationen har hanterats och kommunicerats. Informationssäkerheten garanteras genom dels administrativa åtgärder för att skydda information som till exempel föreskrifter eller behörighetsrutiner, dels tekniska åtgärder för it-säkerhet eller fysiska inpasseringskontroller.

I juli 2016 antogs inom EU ett direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (det s.k. NIS-direktivet), i syfte att förbättra den inre marknadens funktion. Direktivet ska genomföras i svensk rätt och regeringen har lämnat förslag till en ny lag om informationssäkerhet för samhällsviktiga tjänster och digitala tjänster. Regelverket ska enligt förslaget tillämpas av vissa leverantörer av samhällsviktiga eller digitala tjänster. När det gäller reglering avseende informationssäkerhet bör vidare framhållas att sådan information som är sekretessreglerad med hänsyn till rikets säkerhet ges ett särskilt skydd genom säkerhetsskyddslagstiftningen.

Att statliga myndigheter ska se till att informationshanteringen uppfyller krav på säkerhet framgår också i förordningsreglering om krisberedskap och höjd beredskap. Myndigheten för samhällsskydd och beredskap föreskriver dessutom att de statliga myndigheterna dels ska rapportera it-incidenter, dels ska införa ett ledningssystem för informationssäkerhet.

Här finns även anledning att nämna dataskyddsreglernas krav på säkerhet vid behandling av personuppgifter liksom arkivregleringens krav rörande bevarande av handlingar och uppgiftssamlingar över lång tid. Sektorsspecifik reglering om hantering av information kan också innehålla bestämmelser om informationens säkerhet. I sammanhanget bör även den straffrättsliga reglering som innebär kriminalisering av vissa handlingar nämnas, t.ex. brottsbalkens reglering av dataintrång. Det kan konstateras att reglering beträffande informationssäkerhet som träffar olika aktörer och information, med delvis olika syften, finns spridd på olika håll.

På vilket sätt förvaltningen svarar upp mot de olika kraven på informationssäkerhet måste bedömas i enskilda fall så att skyddet för olika typer av information i olika verksamheter varken blir för begränsat eller för krångligt och dyrt. Det förtjänar också att framhållas att en digital förvaltning inte bara medför nya risker som vid varje tidpunkt behöver mötas av en god och väl avvägd informationssäkerhet. En digital förvaltning kan också möjliggöra en hantering av information som är mer säker än en traditionell informationshantering per telefon, fax eller papperspost, utan krav på tidsödande administration som motringningar, säkerställande av att rätt person står vid faxen hos mottagande myndighet vid rätt tidpunkt eller hantering av rekommenderade brev.

4.4 Rättssäkerheten kan stärkas med digitala medel

Vissa grundläggande principer anses kännetecknа en rättsstat och tillmäts en avgörande vikt i EU:s rättssystem liksom i Europakonventionen. Legalitetsprincipen brukar framhållas som ett skydd mot en nyckfull och godtycklig maktutövning från det allmännas sida. Principen kommer till uttryck i regeringsformens krav på att all offentlig makt i Sverige ska utgå från folket och utövas under lagarna. I förarbetena till den nya förvaltningslagen ställs också krav

på att myndigheternas maktutövning i vidsträckt mening måste ha stöd i någon av de källor som tillsammans bildar rättsordningen – exempelvis förvaltningslagen, speciallagstiftning, myndighetens instruktion eller annan förordningsreglering eller regeringsbeslut. Även likabehandlingsprincipen, eller objektivitetsprincipen, vilken regleras i regeringsformen och som därtill kommer till uttryck i motiven till den nya förvaltningslagen bör här särskilt framhållas. Till skydd mot godtycke och diskriminering vid tillämpning av regler ska myndigheter vara sakliga och opartiska. En allmän proportionalitetsprincip har under tid utvecklats genom Högsta förvaltningsdomstolens praxis och innebär ett skydd för enskilda intressen mot en ensidig prioritering av det allmännas önskemål vid myndigheternas agerande. Också den principen kommer till uttryck i förslaget till ny förvaltningslag.

Att myndigheter vid service, ärendehandläggning och faktiskt handlande möter sådana krav på rättssäkerhet som de ovan angivna principerna ger uttryck för är av avgörande betydelse för allmänhetens tilltro till den offentliga förvaltningen. Det är med andra ord givet att den digitala förvaltningen ska följa den reglering som ger uttryck för dessa grundläggande principer. Här redogörs inte närmare för hur den digitala förvaltningen möter och i takt med utvecklingen fortsatt kan leva upp till dessa krav, bl.a. när det gäller att inkludera och tillgodose olika gruppers behov för en tillgänglig digital förvaltning där alla har möjlighet att tillvarata sin rätt. Dessa och andra frågor som rör grunderna för rättssäkra förfaranden i den digitala förvaltningen återkommer vi till i samband med våra överväganden och förslag.

Ur rättssäkerhetssynpunkt är det emellertid inte tillräckligt att förvaltningen rent principiellt uppfyller de ovan angivna kraven. Kraven måste därtill mötas i tid och på ett kostnadseffektivt sätt. För att enskilda ska ha en reell möjlighet att ta tillvara sin rätt krävs nämligen att ärenden avgörs och frågor besvaras utan oskälig fördröjning. Att behöva vänta lång tid på ett myndighetsbeslut kan skapa otrygghet, leda till ekonomiska förluster eller i värsta fall personligt lidande för den enskilde. Långa förseningar i det offentligas verksamhet kan också undergräva allmänhetens förtroende för förvaltningen i stort. Myndigheterna behöver därför kunna lämna snabba, enkla och entydiga besked och hjälpa den enskilde att ta till

vara sin rätt, utan att detta förenas med orimliga kostnader för den offentliga förvaltningen.

När myndigheter ger service och handlägger ärenden digitalt innebär det generellt sett fördelar för enskilda ur rättssäkerhetssynpunkt. Digitala lösningar medför nämligen oftast en snabbare, enklare och mer kostnadseffektiv service och ärendehandläggning än vad som är möjligt att erbjuda med en manuell hantering av frågor och ärenden. På så sätt stärks rättssäkerheten med digitala medel. Generellt sett har myndigheter redan kommit långt i arbetet med att digitalisera den egna verksamheten även om det finns undantag. När en viss verksamhet har övergått från manuella till automatiserade förfaranden är det sällan möjligt att återgå till en manuell och pappersbaserad handläggning som möter kraven på rättssäkerhet med rimliga svars- och handläggningstider inom tänkbara kostnadsramar. Som exempel kan nämnas Försäkringskassans och Skatteverkets befintliga automatiserade förfaranden på socialförsäkringsområdet och skatteområdet. Hur fortsatt utveckling på området för automation i förvaltningen genom effektiv användning av ny teknik kan förenas med rättssäkra förfaranden förtjänar noggranna överväganden.

I takt med att de tekniska möjligheterna att inhämta eller ta del av uppgifter av god kvalitet ökar, höjs också förväntningarna på att förvaltningens åtgärder och beslut grundas på fullgoda och korrekta underlag. I detta sammanhang bör principen om uppgiftslämnande endast en gång, ”The Once-Only Principle” nämnas. Principen har kommit till uttryck inom EU med syfte att i första hand minska de administrativa bördorna för företag som kommunicerar med offentlig sektor. Den syftar också till att minska administrationen inom förvaltningen. Att återanvända uppgifter av god kvalitet, som redan finns hos myndigheter, som underlag för olika typer av åtgärder och beslut skapar förutsättningar för än mer rättssäkra förfaranden. Att förvaltningen inte gång efter annan kräver inrapportering av samma uppgifter underlättar för de enskilda samtidigt som antalet tillfällen när fel kan uppstå i de uppgifter som lämnas minskar. Vikten av att uppgifter som direkt eller indirekt relaterar till en person är korrekta speglas också i dataskyddsregleringens principer om skydd för personuppgifter.

4.5 Personlig integritet – en mänsklig fri- och rättighet som inte är absolut

Grundläggande bestämmelser till skydd för den personliga integriteten finns i regeringsformen. Den offentliga makten ska utövas med respekt för den enskilda människans frihet och det allmänna ska värna den enskildes privatliv och familjeliv. Var och en är gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Inskränkningar i det grundlagsfästa skyddet kan dock under vissa förutsättningar göras genom lag.

I EU:s stadga om de grundläggande rättigheterna bekräftas de rättigheter som har sin grund i medlemsstaternas gemensamma författningstraditioner, internationella förpliktelser och rättspraxis vid Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna. Enligt rättighetsstadgan har var och en rätt till skydd av de personuppgifter som rör honom eller henne. Sådana uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få dem rättade. En oberoende myndighet ska kontrollera att reglerna följs. I detta sammanhang bör även Europakonventionen nämnas, som reglerar att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Med detta avses bl.a. skyddet av personuppgifter. Rättigheterna enligt EU:s stadga och Europakonventionen är dock inte heller absoluta. Vissa inskränkningar får göras med stöd av lag om det är nödvändigt och proportionerligt i ett demokratiskt samhälle med hänsyn till vissa särskilt angivna ändamål.

Inom EU har det sedan mitten av 90-talet funnits gemensamma regler om dataskydd. Mot bakgrund av den tekniska och samhälleliga utvecklingen sedan de reglerna antogs, och den fortsatt snabbt förändrliga digitala miljön, beslutades år 2016 om en ny dataskyddsreform inom EU. Reformen har flera övergripande syften – att ytterligare harmonisera och effektivisera skyddet för personuppgifter och öka enskildas kontroll över sina personuppgifter, men också att förbättra framför allt den digitala inre marknadens funktion. Här

redogörs inte i detalj för innebörden av de dataskyddsregler som ska börja tillämpas i maj 2018. De grundläggande principerna om dataskydd kan dock förklaras på följande sätt.

- Personuppgifter får behandlas bara om det finns lagligt stöd för det.
- Personuppgifter ska alltid behandlas på ett korrekt sätt och i enlighet med god sed. Uppgifterna ska som huvudregel behandlas på ett öppet sätt i förhållande till den registrerade.
- Personuppgifter får samlas in endast för särskilda, uttryckligt angivna och berättigade ändamål.
- Personuppgifter får inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in.
- Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen.
- Personuppgifter får behandlas endast om det är nödvändigt med hänsyn till ändamålen med behandlingen, det vill säga fler uppgifter än vad som är nödvändigt får inte behandlas.
- Personuppgifter som behandlas ska vara riktiga och, om nödvändigt, aktuella.
- Personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen ska rättas, blockeras eller utplånas.
- Personuppgifter får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

För den offentliga förvaltningen gäller i stor utsträckning specifika regler om när personuppgifter får behandlas och under vilka förutsättningar. Ofta finns reglerna i de så kallade registerförfattningarna. Det förekommer att digitalisering inom förvaltningen inte innebär behandling av personuppgifter, t.ex. vid användande av en viss typ av sensorer för mätning av luftföroreningar, men det är dock vanligare att digitalisering också innebär att direkta eller indirekta personuppgifter på något sätt kommer att behandlas. Mot bakgrund av EU-rätten om dataskydd och att det finns ett stort antal nationella författningar på relativt detaljerad nivå ställs det därför höga krav på

i första hand lagstiftaren att i tillräcklig takt göra de avvägningar som behövs för att förena regelverket med en önskad utveckling. Lagstiftaren har, med beaktande av den utveckling som är önskvärd och under de förutsättningar som översiktligt redogjorts för ovan, vissa möjligheter att inskränka skyddet för personuppgifter och se till att sådana inskränkningar står i rimlig proportion till ändamålet med behandlingen.

Det bör lyftas fram att det för myndigheters arbete med digitalisering också är möjligt att söka stöd i regelverket om skydd för personuppgifter. I samband med utveckling av ny teknik som innebär personuppgiftsbehandling finns det exempelvis ofta möjlighet att bygga in ett särskilt skydd för den personliga integriteten (så kallad inbyggd integritet eller ”privacy by design”). Det kan till exempel handla om att minska mängden personuppgifter som ska registreras, att införa tekniska begränsningar för tillgång till personuppgifter och att låta systemet styra hur personuppgifter registreras.

4.6 Välavvägd sekretess för skyddsvärda uppgifter

Offentlighetsprincipen innebär, som framgått ovan, att allmänheten ska ha möjlighet till insyn i den offentliga förvaltningens verksamhet. Rätten att ta del av allmänna handlingar får bara begränsas av vissa särskilda skäl som räknas upp i tryckfrihetsförordningen. Sådana begränsningar ska anges noga i bestämmelser i offentlighets- och sekretesslagen eller lag som denna lag hänvisar till. En sådan begränsning av rätten att ta del av allmänna handlingar, med andra ord sekretess, innebär ett förbud att röja en uppgift vare sig det sker muntligen, genom utlämnande av allmän handling eller på något annat sätt. Sekretessen innebär alltså både en handlingssekretess och en tystnadsplikt. I vissa fall begränsas även den grundlagsfästa rätten att meddela och offentliggöra uppgifter. Det finns sekretessbestämmelser som är tillämpliga för alla myndigheter. Andra sekretessbestämmelser riktar sig bara till vissa myndigheter, t.ex. inom skolområdet eller socialtjänsten. Sedan finns det sekretessbestämmelser som avser att skydda vissa allmänna intressen, t.ex. det allmännas ekonomiska intresse. Flertalet sekretessbestämmelser syftar till att skydda enskildas personliga eller ekonomiska intressen. Även

vissa privaträttsliga organ ska tillämpa reglerna i offentlighets- och sekretesslagstiftningen.

Sekretessbestämmelser består i regel av tre förutsättningar för bestämmelsens tillämplighet. För det första anges alltid sekretessens föremål, dvs. vilken information eller med andra ord vilka uppgifter som kan eller ska hemlighållas. Till exempel kan det gälla uppgift om enskilds personliga förhållanden. För det andra anges i de flesta fall sekretessbestämmelsens räckvidd, dvs. om sekretessen bara gäller i en viss typ av ärende, i en viss typ av verksamhet eller hos en viss myndighet. För det tredje bestäms sekretessens styrka med hjälp av ett s.k. skaderekvisit. Här finns olika varianter, allt från att sekretessen är absolut, dvs. alltid gäller, till att uppgifterna som utgångspunkt är offentliga och att sekretess bara gäller om det kan antas att en viss skada uppkommer om uppgiften röjs.

Sekretess gäller som huvudregel inte bara i förhållande till enskilda utan också mellan myndigheter, eller inom en myndighet om där finns olika verksamhetsgrenar som är att betrakta som självständiga i förhållande till varandra. Så kan vara fallet t.ex. inom en kommun med flera förvaltningar inom organisationen. När sekretess gäller i förhållande till andra myndigheter eller inom en myndighet krävs sekretessbrytande bestämmelser för att uppgifter ska få lämnas ut från myndigheten eller verksamheten där de finns. Som huvudregel följer inte sekretessen med när en uppgift har förts över till en annan myndighet. Det beror bl.a. på att behovet av och styrkan i en sekretess inte kan bestämmas enbart med hänsyn till intresset av att skydda uppgiften. Skyddsintresset måste nämligen i varje sammanhang vägas mot insynsintresset i den myndighet eller verksamhet där uppgiften finns. Det finns dock vissa bestämmelser om överföring av sekretess, som innebär att sekretessen följer med uppgiften när den flyttas till en annan myndighet eller verksamhet.

I den digitala förvaltningen, likväl som varit fallet i den traditionella förvaltningen, gäller att insynen i en myndighets verksamhet ibland behöver begränsas genom sekretess, under de särskilda förutsättningar som regleras i grundlag och för att skydda vissa utpekade intressen. Däri ligger också att uppgifter i vissa fall inte ska lämna en viss myndighet, verksamhet eller databas på grund av den rådande sekretessen. Det finns emellertid aspekter i samband med digitaliseringen som gör det nödvändigt för i första hand lagstiftaren att överväga hur regleringen till skydd för dessa intressen bör se ut.

Utvecklingen går mot att myndigheter i allt högre grad antingen åläggs att samverka med varandra med stöd av tekniska lösningar eller av andra skäl behöver samverka för att fullgöra sina uppdrag på ett sätt som möter allmänhetens förväntningar och inom givna kostnadsramar. En sekretessreglering som utformats med andra arbetssätt hos myndigheterna i åtanke, eller utifrån dåtida teknik, kan därför behöva anpassas så att inte befintlig reglering av sekretess nu hindrar en önskad utveckling. Nya bestämmelser som rör sekretessregleringen kan också behöva tillkomma för att stödja den fortsatta digitaliseringen.

4.7 Regleringen behöver stå i samklang med den önskade utvecklingen

Redogörelsen ovan visar på några centrala rättsliga områden som varit och fortsatt kommer att vara av avgörande betydelse för allmänhetens förtroende för den offentliga verksamheten. Trots att redogörelsen inte gör anspråk på att vara fullständig framgår med tydlighet att det är en omfattande regelmassa som den offentliga förvaltningen har att förhålla sig till vid all digital utveckling. De beskrivna värdegrunderna är alltjämt centrala för tilltron till förvaltningen. Förändringar i regleringen behöver emellertid löpande göras för att tillåta och stödja sådan utveckling och digitalisering som är önskvärd och nödvändig i vårt demokratiska samhälle. I detta sammanhang kan inte heller bortses från den pågående rättsutvecklingen inom EU som i flera avseenden drivs av att i tid finna rättsliga lösningar som upprätthåller centrala värdegrunder och möter den tekniska utvecklingen liksom samhällsutvecklingen i stort. Om inte rättsutvecklingen bedrivs i takt med teknik- och samhällsutvecklingen ser vi risk för två alternativa scenarier.

Å ena sidan löper den offentliga förvaltningens digitalisering en risk för att stagnera om gällande reglering hindrar eller hämmar en önskad utveckling. Det kan leda till att förvaltningen framöver får en minskad förmåga att möta kommande samhällsutmaningar och att förtroendet för förvaltningen därför avtar. Den offentliga förvaltningen kan i det sammanhanget inte ses fristående från samhället i övrigt. En förvaltning som inte är föränderlig kan också leda till

bristande förmåga till innovation och utveckling i övriga samhället med ekonomiska eller andra konsekvenser som följd.

Å andra sidan finns det också en risk för att andra incitament eller styrmedel snabbt driver utvecklingen i offentlig verksamhet vidare utan att regleringen anpassas eller beaktas i tillräcklig utsträckning. Det kan leda till att lagstiftningen slutligen står för långt ifrån verkliga förhållanden, eller t.o.m. att centrala värden träds för när eller går förlorade.

Det framstår som angeläget att finna en god balans och att stödja den digitala utvecklingen i förvaltningen genom rättsutveckling som står i samklang med den önskade digitala utvecklingen.

5 Kartläggning av hindrande eller hämmande lagstiftning

5.1 Genomförandet av kartläggningen

5.1.1 Vårt uppdrag

I vårt uppdrag ingår att i ett brett perspektiv kartlägga lagstiftning som i onödan försvårar digitalisering och digital samverkan inom den offentliga förvaltningen. Kartläggningen ska också omfatta lagstiftning som inte i sig är direkt hindrande men där det finns en rättslig osäkerhet som har en hämmande inverkan på den digitala utvecklingen inom den offentliga förvaltningen.

Enligt uppdraget ska vi vid kartläggningen särskilt prioritera frågor som rör regeringens satsning Digitalt först, där digitala tjänster så långt det är möjligt och där det är relevant ska vara förstahandsval vid den offentliga sektorns kontakter med medborgare, organisationer och företag. Vi ska också prioritera sådan lagstiftning som i onödan försvårar digitalt informationsutbyte inom den offentliga förvaltningen och behandla frågor om digitalt informationsutbyte mellan den offentliga förvaltningen och privata utförare av offentligt finansierade tjänster.

Vid kartläggningen ska vi vidare prioritera sådan lagstiftning som i sin helhet, eller i stora delar, påverkar den offentliga förvaltningen. I möjligaste mån ska vi visa på konkreta fall där utvecklingen av digitala tjänster hindrats som en följd av den aktuella lagstiftningen.

5.1.2 Metod

Vi har uttolkat vårt uppdrag som att kartläggningen ska avse inte endast lagstiftning i form av lag beslutad av riksdagen, utan även normgivning genom förordning eller föreskrift. Inledningsvis övervägde vi att genomföra en enkät till underlag för kartläggningsdelen av vårt uppdrag. Vi insåg emellertid att det inte skulle vara enkelt att beskriva hindrande eller hämmande lagstiftning i enkätsvar och att den formen för genomförande av uppdraget skulle innebära att vi inte gavs möjligheter till följdfrågor för djupare förståelse av svaren. För att genomföra vårt kartläggningsuppdrag har vi i stället valt att träffa representanter för ett antal myndigheter och andra berörda aktörer vid särskilda s.k. kartläggningsmöten.

Vid urvalet av de verksamheter vi har besökt har ansatsen varit att inhämta information ur ett brett perspektiv. Vår utgångspunkt har därför varit att träffa personer vid såväl statliga, kommunala som landstingskommunala myndigheter, myndigheter ur olika sektorer, med skilda uppdrag, av olika storlek, med olika geografisk belägenhet och olika förutsättningar när det gäller hur verksamheten finansieras. Vi har vidare vinnlagt oss om att inkludera både myndigheter som har kommit långt i sitt arbete med digitalisering och digital samverkan men också sökt träffa representanter för myndigheter som befinner sig i en mer inledande fas i sitt digitaliseringsarbete. Därtill har vi även besökt privata aktörer vars verksamhet har en nära koppling till det offentliga.

Under kartläggningen har vi mött representanter vid Arbetsförmedlingen, Bolagsverket, Centrala studiestödsnämnden (CSN), Stockholms universitet (eGovLab), eHälsomyndigheten, Försäkringskassan, Institutet för framtidsstudier, Inera AB, Kungliga Tekniska högskolan (KTH), Lantmäteriet, Länsstyrelsen i Norrbottens län, Migrationsverket, Naturvårdsverket, Pensionsmyndigheten, Polismyndigheten, Region Halland, Riksarkivet, Skatteverket, Socialstyrelsen, Statens servicecenter, Stockholm stad, Sveriges kommuner och landsting (SKL), Tillväxtverket, Transportstyrelsen, Tullverket och Uppsala kommun. SKL har i detta arbete varit behjälpliga med att samla in information från ytterligare kontaktpersoner vid kommuner. I något fall har fler än ett möte ägt rum.

Gensvaret från de aktuella myndigheterna och andra aktörerna har varit mycket positivt. Vi är tacksamma för den respons vi fått vid

våra mötesförfrågningar och den tid som representanter för olika discipliner (arkiv, it, juridik, ledning, verksamhet etc.) har lagt ned på att bereda oss ett gott underlag. Endast ett par av dem vi sökt kontakt med har svarat att de inte haft tillfälle att träffa utredningen.

Kartläggningsmötena har genomförts i samtalsform. Som diskussionsunderlag har vi använt ett mötesstöd (se bilaga 2) men vid mötena har i hög grad våra samtalspartners fått styra vilka områden som lyfts fram för oss. Det har rört sig om beskrivningar av rättsliga hinder och utmaningar i genomfört, pågående eller planerat digitaliseringsarbete liksom rättsliga hinder eller trösklar som hämmar effektiv myndighetssamverkan i digitala utvecklingsarbeten. Vi har även samlat in tankar om hur en effektivare samverkan kring rättslig reglering kan utvecklas i syfte att skapa bättre förutsättningar för författningsarbetet att gå i takt med önskad digital verksamhetsutveckling.

Vid samtliga kartläggningsmöten har minnesanteckningar förts. De representanter vi träffat har fått tillfälle att ge synpunkter på anteckningarna som också har omhändertagits för arkivering.

Som framgått i kapitel 2 har vi också anordnat en hearing där såväl deltagare från det privata näringslivet som myndighetsrepresentanter deltog, haft särskilda möten med representanter för företag och, utöver SKL, även samrått med Datainspektionen och Myndigheten för samhällsskydd och krisberedskap (MSB). Erfarenheterna från dessa och andra aktiviteter har också höjt vår kunskap men har inte dokumenterats på samma sätt som de särskilda kartläggningsmötena.

5.1.3 Läsanvisningar

Sammanfattningen i detta kapitel tar sin utgångspunkt i den information, synpunkter, förslag och konkreta exempel som de deltagande aktörerna i kartläggningsarbetet har förmedlat till oss. Att fullständigt återge all den information vi har fått ta del av inom ramen för kartläggningsarbetet låter sig inte göras eftersom materialet är alltför omfattande. Vi har alltså tvingats sålla och prioritera vid sammanställningen av kartläggningsresultatet. Vi har valt att främst lägga fokus på de områden där de deltagande aktörerna varit i någon utsträckning samstämmiga och vissa områden där påtagliga

rättsliga utmaningar för en trygg, innovativ och effektiv digital förvaltning har lyfts fram. För en fullständigare bild av kartläggningsresultatet hänvisas till de minnesanteckningar som vi fört och arkiverat.

I detta kapitel ges således den övergripande bilden av kartläggningsresultatet. Framställningen utgår från vad vi fångat under kartläggningen. Vi har alltså inte anlagt ett eget analysperspektiv i det förevarande kapitlet. Vid våra överväganden och förslag i följande kapitel fördjupar vi dock i flera avseenden beskrivningen av kartläggningsresultatet. I dessa följande kapitel gör vi också egna analyser och presenterar rättsläget på ett närmare sätt.

Vid våra samtal under kartläggningen har det visat sig att det kan vara svårt att separera de rättsliga utmaningarna från hämmande faktorer som t.ex. har med tekniska möjligheter eller finansiering att göra. I vissa av beskrivningarna och exemplen som följer framgår detta. En påtaglig del av de rättsligt relaterade hinder eller hämmande faktorer som lyfts fram för oss har också handlat om en önskan om tydligare stöd i juridiken för att möta en kommande digital framtid som i viss utsträckning redan är här, snarare än en uppräkning av konkreta hinder som man har stött på i gällande lagstiftning. Även detta speglas i den följande beskrivningen.

5.2 Digital kommunikation med enskilda

5.2.1 Gränserna för Digitalt först

Regeringens ansats är att digitala tjänster, när det är möjligt och relevant ska vara förstahandsval i den offentliga sektorns kontakter med medborgare, organisationer och företag. Ansatsen kan sammanfattas vara en princip om Digitalt först.

I vårt kartläggningsarbete har det tydliggjorts att flertalet myndigheter, men inte alla, tekniskt och utvecklingsmässigt har möjlighet att erbjuda digitala kanaler för enskildas myndighetskontakter och ärenden. Flera av dem vi talat med har emellertid fört fram att det behöver klargöras var de rättsliga gränserna går för hur långt myndigheterna kan tillämpa principen om Digitalt först. Ett exempel på en fråga som lyfts är om en myndighet kan kräva att enskilda ska använda digitala kanaler för att kontakta myndigheten eller för

att ge in en ansökan eller anmälan. Det har framförts vara ett värdefullt stöd för myndigheterna om gränserna för Digitalt först förtydligas rättsligt i stället för att myndigheterna på egen hand ska söka sig fram. Med ett tydligare rättsligt stöd beskrivs det också vara lättare för myndigheterna att ta ytterligare steg framåt i sin digitalisering.

Kartläggningsarbetet visar att även om myndigheterna strävar efter att använda digitala kanaler för sin kommunikation med privatpersoner och företag behövs ibland komplement med möjlighet till kontakt via andra kanaler. Vissa personer har inte de förutsättningar som krävs för att kunna kommunicera digitalt med förvaltningen. Det kan röra sig om otillräcklig kunskap om, och tillgång till, den digitala tekniken eller om språkförbistringar. Men det behöver inte betyda att skriftlig kommunikation medelst papper och postbefordran är det bästa alternativet till digitala kommunikationskanaler för dessa personer.

> Exempel: Pensionsmyndigheten, som inom ramen för sitt uppdrag har omfattande kontakter med den äldre delen av befolkningen, har funnit att kommunikation via telefon är den kanal som bäst matchar servicenivån i en digital tjänst. Vid muntlig kontakt kan handläggare anpassa det stöd och den information som ges direkt efter samtalspartens behov.

I detta sammanhang har vi också hört önskemål om förbättrade tekniska förutsättningar för säker digital tvåvägskommunikation med enskilda.

5.2.2 Registerförfattningar

Reglering i författningar om skydd för personuppgifter (registerförfattningar[1]) kan begränsa myndigheters möjligheter att kommunicera digitalt med enskilda. Det rör sig främst om begränsningar i snävt formulerade ändamålsbestämmelser eller särskild reglering om direktåtkomst till personuppgifter.

> Exempel: CSN har tekniska möjligheter att skicka e-post eller sms i stället för brevförsändelse till personer som har antagits till en studiemedelsberättigad utbildning för att informera om rätten att ansöka om studiemedel. Att skicka e-post eller sms vore lämpligt dels för att unga

[1] En registerförfattning innehåller bestämmelser om personuppgiftsbehandling som främst kompletterar regleringen i dataskyddsförordningen. Myndigheter som behandlar (känsliga) uppgifter om ett stort antal personer tillämpar ofta en särskild registerförfattning.

människor inte alltid bor på den adress där de är folkbokförda, dels för att många är vana att kommunicera via en mobil enhet t.ex. en smart telefon. CSN är dock förhindrad att skicka e-post eller sms eftersom CSN saknar lagligt stöd i studiestödsdatalagen och studiestödsdataförordningen[2] för att behandla uppgifter om e-postadress och telefonnummer för ändamålet att informera studiestödsberättigade om studiestödsförmåner.

Exempel: På fordonsområdet hindrar de nuvarande bestämmelserna om direktåtkomst till uppgifter i vägtrafikregistret och i viss mån även ändamålsbestämmelserna en önskvärd utveckling av tillgången till uppgifter i digitala servicetjänster. Transportstyrelsen lämnade i juni 2014 en framställan till regeringen om ändring i vägtrafikregisterlagen och vägtrafikregisterförordningen för att möjliggöra detta. Framställan har lett till ändring såtillvida att enskilda kan ges direktåtkomst till egna personuppgifter. I övrigt har framställan inte lett till ändringar.[3]

5.2.3 Sekretess

Sekretess kan verka hindrande vid utveckling av effektiva och ändamålsenliga digitala tjänster på ett sätt som förefaller vara i viss utsträckning onödigt. Viss typ av sekretessreglering, s.k. absolut sekretess, gör ingen skillnad på typen av uppgifter utan sekretess gäller för alla uppgifter som omfattas av regleringen. Det innebär att den sekretessen gäller oavsett om det rör sig om utlämnande av en enstaka och mer harmlös uppgift.

Exempel: Att använda förvalslistor i digitala tjänster genererar goda förutsättningar att automatisera ärendehandläggning. En positiv effekt av förvalslistor är dessutom att uppgifterna som hämtas in är kvalitetssäkrade och att uppgifterna som ska ligga till grund för handläggning och beslut i ärendet blir rätt från början. Skatteverket har emellertid mycket begränsat utrymme att tillhandahålla förvalslistor i digitala tjänster oavsett om det är en intern eller myndighetsgemensam tjänst. Eftersom samtliga uppgifter i beskattningsdatabasen omfattas av absolut sekretess[4] har Skatteverket gjort bedömningen att dessa uppgifter inte kan användas i förvalslistor i digitala tjänster. Ett konkret exempel är hantverksföretagens ansökningar om rotavdrag.[5] I ansökan krävs att det ansökande företaget registrerar korrekt fastighetsbeteckning för den

[2] Studiestödsdatalagen (2009:287) och studiestödsdataförordningen (2009:321).
[3] Framställan om ändring i lagen (2001:558) och förordningen (2001:650) om vägtrafikregister gällande behandling av personuppgifter i vägtrafikregistret i Transportstyrelsens servicetjänster, 16 juni 2014, (TSV 2014:1632).
[4] 27 kap. 1 § offentlighets- och sekretesslagen (2009:400).
[5] Rotavdrag är en skattesubvention som ges till privatpersoner för vissa typer av renoveringsarbeten som utförs i hemmet.

fastighet som rotavdraget avser. Ett sätt att säkerställa att den som fyller i ansökan verkligen får alla bokstäver och siffror rätt i fastighetsbeteckningen skulle vara att ta hjälp av en s.k. förvalslista som anger relevanta förslag i takt med att fastighetsbeteckningen fylls i. Men eftersom de förslag på fastighetsbeteckning som lämnas i förvalslistan skulle behöva hämtas från beskattningsdatabasen menar Skatteverket att en sådan funktion inte kan tillhandahållas.

Företeelsen journaler på nätet har också lyfts fram. Vissa landsting tillhandahåller journaler på nätet till enskilda individer. En förutsättning för att journaler ska kunna tillhandahållas på det sättet är att vårdgivaren säkerställer att inga uppgifter som är sekretessbelagda i förhållande till patienten lämnas ut. I regel kan enskilda ta del av all sin patientinformation men det finns vissa begränsningar om det med hänsyn till ändamålet med vården eller behandlingen är av synnerlig vikt att uppgiften inte lämnas ut till den enskilde.[6] Eftersom sekretess för vissa uppgifter alltså kan gälla även mot den enskilde har det beskrivits att det, innan en kanal för utlämnande av patientuppgifter på nätet etableras, först behöver genomföras en menprövning i fråga om sekretessen hindrar utlämnande. Men hur ska en sådan gå till i praktiken? Kan menprövningen göras schablonmässigt?[7] Vem fattar beslutet i fråga om sekretess? Och kan beslutet läggas till grund för automatiserat utlämnande?

5.2.4 Digitala tjänster med eget utrymme

Kartläggningsarbetet visar att det blir allt vanligare att myndigheter utvecklar digitala tjänster som innefattar ett s.k. eget utrymme för tjänstens användare. Ett eget utrymme tillhandahålls som en service åt användaren och ingen annan än användaren ska ha insyn i den information som lagras där. Avsikten är att det ska vara möjligt för enskilda att t.ex. spara utkast för en ansökan eller anmälan eller vidta andra åtgärder utan att handlingarna i det egna utrymmet ska anses ha kommit in till myndigheten enligt tryckfrihetsförordningen eller förvaltningslagen.[8]

[6] 25 kap. 6 § offentlighets- och sekretesslagen.
[7] Jfr *Regeringens proposition med förslag till sekretesslag m.m.*, prop. 1979/80:2 Del A, s. 80 f. om s.k. massuttag.
[8] Här och i det följande avses förvaltningslagen (2017:900) med ikraftträdande den 1 juli 2018 om inte referens till äldre version av lagen särskilt anges.

Det blir också allt vanligare att myndigheter, och ibland även privata aktörer, i samverkan utvecklar eller använder tjänster som omfattar ett eget utrymme. Som exempel kan nämnas Mina meddelanden hos Skatteverket, det personliga hälsokontot Hälsa för mig som utvecklas av eHälsomyndigheten samt verksamt.se som är en myndighetsgemensam webbplats där det egna utrymmet tillhandahålls av den samverkande myndigheten i respektive e-tjänst.

Å ena sidan har kartläggningen visat att flera av de myndighetsrepresentanter som vi talat med känner sig trygga med den myndighetspraxis som har utvecklats när det gäller utformning av tjänster med eget utrymme. Att en sådan myndighetspraxis har kunnat utvecklas, och digitala tjänster har kunnat införas, beror till stor del på de vägledningar som har tagits fram inom ramen för E-delegationen.[9] Å andra sidan har flera av dem vi mött under kartläggningen framhållit att det fortfarande råder en rättslig osäkerhet inom området. Vilka tjänster kan anses omfattas av tryckfrihetsförordningens lokution ”endast som led i teknisk bearbetning eller teknisk lagring för annans räkning”? Vilken service kan en myndighet ge inom ramen för ett eget utrymme utan att en handling ska anses inkommen? Behövs ett uttryckligt författningsstöd för behandling av personuppgifter i ett eget utrymme? Dessa frågeställningar har också samband med frågor om hur dataskyddsregleringens krav på rättslig grund för personuppgiftsbehandling ska förstås beträffande egna utrymmen och hur personuppgiftsansvaret för behandling av personuppgifter i utrymmet ska fördelas. Även frågor om vem som tar ansvar för informationssäkerheten har relevans i sammanhanget.

Flera myndigheter framhåller att oproportionerligt mycket tid och resurser avsätts för att utreda fördelningen av personuppgiftsansvar i egna utrymmen. Under kartläggningen har någon röst hörts för att författningsreglering av tjänster med egna utrymmen är det enda rimliga alternativet för att bl.a. lösa fördelningen av personuppgiftsansvaret.

Myndigheter med breda kontaktytor mot allmänheten har en hög ambitionsnivå för den service de vill kunna erbjuda enskilda i deras användning av myndighetens digitala tjänster som inkluderar ett eget utrymme. Det ska vara enkelt för enskilda att hantera sina ärenden och myndigheten ska hålla hög kvalitet i handläggningen. Inom ramen för det egna utrymmet finns stor potential att förenkla för

[9] Vägledningarna är publicerade på eSamverkansprogrammets (eSam) webbplats, www.esamverka.se

enskilda i deras myndighetskontakter. Samtidigt kräver den service som lämnas inom ramen för ett eget utrymme ibland att myndighetens personal tar sådan befattning med de uppgifter som hanteras där, att det uppstår svåra gränsdragningsfrågor om åtgärden ska anses leda till att uppgifterna i utrymmet blir att anse som allmän handling. Även nödvändig teknisk support kan föranleda rättsfrågor. Har felaktigheter av någon anledning uppstått kan teknikerna behöva komma ”under huven” i systemet vilket innebär att de oundvikligen kommer att ta del av uppgifter som finns lagrade i den enskildes eget utrymme. Medför denna åtkomst att uppgifterna som teknikerna tar del av ska anses ha kommit in till myndigheten?

Kartläggningsarbetet visar vidare att det vid sidan av eget utrymme för enskilda också förekommer att myndigheter tillhandahåller motsvarande funktioner åt andra myndigheter. En sådan funktion, t.ex. ett mottagningsställe för elektroniska handlingar, kan fungera som ett eget utrymme för respektive myndighet där syftet är att de handlingar som hanteras inte anses som inkomna hos den mottagande myndigheten innan detta varit avsändarens avsikt. Eget utrymme för myndigheter är en företeelse som, såvitt vi kan bedöma, sannolikt kommer bli allt vanligare ju fler myndighetsgemensamma processer som digitaliseras.

> Exempel: I Lantmäteriets digitala tjänst för ansökan om lantmäteriförrättning tillhandahåller Lantmäteriet mottagningsställen för elektroniska handlingar åt de kommunala lantmäterimyndigheterna. Först när ansökningar når respektive kommuns mottagningsställe anses de vara inkomna till den kommunala lantmäterimyndigheten.

5.2.5 Språklagen

Frågan om vilket språk som kan användas i digitala tjänster är ytterligare en aspekt som har framhållits för oss. För domstolar, förvaltningsmyndigheter och andra organ som fullgör uppgifter i offentlig verksamhet är språket svenska.[10] Men för att alla och envar ska kunna använda sig av de digitala tjänster som det offentliga tillhandahåller behöver tjänsterna erbjudas på flera språk och enskilda måste kunna kommunicera på andra språk än svenska i tjänsterna.

[10] 10 § språklagen (2009:600).

Exempel: Till följd av bl.a. företagsrörligheten inom EU, tjänstedirektivet[11] och eIDAS-förordningen[12] ökar kraven på svenska myndigheters digitala tjänster. I Sverige gäller språklagen och det innebär t.ex. för en digital tjänst som tillhandahålls företag att information om ett företags verksamhet ska vara på svenska. När informationsutbyte sker över gränserna blir språket ett hinder eftersom enskilda från andra EU-länder i regel inte har tillräckliga kunskaper i svenska språket för att kunna använda sig av våra nationella digitala tjänster. Ska svenska alltjämt krävas för att t.ex. göra en ansökan i en digital tjänst behöver översättning ske automatiskt om tjänsten ska kunna utnyttjas av icke-svenskspråkiga individer. Norge har löst en viss del av problemet genom att företagsinformation kan registreras antingen på norska eller på engelska.

Myndigheter med breda kontakter mot allmänheten kan se en fortsatt inriktning mot att det behöver finnas rättsliga förutsättningar för att tillhandahålla digitala tjänster med flera olika språkalternativ. Förutom nationella minoritetsspråk rör det sig om språk som talas inom EU eller stora invandrarspråk.

5.3 Identiteter, underskrifter och annan koppling till person

5.3.1 Identiteter och identifiering

En effektiv och ändamålsenlig digital förvaltning kräver att traditionellt analoga förfaranden, t.ex. identifiering med id-kort, upprättande av pappersfullmakt, underskrift på papper m.m., kan ersättas av digitala motsvarigheter med bibehållen rättsverkan. Nya digitala rättsinstitut med koppling till fysiska personer behöver vara tillgängliga och användbara för alla oavsett om det är en privatperson, juridisk person eller behörig företrädare som utför en rättshandling.

En digital identitet måste kunna säkerställa kopplingen till en fysisk person. Det kan t.ex. göras genom att den digitala identiteten knyter an till en unik identitetsmarkör såsom personnummer. I kartläggningsarbetet pekar ett par myndighetsrepresentanter på att det i framtiden inte kommer vara tillräckligt att enbart använda person-

[11] Europaparlamentet och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden.
[12] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

nummer som unika identitetsmarkörer. Andra unika identitetsmarkörer som kan komma att bli aktuella sägs vara biometriska uppgifter eller passnummer.

Att en enskilds personnummer utgör den enda unika identitetsmarkören mellan dennes digitala identitet och det verktyg han eller hon använder för identifiering, t.ex. en e-legitimation, kan vara problematiskt.

Exempel: En enskild näringsidkare har inte något organisationsnummer utan driver sin verksamhet under sitt personnummer. En individ kan emellertid ha fler än en enskild firma vilket kan leda till otydligheter vid myndighetskontakter. I de fall den enskilde företräder sin firma är det ett problem att personnumret är den enda identifieraren. Hur ska myndigheten veta i vilken roll den enskilde agerar när denne använder sig av myndigheternas digitala tjänsteutbud? Företräder den enskilde sig själv som privatperson eller något av sina bolag? Bolagsverket framhåller att det vore önskvärt att näringsidkare, i stället för personnummer, tilldelas en annan typ av identitetsmarkör t.ex. ett löpnummer.

Exempel: Inom utbildningsväsendet skulle det underlätta om varje elev hade en digital identitet som kan användas i alla skol- och utbildningssammanhang, oavsett vilken skola eller utbildning eleven deltar i. En digital identitet möjliggör bl.a. för eleven att lagra sin information och kunna ta den med sig vid ett skolbyte.

5.3.2 Behöriga företrädare

Inom ramen för kartläggningsarbetet har några framfört uppfattningen att det ur vissa perspektiv är lättare att utveckla digitala tjänster som riktar sig till privatpersoner, t.ex. för socialförsäkringsförmåner, studiestöd, ansökan om förskola m.m. När det gäller digitala tjänster riktade till juridiska personer verkar utvecklingen ha gått långsammare. En förklaring kan vara att det saknas en utpekad myndighet som ensam ansvarar för att registrera alla typer av juridiska personer. Registreringsansvaret är i stället fördelat på flera olika aktörer, bl.a. Bolagsverket, Skatteverket, länsstyrelser och Lantmäteriet. För vissa juridiska personer saknas krav på registrering, t.ex. för föreningar, nätverk, klubbar och andra liknande sammanslutningar.

En konsekvens av det splittrade ansvaret är att det saknas ett centralt register eller decentraliserat system över samtliga juridiska personer dit det också skulle gå att koppla uppgifter om behöriga

företrädare. På samma gång är det orimligt att behörig firmatecknare i ett stort bolag själv ska utföra alla ärenden som rör registrering, avregistrering eller redovisning och som kräver behörig firmatecknares signering. När enskilda individer tvingas identifiera sig i rollen som privatperson, fast de företräder ett företag, väcks bl.a. frågor om vem som skulle bära det rättsliga ansvaret om ansvarsfrågor uppkommer under det aktuella digitala förfarandet.

Myndigheternas förutsättningar att utveckla e-tjänster där en behörig företrädare tillåts att agera för en juridisk persons räkning ser olika ut.

> Exempel: Inom ramen för programmet Serverat[13] har man identifierat att det finns behov av en nationell och tvärfunktionell behörighetslösning. Många av de ansökningar och anmälningar som kan göras till kommuner genom Serverat behöver utföras av behöriga företrädare för bolag. En behörig företrädare kan vara en fysisk person som har fått ledningens ansvar att agera för bolagets räkning. Det kan också vara ett externt företag som på uppdrag av ett annat bolag ska utföra en uppgift som kräver en ansökan eller anmälan, t.ex. ett skyltföretag som ska montera en skylt på en restaurangfasad och som behöver ansöka om bygglov hos kommunen.

Även myndigheter behöver utse behöriga företrädare för att utföra rättshandlingar digitalt i myndighetens namn, t.ex. i bygglovsärenden. Därtill kan även fysiska personer ha behov av att låta ett ombud agera i deras ställe.

5.3.3 Fullmakter

En del av de myndighetsrepresentanter som deltagit i kartläggningsarbetet menar att ett centralt fullmaktsregister skulle underlätta digitala processer och på sikt möjliggöra fler automatiserade myndighetsbeslut. Det förtjänar dock att nämnas att även motsatta synpunkter har lagts fram. Frågan om digitala fullmakter är komplex, oavsett om de finns att tillgå i ett centralt register eller inte. Hur återkallas en digital fullmakt? Går det att använda blockkedjeteknik[14] för att upprätta en rättsligt giltig fullmakt? Finns det eller

[13] SKL driver programmet Serverat tillsammans med kommuner, Tillväxtverket och Bolagsverket. Syftet med Serverat är att utveckla digitala lösningar för att förenkla för restaurangföretagare att starta och driva företag. Se även kapitel 5.11.5.
[14] Se kapitel 7.3.4 för beskrivning av blockkedjetekniken.

går det att åstadkomma nödvändiga rättsliga förutsättningar för en aktör att tillhandahålla ett centralt register över fullmakter?

5.3.4 Underskrifter och andra liknande rättsinstitut

Kartläggningsarbetet visar att det inte alltid är tydligt när en fysisk underskrift kan ersättas med en digital. Ibland är det juridiska förutsättningar i kombination med andra svårlösta frågor som gör att det tar tid att utveckla nya lösningar.

> Exempel: Socialstyrelsen har utvecklat en tjänst för digitala ansökningar om vårdlegitimation, bl.a. läkarlegitimation. Det kvarstår dock vissa manuella moment kopplade till underskrifter som måste kunna lösas tekniskt innan hela förfarandet kan digitaliseras. Den som ansöker om läkarlegitimation ska bifoga en s.k. AT-bok vari klinikernas verksamhetschefer ska lämna fyra separata intyganden om den utförda allmäntjänstgöringen. En förutsättning för att AT-boken ska kunna skickas in digitalt är att verksamhetscheferna kan lämna digitala intyganden, t.ex. med stöd av digitala underskrifter. Socialstyrelsen måste dessutom ha anpassad teknik som ger möjlighet att hantera och verifiera de digitala underskrifterna. Exemplet är belysande i så måtto att det pekar på svårigheterna, juridiskt och tekniskt, med att implementera digitala underskrifter i en i övrigt automatiserad process.

Ett flertal myndighetsrepresentanter vittnar om problematiken i att avgöra när det befintliga regelverket medger, kräver eller hindrar användning av elektroniska underskrifter. Om uppgifter ska lämnas på *heder och samvete* – innebär det att den enskilde måste bekräfta uppgifternas riktighet med stöd av en elektronisk underskrift? Eller går det lika bra att bekräfta att uppgifterna är riktiga genom att klicka i en ruta i webbläsaren eller att lämna ett muntligt intygande per telefon?

Det kan dessutom finnas behov av att kunna koppla både digitala och analoga underskrifter till ett och samma dokument utan att behöva framställa dubbletter av dokumentet i fråga, t.ex. när flera olika individer med sinsemellan olika tekniska förutsättningar ska signera samma handling.

Frågor om hur andra traditionellt analoga rättsinstitut kan överföras till digitala processer har också lyfts fram. Det är t.ex. oklart hur ett bestyrkande kan göras i en digital process. Inom fastighetsrättens område används också s.k. makemedgivanden. Om det i

dagsläget finns rättsliga förutsättningar att lämna ett sådant medgivande digitalt är ännu inte utrett.

5.3.5 Delgivning

Behovet av att använda nya tekniska lösningar för att delge enskilda personer handlingar med t.ex. kallelse till domstolsförhandling har framhållits under kartläggningen. Inställda domstolsförhandlingar är ett stort problem för rättsväsendet, nästan en fjärdedel av alla förhandlingar ställs in och huvudorsaken är bristande delgivning. En förändring av delgivningssystemet i linje med den danska modellen, där varje medborgare utrustas med en officiell e-postbrevlåda och där man anses delgiven om meddelandet skickats dit har diskuterats av vissa. Nuvarande delgivningsmöjligheter beskrivs ha flera brister som, i vart fall delvis, skulle kunna åtgärdas med hjälp av rättslig reglering som stödjer digitala förfaranden.

Exempel: Delgivningslagen[15] innehåller flera regler med koppling till analoga förfaranden. I dag hanteras delgivningshandlingar på papper i stängda kuvert. Det rör sig många gånger om brådskande ärenden, t.ex. en kallelse till en förhandling, som ska delges en enskild. När personen som ska delges väl påträffas sker det dock inte sällan på en annan plats än där de fysiska delgivningshandlingarna befinner sig. Följden kan bli att delgivning inte kan ske och att t.ex. en domstolsförhandling måste ställas in.

5.4 Grunddata och informationsförsörjning

Bolagsverket, Lantmäteriet, Skatteverket och Transportstyrelsen är registeransvariga myndigheter för s.k. grunddata.[16] I ett grunddataregister lagras uppgifter som på ett eller annat sätt inhämtats från en rad olika aktörer till den registeransvariga myndigheten. Den inrapporterande aktörens skyldighet att överföra uppgifter till den registeransvariga myndigheten är i regel författningsstyrd. Lagstiftningen är, såsom vi fått det beskrivet, inte sällan omfattande och fragmenterad.

[15] Delgivningslagen (2010:1932).
[16] Det saknas en legaldefinition av begreppet grunddata. I detta sammanhang avses med grunddata sådan grundläggande registerinformation som finns i fastighetsregistret, folkbokföringsregistret, vägtrafikregistret, de olika företagsregistren och viss geografisk information.

Kartläggningsarbetet visar vidare att det inte är helt tydligt vad ett författningsreglerat registeransvar faktiskt innebär. Måste myndigheten som ska föra registret lagra all information själv? Eller är det tillräckligt att informationen är åtkomlig via den myndigheten genom att myndigheten, när informationen behövs eller efterfrågas, gör ett direktanrop till den aktör som faktiskt producerar informationen i fråga? Flera anser att uppgifter exempelvis bara ska lagras hos den myndighet som ursprungligen har inhämtat eller producerat uppgiften och hämtas där vid behov. Det finns med andra ord en strävan mot att uppgifter ska hämtas vid den ”bästa källan”.

Exempel: Lantmäteriet har i uppdrag att tillhandahålla fastighetsregistret. Varje dag fattas tusentals beslut baserade på beslutsunderlag från fastighetsregistret. Uppdateringen av registret sker i dag på olika sätt och med olika handläggnings- och registreringssystem. I vissa fall är uppdateringen helt eller delvis digital men ren analog registrering förekommer fortfarande. Att uppdateringen sker på flera olika sätt och av flera olika aktörer innebär att uppgifterna kan variera i kvalitet och aktualitet.

Några myndighetsrepresentanter har också gett uttryck för att insamling och registrering av uppgifter, även när det inte rör sig om grunddata, kan kräva mycket manuellt arbete. Det kan vara en utmaning att se till att registren innehåller uppgifter av god kvalitet och som därtill är aktuella och uppdaterade.

Exempel: Socialstyrelsen ansvarar för flera olika register med koppling till hälso- och sjukvård och socialtjänstområdet. Insamlingen av registeruppgifter regleras av flera olika förordningar och i vissa fall finns formatkrav för uppgifterna i Socialstyrelsens egna föreskrifter. För vissa av registren krävs det i nuläget mycket manuellt arbete både hos de aktörer som ska förse Socialstyrelsen med uppgifter och hos Socialstyrelsen för att säkerställa att de uppgifter som tillförs registren håller en godtagbar kvalitet. Den manuella hanteringen medför eftersläpningar i registreringen vilket leder till att underlag för rapporter m.m. inte är uppdaterade i den mån som eftersträvas. För Socialstyrelsen och för de aktörer som använder uppgifterna i registren finns stora vinster att vänta om den manuella hanteringen framöver kan minskas.

Behovet av ytterligare uppgifter än dem som i nuläget finns i t.ex. nationella grunddataregister har också framförts. Det gäller särskilt uppgifter om personer, där folkbokföringsadress m.fl. befintliga uppgifter anses behöva kompletteras med kontaktuppgifter för digital kontakt med enskilda.

I dagsläget kan statliga myndigheter utbyta grunddata avgiftsfritt. Ekonomistyrningsverket har i en rapport föreslagit en ny finansieringsmodell i syfte att även kommuner och landsting ska omfattas av det avgiftsfria grunddatautbytet.[17] Även om förslaget genomförs kommer dock avgiftskravet kvarstå i förhållande till privata aktörer. Flera myndigheter påtalar att kravet på att ta ut avgifter för grunddata kan verka hindrande för en effektiv och ändamålsenlig användning av informationen.

> Exempel: Inom ramen för tjänsten Mina meddelanden lämnar Bolagsverket efter begäran ut uppgifter om behöriga företrädare för företag, t.ex. firmatecknare, till Skatteverket. Skatteverket lämnar i sin tur ut uppgifterna i fråga till privata brevlådeoperatörer anslutna till Mina meddelanden. Utlämnandet av uppgifter från Bolagsverket till Skatteverket sker avgiftsfritt liksom utlämnandet från Skatteverket till brevlådeoperatörerna. Bolagsverket saknar dock förutsättningar att utan avgift lämna ut uppgifterna direkt till de privata brevlådeoperatörerna. Det är dock värt att notera att huvudskälet till den valda lösningen är en annan, nämligen att få likformig tolkning av regelverket. Att avgifterna hanteras är en positiv bieffekt av detta.

Ett annat rättsligt problem som kan uppstå bl.a. till följd av avgiftskravet är att det skapas kopior av register med uppgifter av sämre kvalitet hos andra aktörer som t.ex. har begärt ut uppgifterna i fråga med stöd av offentlighetsprincipen. Kopior av register med uppgifter av sämre kvalitet, och som inte hålls uppdaterade i samma utsträckning, kan vara olämpligt ur dataskyddssynpunkt.

5.5 Informationsutbyten

5.5.1 Informationssäkerhet

I digitaliseringsarbetet står myndigheterna inför många gemensamma utmaningar. Det gäller inte minst informationssäkerheten. Flera av dem vi träffat har påtalat att ju mer information som samlas in och hanteras desto svårare blir det att leva upp till säkerhetskraven.

[17] *Ny finansieringsmodell för grunddatautbyte mellan statliga myndigheter samt kommuner och landsting* (ESV 2017:54).

Varje myndighet ansvarar självständigt för att informationsklassa sin information.[18] Men när myndigheter samverkar och utbyter information framhålls att det behövs en enhetlig informationsklassning för att informationen ska få likvärdigt skydd hos alla myndigheter som hanterar den. Inom ramen för myndighetsgemensamma system uppstår dessutom ofta nya informationsmängder och även dessa måste kunna hanteras korrekt ur ett informationssäkerhetsperspektiv.

I kartläggningsarbetet har vissa myndighetsrepresentanter efterfrågat mer styrande reglering kring myndigheternas informationssäkerhetsarbete. Någon har framfört att det vore lämpligt med en förvaltningsgemensam reglering av behörighetsstyrning. På så sätt skulle man kunna säkerställa tillgänglighet till information av god kvalitet till dem som har ett konstaterat behov av att ta del av informationen från en viss källa. Någon annan har framfört att ett bredare tillsynsuppdrag över myndigheters arbete med informations- och cybersäkerhet behövs.

5.5.2 Registerförfattningar

En majoritet av dem vi träffat har framhållit att lagstiftningen ofta hindrar eller hämmar myndigheternas önskade informationsutbyten vid digitala utvecklingsarbeten. Problemen beskrivs vara främst hänförliga till dataskyddsregleringen i särskilda registerförfattningar och sekretessregleringen.

Myndighetsrepresentanterna är relativt samstämmiga i uppfattningen att dataskyddsregleringen är svåröverskådlig, komplex, fragmenterad och onödigt detaljerad. Detaljreglering av informationsutbyten har lett till att regelverket över tid har blivit ett lappverk eftersom nya uppgiftsutbyten ideligen kräver författningsändringar. Lagstiftningsarbetet håller inte heller det tempo som myndigheternas utvecklingsarbeten kräver vilket leder till att arbetena fördröjs eller genomförs endast delvis, dvs. inte med den fulla potential som först identifierats. Några har framfört att det vore önskvärt att

[18] Med informationsklassning avses att genom konsekvensanalys identifiera skyddsbehovet för en viss informationsmängd. Se 4 § Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1).

författningsreglera digitala informationsutbyten på mer principiell nivå, kanske inom ramen för en generell myndighetsdatalag.[19]

Två sätt att reglera digitalt utlämnande

I registerförfattningar regleras inte sällan i vilken utsträckning det är tillåtet med utlämnande på medium för automatiserad behandling eller med direktåtkomst till personuppgifter. Det saknas legaldefinition av såväl begreppet utlämnande på medium för automatiserad behandling som begreppet direktåtkomst.

Frågan om vad som är direktåtkomst och vad som är utlämnande på medium för automatiserad behandling har emellertid börjat klarna efter Högsta förvaltningsdomstolens (HFD) dom om Försäkringskassans fråga/svartjänst LEFI Online.[20] I regel synes myndigheternas målsättning nu vara att de system som utvecklas för informationsöverföring ska spegla den tekniska lösningen i LEFI Online. På så sätt blir det inte fråga om direktåtkomst för den mottagande myndigheten. Uppgifterna anses i stället utlämnade på medium för automatiserad behandling och myndigheterna slipper den särskilda problematik med överskottsinformation som blir en effekt av direktåtkomst.[21]

En konsekvens av HFD:s dom är att visst informationsutbyte, som tidigare förmodats vara direktåtkomst och reglerats därefter, snarare utgör utlämnande på medium för automatiserad behandling med den teknik som numera används. Som en följd härav har viss reglering av direktåtkomst kommit att bli överflödig. Någon av dem vi talat med menar dock att bestämmelser om direktåtkomst ändå kan ha ett signalvärde trots att bestämmelserna inte tillämpas i praktiken.

---

[19] Se Informationshanteringsutredningens betänkande *Myndighetsdatalag* (SOU 2015:39).

[20] Se HFD 2015 ref. 61. Frågan i målet gällde om socialnämndernas åtkomst till uppgifter i socialförsäkringsdatabasen genom datasystemet LEFI Online var att anse som direktåtkomst i socialförsäkringsbalkens mening. I målet fann HFD att innebörden av begreppet direktåtkomst i socialförsäkringsbalken skulle bestämmas med utgångspunkt i bestämmelserna i 2 kap. 3 § andra stycket tryckfrihetsförordningen.

[21] Överskottsinformation uppstår därför att det på förhand inte går att avgöra vilka specifika uppgifter i den utlämnande myndighetens informationssamling som den mottagande myndigheten kan komma att behöva ta del av. Oaktat det förhållandet att den mottagande myndigheten inte behöver ta del av vissa uppgifter gäller enligt tryckfrihetsförordningen att uppgifterna anses vara inkommen allmän handling hos den mottagande myndigheten. Se mer om överskottsinformation i Informationshanteringsutredningens betänkande *Överskottsinformation vid direktåtkomst* (SOU 2012:90).

Direktåtkomst

Reglering om direktåtkomst är ofta detaljerad. Inom ramen för kartläggningsarbetet vittnar flera om att en sådan reglering i praktiken inte alltid uppfyller sitt syfte. Det kan bl.a. bero på att det är svårt att förutse exakt vilka uppgifter den mottagande myndigheten faktiskt har behov av. Om behovet förändras krävs en författningsändring som tar tid. När direktåtkomsten inte uppfyller den mottagande myndighetens informationsbehov kan det få effekten att den utlämnande myndigheten, vid sidan av direktåtkomsten, också manuellt måste hantera begäran om utlämnande av uppgifter.

> Exempel: Transportstyrelsen har direktåtkomst till uppgifter i Polismyndighetens misstanke- och belastningsregister. I vissa ärenden, t.ex. körkortstillstånd, har dock Transportstyrelsen behov av ytterligare information än den som ges via direktåtkomsten. Detta leder till att Polismyndigheten årligen, vid sidan av det utlämnande som sker genom direktåtkomsten, behöver hantera över 30 000 begäran om utlämnande till Transportstyrelsen rörande kompletterande ärendeinformation.

Det förekommer också att den mottagande myndighetens direktåtkomst är inskränkt genom sökbegränsningar, dvs. att myndigheten saknar rättsligt stöd för att använda vissa sökbegrepp i den utlämnande myndighetens informationssamling. Om det gjorts avsevärda sådana sökbegräsningar kan det innebära att den mottagande myndigheten inte kan få den information som den har behov av.

> Exempel: I lagen om fastighetsregister[22] finns ett förbud mot att använda personnummer eller del av personnummer som sökbegrepp vid direktåtkomst. Vissa myndigheter har emellertid behov av att kunna söka på personnummer i fastighetsregistret. Eftersom nuvarande lagstiftning inte medger detta inom ramen för regleringen av tillåten direktåtkomst behöver den uppgiftshämtande parten kontakta Lantmäteriet för att få stöd med sådana sökningar i varje enskilt fall. Ett annat alternativ som tillämpas i stället för direktåtkomst är att begära ut kopior av relevanta delar av registret för att möjliggöra verksamhetsanpassade sökningar hos den mottagande aktören. En reglering som har till syfte att skydda den enskildes personliga integritet kan på det sättet, dvs. genom att vara alltför restriktiv, leda till ökat utlämnande.

Inom ramen för kartläggningsarbetet har ett par myndighetsrepresentanter också lämnat exempel på oönskad direktåtkomst, dvs. där

[22] Lagen (2000:224) om fastighetsregister.

myndigheterna om val funnits hellre hade fått uppgifterna utlämnade på medium för automatiserad behandling i stället för genom direktåtkomst. På så sätt slipper mottagande myndighet bl.a. att hantera problemet med överskottsinformation.

Utlämnande på medium för automatiserad behandling

Det finns inte någon enhetlig systematik för hur utlämnanden på medium för automatiserad behandling är reglerade. I vissa registerförfattningar, t.ex. 114 kap. socialförsäkringsbalken, är regleringen om utlämnande på medium för automatiserad behandling förhållandevis tillåtande.[23] I andra registerförfattningar, t.ex. studiestödsdatalagen och studiestödsdataförordningen, finns en uttömmande reglering av vilka uppgifter som får lämnas ut under vilka förutsättningar. En sådan detaljerad reglering kan hindra digitala informationsutbyten.

Detaljreglering avseende tillåtligheten av utlämnande på medium för automatiserad behandling kan hindra myndigheter från att exempelvis digitalisera masshantering av ärenden som innefattar informationsöverföring till en annan myndighet, t.ex. överklagandeärenden till domstol eller nämnd. Digitalisering av stora ärendeflöden ger betydande effektivitetsvinster för myndigheterna men kan bara ske under förutsättning att den rättsliga regleringen stödjer elektroniskt utlämnande.

5.5.3 Sekretess

Även sekretessregleringen kan uppställa hinder mot nödvändiga och ändamålsenliga informationsutbyten mellan myndigheter. I kartläggningsarbetet har vissa myndighetsrepresentanter framhållit problematiken med sekretessgränser mellan olika verksamheter i förvaltningen. Sekretessgränser uppstår delvis som en följd av hur statsförvaltningen är organiserad med självständiga myndigheter. Men sekretessgränser kan dessutom finnas inom skilda verksamhetsområden hos en och samma myndighet. Sekretessgränser uppstår också som en effekt av hur en kommunal verksamhet väljer

[23] 114 kap. 24–26 a §§ socialförsäkringsbalken och *Behandling av personuppgifter inom socialförsäkringens administration*, prop. 2002/07:135 s. 97 f.

att organisera sig. Varje enskild nämnd utgör en egen myndighet med egna sekretessgränser. Det kan ifrågasättas om förvaltningens val av organisation verkligen ska ha den betydelsen som sekretessgränserna medför.

En förutsättning för att en myndighet ska kunna lämna ut en uppgift till en annan myndighet är att utlämnandet inte hindras av sekretess. Som utgångspunkt gäller sällan sekretess i förhållande till den enskilde som berörs av ett ärende. I myndighetsgemensamma tjänster som tillhandhålls enskilda har därför i vissa fall valet gjorts att sekretessbelagda uppgifter lämnas ut till den enskilde först. Denne får i sin tur välja om uppgifterna ska lämnas vidare till en annan myndighet. Den enskilde har då själv kontroll över processtegen. Men några har framfört att de tekniska processer som utvecklas blir onödigt tillkrånglade, särskilt med tanke på att digitaliseringen ska förenkla enskildas kontakter med myndigheter.

I sektorsspecifik lagstiftning kan det finnas detaljerad reglering av uppgiftsskyldigheter och sekretessgenombrott. Om det i samband med utvecklingsarbeten klargörs att den mottagande myndigheten har behov av ytterligare någon uppgift, det kan vara en enstaka uppgift, men den inte finns uppräknad i den sekretessbrytande bestämmelsen kan detta utgöra ett hinder i arbetet med att utveckla enklare tjänster för enskilda och därmed uppnå en mer effektiv digital informationshantering. Så som vi fått beskrivet för oss genomförs ändå utvecklingsarbetet med det digitala informationsutbytet, utan att alla uppgifter som det egentligen finns behov av kommer att utbytas. Myndigheterna hemställer således inte alltid om författningsändringar för att få till stånd ett mer effektivt förfarande.

5.5.4 Informationsutbyte med privata utförare

Kartläggningsarbetet visar att den kommunala sektorn upplever hinder för informationsutbyten med privata utförare. Det rör sig delvis om att regelverket, främst dataskydds- och sekretessregleringen, kan uppställa hinder för en kommun att lämna ut information. Det beskrivs emellertid att det även i flera avseenden saknas modeller, system och standarder som möjliggör digitala informationsutbyten. Det är också oklart om en kommun kan kräva av

privata utförare att de ska använda sig av ett specifikt format för att hantera sin information för att möjliggöra informationsutbyte.

Ett exempel är problem med informationsöverföringar när elever byter skola. Den nya skolan behöver information om såväl elevens kunskapsläge som om elevens hälsa och eventuella behov av särskilt stöd. Skolor med kommunala huvudmän kan i regel lämna ut information med stöd av generalklausulen i offentlighets- och sekretesslagen.[24] Men när uppgifter behöver lämnas från en fristående skola, vars anställda lyder under tystnadsplikt, görs i regel bedömningen att eleven eller förmyndaren behöver lämna samtycke för att sekretessbelagda uppgifter ska kunna lämnas ut till den nya skolan. Det upplevs som inkonsekvent att olika regler gäller för den digitala informationsöverföringen beroende på om en skola har en privat eller en offentlig huvudman.

Kartläggningsarbetet visar också att det inom hälso- och sjukvårdssektorn finns utmaningar med informationsutbyte mellan de inblandade aktörerna. Sekretessgränser finns såväl mellan landstingsfinansierade och kommunala vårdgivare som mellan privata vårdgivare och andra privata utförare. Även aktörer som bidrar med åtgärder närliggande vårdsektorns, t.ex. rehabilitering och arbetsterapi, har behov av att kunna ta del av viss information från vårdgivare. Problematiken är särskilt märkbar för multisjuka och deras anhöriga när överlämning mellan vårdgivare inte fungerar optimalt på grund av att regelverket uppställer hinder mot informationsutbyte.

Privata utförare vars anställda omfattas av tystnadsplikt, t.ex. inom hälso- och sjukvården, ställs inför frågan om en informationsöverföring till en myndighet innebär ett obehörigt röjande av sekretessbelagda uppgifter. Det kan röra sig om en privat utförare som agerar på uppdrag av en kommunal nämnd. Kan den privata utföraren i detta läge lämna sekretessbelagda uppgifter till den kommunala nämnden utan att uppgifter röjs obehörigen?

5.5.5 Informationsutbyte ur ett internationellt perspektiv

Frågan om möjligheter att tillhandahålla direktåtkomst eller lämna ut uppgifter på medium för automatiserad behandling aktualiseras också i EU-rättsliga sammanhang. EU-rättsliga regler kan ställa krav

[24] 10 kap. 27 § offentlighets- och sekretesslagen.

på informationsutbyten mellan medlemsländernas myndigheter. Vissa av dem vi träffat framhåller att det behöver klargöras om det, när nationella registerförfattningar innehåller regler om direktåtkomst, också krävs rättsligt stöd för att medge direktåtkomst till utländska organisationer när informationsutbytet följer av EU-rätt. Och har det någon betydelse om utlämnandet sker till statliga eller privata aktörer? Den rättspraxis och de vägledningar som finns rörande direktåtkomst gäller bara nationella förhållanden och i första hand direktåtkomst mellan myndigheter. Frågan om vad som egentligen utgör direktåtkomst har här också relevans (se kapitel 5.5.2).

Även andra exempel på när just internationella informationsutbyten ställer rättsliga frågor på sin spets har lämnats under kartläggningen.

> Exempel: Av förarbetena till studiestödslagstiftningen framgår att CSN förutsätts lämna ut personuppgifter till studiestödsmyndigheter i andra länder i syfte att säkerställa att enskilda inte uppbär studiestöd från flera olika länder samtidigt. Studiestödsdatalagen ger CSN rätt att behandla personuppgifter för ändamålet att lämna ut dem i den mån en sådan skyldighet föreligger för myndigheten. Det saknas dock en rättslig skyldighet för CSN att lämna ut uppgifter till utländska studiestödsmyndigheter varför det rättsliga stödet är mycket svagt för den personuppgiftsbehandling CSN förutsätts utföra.

5.5.6 En uppgift en gång – The Once-Only Principle

Arbetet med att förenkla för företagare och privatpersoner genom att de bara ska behöva lämna samma uppgift en gång till den offentliga förvaltningen bedrivs både nationellt och på EU-nivå.[25] Regeringens målsättning är att uppgifter, i de fall det är möjligt och relevant, bara ska behöva lämnas en gång.[26]

Av kartläggningsarbetet framgår att principen om en uppgift en gång än så länge inte har fått något större genomslag i den offentliga förvaltningen. En förutsättning för att principen om en uppgift en gång ska kunna genomföras är att myndigheterna kan hämta informationen från bästa källan t.ex. den myndighet som initialt har hämtat in eller producerat uppgiften i fråga. Sekretesslagstiftningen

[25] Se t.ex. EU:s handlingsplan för e-förvaltning för 2016–2020, Snabbare digital omvandling av förvaltningar, COM (2016) 179 final och Uppgiftslämnarutredningens slutbetänkande *Uppgiftslämnarservice för företagen*, (SOU 2015:33).
[26] *Budgetpropositionen för 2017*, prop. 2016/17:1, utg.omr. 22, avsnitt 4.5.1.

kan emellertid uppställa hinder mot att den myndighet som förfogar över bästa källan lämnar ut uppgifterna i fråga. Även ändamålsbestämmelser i registerförfattningar kan hindra att personuppgifter lämnas ut till en myndighet för fortsatt behandling där.

Exempel: Skatteverkets sekretessreglering utgår i från att absolut sekretess råder för uppgifter i beskattningsdatabasen. Den stränga sekretessregleringen innebär bl.a. att Skatteverket måste samla in enskildas kontaktuppgifter flera gånger när de behövs i Skatteverkets skilda verksamhetsgrenar. Sekretessen hindrar också Skatteverket från att lämna ut enskildas kontaktuppgifter till andra myndigheter.

Exempel: Inom vård- och läkemedelssektorn har principen om en uppgift en gång svagt genomslag på grund av rådande sekretessgränser. Patienter måste gång på gång lämna samma information t.ex. vid sina kontakter med vårdgivare. Det kan röra sig om väsentliga uppgifter om allergier, kontaktpersoner, läkemedel m.m.

Exempel: Sekretessgränser mellan kommunala nämnder kan hindra återanvändande av uppgifter mellan nämnderna. Kommunala nämnder utgör separata myndigheter och uppgifter kan inte överföras från en nämnd till en annan utan att det finns lagligt stöd för detta. Det kan leda till att samma typ av uppgifter lagras på många olika ställen hos de olika nämnderna.

Exempel: De ärendeslag som hanteras inom en och samma myndighet kan spänna över ett stort och mångfacetterat område. Om personuppgifter som enskilda lämnat till myndigheten inom ramen för ett ärendeslag ska kunna behandlas inom ramen för ett annat ärendeslag behöver det finnas rättsligt stöd i dataskyddsregleringen för behandlingen för det nya ändamålet.

5.5.7 Vilka uppgifter uppfyller myndigheternas faktiska informationsbehov?

Vid reglering av uppgiftsutbyten mellan myndigheter kan det vara svårt att förutspå, för såväl lagstiftaren som för myndigheterna i fråga, vilka uppgifter som en mottagande myndighet faktiskt har behov av på längre sikt. Den rättsliga regleringen kring vilka uppgifter som får lämnas ut på medium för automatiserad behandling eller genom direktåtkomst leder inte alltid till att den mottagande myndighetens faktiska informationsbehov uppfylls, trots att detta många gånger får förutsättas ha varit avsikten.

Regleringen kan också innehålla begränsningar såtillvida att informationen inte kan lämnas vid den tidpunkt, eller snarare inte kan lämnas vid det processteg som egentligen önskas. Regleringen kan t.ex. medge att en myndighet får lämna ut en uppgift till en annan myndighet om att ett visst beslut har fattats i ett ärende. Den utlämnande myndigheten får alltså först när beslutet har expedierats upplysa den mottagande myndigheten om viss information. Men redan det förhållandet att en enskild har givit in en ansökan om en förmån till den utlämnande myndigheten kan vara den relevanta informationen för den mottagande myndigheten i den myndighetens ärendehandläggning, inte det beslut som sedermera fattas.

Det förekommer också att reglering kring informationsutbyten knyter an till traditionell pappershantering och till tidsperspektiv som inte längre är aktuella när beslutsprocesser har automatiserats. Lagstiftningen har med andra ord inte uppdateras i takt med att digitala processer har effektiviserat den offentliga förvaltningen. Detta leder till att myndigheter kan behöva fatta beslut som grundas på uppgifter som är onödigt gamla.

> Exempel: Beslut om återbetalning av studiemedel grundar sig bl.a. på enskildas inkomstuppgifter från två år tillbaka i tiden. I dagens digitala förvaltning finns dock reella möjligheter att grunda återbetalningsbeslutet på mer aktuella uppgifter.

Ytterligare en aspekt att beakta vid informationsutbyten är att myndigheter måste kunna förlita sig på att de uppgifter som överförs är korrekta. Det förekommer att enskilda rapporterar in en uppgift till en myndighet som därefter ska överföra samma uppgift till en annan myndighet. Har den enskilde rapporterat in en uppgift som inte överensstämmer med verkliga förhållanden kan det leda till att de myndigheter som är sekundära mottagare av uppgiften i fråga grundar sitt beslutsfattande på felaktig information.

> Exempel: Arbetsgivare ska månadsvis lämna digitala arbetsgivardeklarationer på individnivå till Skatteverket. De uppgifter som rapporteras in ska Skatteverket kunna lämna ut digitalt till Försäkringskassan, Migrationsverket och Arbetsförmedlingen som använder dem som beslutsunderlag i sin respektive ärendehandläggning. Eftersom uppgifterna i fråga initialt härrör från de inrapporterande arbetsgivarna kan Skatteverket inte garantera att uppgifterna är korrekta. Det kan leda till att de mottagande myndigheterna fattar beslut på ett felaktigt eller ofullständigt beslutsunderlag. Regleringen anger emellertid att det är den individuppgift som lämnats av arbetsgivaren som ska lämnas vidare.

Digital information skulle kunna beskrivas ha tre olika beståndsdelar.

1. Beståndsdata, dvs. en saklig uppgift som sådan, t.ex. en uppgift om beskattning.
2. Processdata, dvs. information om hur en uppgift har tagits fram.
3. Metadata, dvs. uppgifter som beskriver innehållet eller strukturen i en viss informationssamling.

Lagstiftning som rör informationsutbyten mellan myndigheter omfattar i regel enbart det som i exemplet ovan benämns som beståndsdata. Med nya tekniska möjligheter skulle det, med ett annat sätt att beskriva problematiken som exemplifierats ovan, kunna vara mer intressant att veta att en person är skönstaxerad (processdata) än själva taxeringsuppgiften (beståndsdata).

5.5.8 Informationsstandarder

Inom ramen för kartläggningsarbetet har det tydligt framgått att myndigheter har behov av gemensamma informationsstandarder. En standard kan sägas vara en gemensamt överenskommen lösning på ett återkommande problem. För informationshanteringen efterfrågas standarder för bl.a. digitala format, certifikat, gränssnitt och metadata. Riksarkivet har ett pågående arbete med att ta fram förvaltningsgemensamma specifikationer[27] för, i första hand, statliga myndigheter.[28] Att det inte funnits någon utpekad aktör som haft ansvar för frågan om gemensamma standarder för informationshanteringen inom den offentliga förvaltningen har påpekats vara en brist.[29]

I kartläggningsarbetet har det påtalats att det behövs en samordning av vilka krav på standarder som ska ställas av det offentliga när system utvecklas eller upphandlas. Avsaknaden av samordning

[27] En förvaltningsgemensam specifikation är en specifikation som beskriver hur man strukturerar information i ett utbytesformat som möjliggör överföring av information till valfritt system, valfri e-tjänst, annan myndighet, mellan arkiv, slutarkiv osv., samt identifiering av informationen.
[28] Se Riksarkivets regleringsbrev för budgetåret 2018 (Ku2017/00774/KL m.fl.).
[29] Regeringen har beslutat att inrätta en ny myndighet för digitalisering av den offentliga sektorn som bl.a. ska. kunna meddela föreskrifter om nationell digital infrastruktur, såsom tillämpning av standarder, format och specifikationer för informationsutbyte, it-system och grunddata (dir. 2017:117).

kan leda till oklarheter när en myndighet t.ex. har fått bemyndigande att på ett visst område föreskriva om standarder. Även på föreskriftsnivå behöver det finnas en samordning för att få en helhetssyn.

Nedan ges ett exempel på arbete med att enhetliggöra olika typer av standarder för att skapa en gemensam informationsstruktur.

> Exempel: Socialstyrelsen har ett pågående arbete för att skapa en gemensam informationsstruktur för hälso- och sjukvården och socialtjänsten i syfte att information som registreras om t.ex. patienter och brukare ska kunna återanvändas på ett ändamålsenligt sätt. En ändamålsenlig och strukturerad dokumentation innebär att varje behov av information är tillgodosett. Det finns flera olika behov varav ett är att dokumentationen ska vara en utgångspunkt för vård, stöd och behandling av en enskild individ. Genom att använda en gemensam beskrivning av processen i vård och omsorg, utifrån ett patient- och brukarperspektiv, kan olika verksamheter strukturera sin dokumentation om en och samma individ på samma sätt även om de bara deltar i delar av processen. Då blir det lättare att sammanställa och samordna vad som är planerat eller genomfört kring individens hälsotillstånd så att nästa aktör kan ta vid och fortsätta processen. Den gemensamma beskrivningen säkerställer att dokumentationen kan återanvändas och att den kan följa individen mellan olika aktörer och organisationer. I Socialstyrelsens arbete ingår för det första att skapa en nationell informationsstruktur med enhetliga process-, begrepp- och informationsmodeller för hälso- och sjukvården och socialtjänsten. För det andra krävs ett nationellt fackspråk grundat på Socialstyrelsens termbank, hälsorelaterade klassifikationer och Snomed CT (ett internationellt medicinskt begreppssystem som är utvecklat för att användas i digitala informationssystem). Den nationella informationsstrukturen beskriver verksamheten inom vård och omsorg på en generisk nivå med processmodeller (vad gör man i verksamheten), begreppsmodeller (vilka företeelser i verksamheten skapar informationsbehov, vilken typ av information behövs av vem i processen) och informationsmodeller (vilken information ska dokumenteras och hur olika informationsmängder hänger ihop). Tillsammans skapar modellerna en karta över det som behöver dokumenteras i verksamheten för att olika informationsbehov ska tillgodoses och säkerställer att information kan återanvändas i flera delar av processen.

Exemplet från Socialstyrelsen visar bl.a. att en ändamålsenlig informationsförsörjning inte i första hand bygger på tekniska komponenter utan på gemensamma definitioner, modeller och beskrivningar av information.

I kartläggningsarbetet framhåller vissa myndigheter att arbetet med gemensamma standarder går fortare på EU-nivå än nationellt och att det kanske beror på att tekniska krav fastställs direkt i de

EU-gemensamma regelverken. I Inspire-direktivet[30] finns en detaljerad reglering av standarder. Det är positivt i bemärkelsen att det ger en god styrning. Men samtidigt är den regleringen så pass detaljerad att den riskerar att snabbt låsa in gammal teknik.

5.6 Digitalisering av ärendeprocesser och automatiserat beslutsfattande

5.6.1 Reglering av ärendeprocesser

Digitalisering av förvaltningen stannar inte vid digital kommunikation med enskilda när t.ex. ärenden inleds i en digital tjänst eller digitala informationsutbyten mellan myndigheter. En påtaglig del av de myndigheter vars representanter vi träffat under kartläggningen undersöker möjligheten att öka graden av automation vid ärendehandläggning och beslutsfattande. Bland aktörer som strävar mot detta återfinns myndigheter som redan har automatiserat vissa ärendeprocesser och beslutsfattande, och som nu överväger om detsamma är möjligt också inom andra områden. Möjligheterna undersöks emellertid också hos myndigheter som hittills inte har använt den automatiserade beslutsformen. Någon har lyft fram för oss att det här finns förutsättningar för effektivitetssprång i förvaltningen.

I kapitel 5.3.4 har vi resonerat kring några av de frågor som framkommit under kartläggningen avseende formkrav på underteckning etc. Den typen av formkrav är emellertid långt i från de enda rättsligt reglerade kraven på viss form för informationshantering. Kartläggningsresultatet visar på ett bredare behov av att anpassa rättsregler som styr formerna för informationshantering vid kommunikation och ärendehandläggning. Det kan röra sig om att regleringen av processen för hur information ska hanteras hindrar fullt tillvaratagande av digitaliseringens möjligheter.

Nedan lämnas ett axplock av de exempel på krav på viss form för att hantera information i en ärendeprocess som vi har fått presenterade för oss under kartläggningen.

[30] Europaparlamentets och rådets direktiv 2007/2/EG av den 14 mars 2007 om upprättande av en infrastruktur för rumslig information i Europeiska gemenskapen (Inspire).

Exempel: Begäran om viss komplettering av en årsredovisning ska enligt årsredovisningslagen[31] skickas till en registrerad postadress. För att Bolagsverket ska kunna digitalisera processen krävs en lagändring.

Exempel: Miljölagstiftningen innehåller regler som utgår från pappersförfaranden. Som exempel kan nämnas bestämmelser om att rekommenderade brev ska användas för en viss försändelse, att en viss informationsmängd ska kungöras i ortstidningar eller att domar ska publiceras på ett visst ställe. Det är ett lappverk av regler som sammantaget är svårt överblicka och hantera i strävan efter en digital förvaltning.

Exempel: I socialförsäkringsbalken finns regler om *anmälan* respektive *ansökan* för t.ex. föräldrapenning. Det härrör från en tid då informationen hanterades i två steg. I den digitala informationshanteringen behövs egentligen inte två olika förfaranden utan det räcker med enbart ansökan. Reglerna som träffar anmälningsförfarandet har helt enkelt blivit överflödiga.

Exempel: Lagstiftningen kring kravet på att certifikat och andra tillståndshandlingar i original ska medföras på fartyg och luftfartyg hindrar en övergång till en helt digital ärendehantering. Även i EU-lagstiftning och andra internationella rättsakter finns framtagna mallar för ansökan och certifikat. Mallarna innehåller krav på underskrifter och fysiska stämplar vilket hindrar en övergång till en helt digital ärendehantering.

Exempel: Inom fastighetsinskrivning är Lantmäteriets mål att ärenden om fastighetsöverlåtelser, upplåtelseavtal och pantbrev ska hanteras i en helt digitaliserad process. Dessa ärendetyper är dock hårt formbundna i jordabalken och utgår från en pappershantering. Det finns även flera olika rättsinstitut, t.ex. bestyrkande, som måste kunna överföras från analoga till digitala förfaranden. Lantmäteriets hantering är av stor betydelse för samhällsutvecklingen i övrigt. En analog hantering hos Lantmäteriet förhindrar digitalisering hos andra aktörer.

5.6.2 Digitala handlingar

Det har framkommit att myndigheter gör olika bedömningar av hur det är möjligt att hantera digitala handlingar. Det generella önskemålet är dock att slippa hantera pappershandlingar. Men under vilka förutsättningar är det möjligt att enbart hantera en handling digitalt? Kan en digital handling vara säkrare och svårare att förfalska än ett pappersdokument? En annan fråga som lyfts fram är om det är nödvändigt att bevara fysiska handlingar när handlingarna har skannats

[31] Årsredovisningslagen (1995:1554).

in och finns i digital version. Kan den fysiska handlingen gallras eller finns det risk för att handlingens autenticitet i ett senare skede inte går att fastställa?[32]

Exempel: Sedan slutet av 1990-talet rapporteras alla slutbetyg in digitalt. Kommuner kan dock fortfarande välja om de vill arkivera betygskatalogen analogt eller digitalt.

5.6.3 Automation av ärendehandläggning och beslutsfattande

Förutsättningarna för automatiserat beslutsfattande har förtydligats genom ny reglering i förvaltningslagen.[33] Men hur långt är det möjligt att gå i fråga om automatiserat beslutsfattande? Och utgör särreglering i andra författningar om automatiserade beslut ett hinder för de myndigheter som har att tillämpa dessa specialförfattningar att automatisera andra beslut än dem som medges där?

Under kartläggningsarbetet har några framhållit att en förutsättning för att myndigheter i ökad utsträckning ska kunna digitalisera sina beslutsprocesser, i alla fall med nu kända medel, är att författningstext kan översättas till algoritmer.[34] Vidare har reflektioner gjorts och frågor ställts som rör säkerställande av beslutsunderlag, t.ex. om det rör sig om stora underlag såsom informationssamlingar med sensordata.

Såväl rättsliga hinder i gällande rätt som oklara rättsförhållanden har vidare beskrivits kunna hindra eller hämma en utveckling mot en ökad grad av automation i en digital förvaltning. Under kartläggningen har också ett antal frågor och reflektioner framkommit som på en övergripande nivå kan sägas utgöra en rättslig osäkerhet avseende på vilka sätt den allt mer digitala förvaltningen ska gå tillväga för att säkerställa att förfaranden både är, och kan visas vara, rättssäkra.

Exempel: En kommun använder ett automatiserat förfarande för skolplaceringar. I det fria skolvalet beaktas bl.a. närhetsprincipen. Närhetsprincipen är som sådan inte exakt utan bara en vag princip. Det behöver fastställas var den geografiska punkten för skolan ska förläggas. Är det i matsalen, rektors kontor eller på skolans parkeringsplats? Valet av

[32] Riksarkivet kan i sina myndighetsspecifika föreskrifter (RA-MS) reglera statliga myndigheters möjligheter att gallra en fysisk handling som har skannats in.
[33] 28 § förvaltningslagen.
[34] En algoritm är enligt en klassisk definition en noggrann plan eller metod för att stegvis göra något.

geografisk markering för skolans belägenhet kan få en avgörande betydelse i förhållande till vilken elev som därefter bedöms ha närmast till skolan. Ett urval baserat på närhetsprincipen måste vidare baseras på ett kartunderlag. Men vilket?

Kartläggningsresultatet visar även på osäkerhet om vilka rättsliga förutsättningar som finns när det gäller en övergång till förfaranden där stora datamängder används i förening med artificiell intelligens och anknytande maskininlärda algoritmer.[35] Dessa frågor gör sig också, och i kanske än högre grad, gällande i ett kunskapsperspektiv. Hur kan man göra det möjligt att nyttja förvaltningens informationsmängder för att med hjälp av ny teknik nå ökad kunskap?

Det är vidare inte bara lagtext som behöver översättas till algoritmer för att digitala processer ska kunna utnyttjas. Även den fysiska världen behöver ibland få en digital motsvarighet som enskilda sätter tillit till och som är rättsligt accepterad.

Exempel: Lantmäteriet har utrett förutsättningarna för ett nytt regelsystem för fastighetsgränser där i första hand koordinater bestämmer gränspunkternas läge.[36] I arbetet har bl.a. följande frågor ställts på sin spets. Hur kan samhället gå över till ett system där digital information, t.ex. koordinater över en fastighet, i stället för analog information, t.ex. fysiska gränsmärken, utgör rättsfigurer eller handlingar som medför rättsverkan? Hur kan det säkerställas att rättigheter, t.ex. äganderätten, och skyldigheter som baseras på det hittillsvarande analoga systemet inte inkräktas på? Digitala fastighetsgränser som fastställs med koordinater kommer inte bli identiska med de nuvarande fastighetsgränserna. Men förtroendet för det digitala systemet behöver vara lika stort som för det befintliga analoga systemet.

Inom ramen för kartläggningsarbetet framhåller flera av dem vi träffat att handläggning med helt eller delvis stöd av automatiserade processer många gånger är mer rättssäker än motsvarande manuell handläggning, åtminstone när beslutsunderlaget utgörs av ”hårda fakta” där bedömningsutrymme saknas eller är litet. När man ser till helheten av de beslut som i dag fattas automatiserat beskrivs detta normalt leda till en mer rättssäker hantering.

Exempel: När Skatteverket tidigare masshanterade deklarationer i pappersformat kontrollerades maskinellt att blanketterna var undertecknade. Det fanns emellertid inga maskinella funktioner för att kontrollera att det var rätt individ som hade undertecknat deklarationen i fråga. I dag

[35] Se kapitel 7.3.2 för förklaring av begreppen.
[36] Lantmäteriets rapport *Koordinatbestämda gränser*, 27 mars 2017, dnr 508-2017/939.

deklarerar större delen av befolkningen digitalt vilket innebär att det med en hög grad av säkerhet kan fastställas att det är rätt person som har undertecknat deklarationen i fråga eftersom undertecknandet sker med stöd av en tvåstegsautentisering t.ex. e-legitimation.

Men hur blir det om automatiserade förfaranden ska börja tillämpas på ärendeprocesser som inte enbart utgår från t.ex. sifferberäkningar? Under kartläggningen har vi också fått veta att Försäkringskassan har påbörjat en utredning av vilka möjligheter som finns att, med bibehållen eller ökad rättssäkerhet, göra mer avancerade bedömningar med stöd av automatiserade förfaranden. Vilka risker för rättsosäkerhet kan uppstå och hur kan de hanteras? Standardisering av individärenden får t.ex. inte leda till att vissa grupper diskrimineras.

Exempel: Inom sjukförsäkringen är bedömningsutrymmet större än i de processer som Försäkringskassan hittills har automatiserat t.ex. beslutsprocesser för föräldrapenning och tandvård. Försäkringskassan har drivit ett utvecklingsarbete med utgångspunkten att hitta ärenden där risken för längre sjukskrivning statistiskt sett är låg och där automatiserade processer inte skulle leda till ett annat utfall än vid en manuell handläggning. Detta skulle möjliggöra en förflyttning av handläggare till ärenden där manuell handläggning skapar mer värde. Under utvecklingsarbetet gjorde dock Försäkringskassan det juridiska ställningstagandet att vissa moment i ärendeprocessen som bedömning av arbetsförmåga, kräver manuell handläggning.

Vi har också under kartläggningen fått höra ett par exempel på när det varit svårt att uppmärksamma och utreda fel i bakomliggande tekniska förfaranden. Hur säkerställs att de upptäcks, och vem bär ansvaret för den typen av fel och för dess följder?

5.7 Automation av faktiskt handlande

En annan form av digitalisering som ökar i den offentliga förvaltningen är automatisering av uppgifter som hittills skötts av människor och som inte utförs inom ramen för förvaltningens ärenden eller ärendehandläggning. Ett exempel som har lyfts fram under kartläggningsarbetet är användningen av digitala trygghetstekniker i bl.a. socialtjänstens verksamhet. Digitala trygghetstekniker (även kallat välfärdsteknik) är t.ex. kameror och sensorer som används för tillsyn i stället för att vårdpersonal är fysiskt på plats för att se till

vårdtagaren. Det kan röra sig om nattlig tillsyn via kamera eller sensorer som larmar när en blöja behöver bytas.

I kartläggningsarbetet har aktörer med koppling till vård- och omsorgssektorn pekat på behovet av en ändamålsenlig reglering för att skapa bättre förutsättningar för användning av digitala trygghetstekniker. Att det saknas särskild reglering om användandet av dessa tekniker medför bl.a. att det i allmänhet krävs att vårdtagaren samtycker till den behandling av personuppgifter som äger rum. I praktiken är det dock inte alltid möjligt att inhämta den enskildes samtycke. Exempelvis har inte alla vårdtagare beslutsförmåga, t.ex. till följd av demenssjukdom.

5.8 Öppenhet i den digitala förvaltningen

5.8.1 Dokumentation

En förutsättning för att upprätthålla öppenheten i den digitala förvaltningen är att det finns dokumentation av vilka informationstillgångar och/eller it-system som finns.[37] Utan en sådan god offentlighetsstruktur är det inte möjligt för allmänheten att veta vilken information som finns tillgänglig hos myndigheterna och som kan begäras ut. Dokumentation är också av stor vikt inte minst när det gäller frågor om i vilken utsträckning myndigheter ska eller kan tillhandahålla öppna data eller öppen källkod. Under kartläggningsarbetet har det framkommit att kunskapen om författningsreglerade dokumentationskrav kan stärkas. Det gäller särskilt i frågor som rör utveckling av, eller ändringar i, de it-system som används.

5.8.2 Öppna data

Med öppna data menas all information som uppfyller kraven för s.k. öppen kunskap, dvs. information som tillhandahålls fritt utan krav på avgifter och med få eller inga tekniska eller rättsliga begränsningar för hur den får användas.[38] Skillnaden mellan öppna data och Public Sector Information (PSI) som utgångspunkt för vidareutnyttjande

[37] Se vidare kapitel 7.6 i fråga om vissa dokumentationskrav.
[38] Se www.vidareutnyttjande.se/om-vagledningen/terminologi/

av handlingar från den offentliga förvaltningen är långt i från självklar.[39] Det kan med andra ord skönjas en viss otydlighet vad gäller förhållandet mellan de skyldigheter som regleras av PSI-direktivet[40] och lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen jämfört med den frivilliga möjligheten att publicera öppna data.

Att det inte finns någon särskild författning som styr publiceringen av öppna data har vi också under kartläggningen uppfattat leda till osäkerhet. Vad är öppna data i förhållande till den rättsliga regleringen? Vilka uppgifter bör publiceras som öppna data och hur? Under kartläggningen har vi i något sammanhang uppfattat att frivillig publicering av öppna data inte varit prioriterat när nyttan med sådan publicering främst uppstår utanför den egna verksamheten. Samtidigt framhålls att det finns potentiell nytta även för myndigheter att ta del av andra myndigheters öppna data. Någon har framfört behov av att explicit reglera skyldigheter att tillhandahålla öppna data.

Representanter för myndigheter som är i färd med att börja eller som redan har börjat publicera öppna data vittnar om att det kan vara besvärligt att avgöra vilken slags information som kan publiceras som öppna data. Varje myndighet ansvarar för sina bedömningar och informationssäkerhets-, dataskydds- och sekretessfrågor måste beaktas såväl ur ett individ- som ur ett samhällsperspektiv. Det finns en oro över att uppgifter som en myndighet publicerar på aggregerad nivå ska kunna återskapas till personuppgifter om de kombineras med uppgifter som t.ex. har hämtats från en annan källa, eller att något säkerhetsrelaterat hot kan uppstå som en enskild myndighet inte har överblick över. Ett par aktörer har därför uppmärksammat behovet av en central aktör som har överblick över samtliga öppna data som publiceras av myndigheterna. Någon annan har pekat på att myndigheterna också måste beakta eventuella verksamhetsrisker som kan uppstå till följd av publicering av öppna data som rör verksamheten. Det har emellertid också poängterats att publicering av öppna data i de rekommenderade standarder som finns möjliggör för privata näringslivet att utveckla tjänster och bygga nya lösningar

[39] Riksarkivet beskriver på webbplatsen www.oppnadata.se hur de olika begreppen skiljer sig åt.
[40] Europaparlamentets och rådets direktiv 2003/98/EG av den 17 november 2003 om vidareutnyttjande av information från den offentliga sektorn.

som kan komma till nytta hos myndigheterna. I förlängningen kan myndigheterna dra nytta av det privata näringslivets innovationer.

Vissa myndigheter, t.ex. Bolagsverket och Lantmäteriet, är skyldiga att ta ut avgifter för sin information. Ett sådant avgiftskrav kan inte kombineras med ett tillhandahållande av öppna data som per definition ska ske avgiftsfritt. Avgiftsfinansieringen beskrivs vara hämmande.

> Exempel: Lantmäteriet har publicerat en liten mängd s.k. geodata som öppna data, motsvarande cirka 2 procent av avgiftsintäkterna. Innan publiceringen gjordes cirka 8 000 nedladdningar av denna datamängd under en kalendermånad. När avgifter inte längre togs ut ökade siffran till över 40 000 nedladdningar på en kalendermånad. Intresset av myndighetens uppgifter som öppna data har alltså varit stort.

Ett annat rättsområde som i något fall kan inbegripa hinder mot publicering av öppna data är immaterialrätten. Företrädare för Lantmäteriet har påpekat att geodata, bl.a. kartor, skyddas av upphovsrätt. Skyddsintresset är emellertid enbart myndighetens ekonomiska rättighet. Om avgiftskravet skulle slopas skulle det inte heller finnas hinder i immaterialrätten för publicering som öppna data. Om avgiftskravet behålls kan informationen inte publiceras som öppna data eftersom den inte får vidareutnyttjas gratis.

I samarbeten om öppna data mellan myndigheter och/eller andra aktörer kan vidare nya informationsmängder uppstå, s.k. auktoritetslistor. En sådan lista skapas för att hålla samman uppgifter som rör samma ämne, händelse eller annat och som hämtas från olika aktörer, dvs. för att hålla samman s.k. distribuerade data. Det kan vara oklart vem som är ansvarig för den nya informationsmängden i en sådan lista och var den ska förvaltas och bilda arkiv.

5.8.3 Elektroniskt utlämnande av allmän handling

I ett digitaliserat samhälle förväntar sig enskilda att få allmänna handlingar utlämnande digitalt. Vi har under kartläggningen uppfattat att det finns pedagogiska svårigheter med att förklara för enskilda som önskar använda e-post för att ta emot de efterfrågade handlingarna varför en myndighet inte lämnar ut handlingar digitalt, eller varför vissa handlingar lämnas ut digitalt men inte andra. Det har framförts att enskilda ibland i onödan och oriktigt har uppfattat

det som att en myndighet försöker dölja något när vissa handlingar bara lämnas ut på papper och inte i den digitala form som har begärts. Utöver de handlingar som har lämnats ut på papper begärs då ytterligare handlingar ut avseende digitala spår, t.ex. loggar och cookiefiler.

Det har vidare beskrivits för oss att det inte alltid är enkelt att avgöra vad som utgör en handling och när den är allmän i dagens digitala informationsflöden och behandling av stora mängder data. Bedömningen kan innebära komplicerade avvägningar i det dagliga arbetet. Ibland rör det sig om begäranden om utlämnande av allmän handling som omfattar stora informationsmängder och mycket arbetstid läggs vid myndigheterna på att beräkna kostnader för utlämnanden. Det förekommer också att begärandena inte fullföljs när det står klart vad kostnaderna blir.

Exempel: På en myndighet ägnades två veckor åt att rensa cookiefiler från uppgifter som inte skulle lämnas ut. Totalt sett rörde det sig om ca 60 000 sidor med uppgifter. Den som begärt ut uppgifterna hämtade sedan aldrig handlingarna.

5.9 Rensning, arkivering, gallring och bevarande

Digital informationshantering ger förutsättningar att samla in och lagra stora mängder information. I digitala miljöer betraktas inte arkivet som en slutdestination för information. Snarare uppkommer frågor om vilka uppgifter som genast kan rensas, vilka uppgifter som ska lagras, var de ska lagras och hur länge de ska bevaras. När data i realtid samlas in genom t.ex. sensorer kan det innebära att informationsmängden hela tiden förändras. Vad gäller då om informationsmängden ska användas som beslutsunderlag? Är myndigheten skyldig att för varje enskilt beslut lagra all den data som har samlats in eller räcker det att lagra informationsmängden på ett ställe med fastställda intervall? Är det verkligen relevant att tillämpa arkivlagens krav på alla de informationsmängder som kommer att skapas i den digitala förvaltningen?

I vårt kartläggningsarbete har det framkommit att arkivfrågorna, trots dess centrala betydelse inte minst för bibehållen öppenhet i förvaltningen, har en viss tendens att hamna i skymundan vid utvecklingsarbeten. Men frågor om rensning, arkivering, gallring eller bevarande av uppgifter i myndighetsgemensamma system kan

innebära särskilda svårigheter som måste redas ut. Företrädare för Riksarkivet framhåller att det är av stor vikt att fastställa arkivansvaret, inte minst för att veta vilken aktör som är arkivbildande myndighet. Det blir både kostsamt och ineffektivt att behöva utreda frågan om arkivansvar i efterhand, när det blir aktuellt att arkivera, för att senare gallra eller bevara.

Utgångspunkten vid fastställande av arkivansvar när flera myndigheter har åtkomst till en viss informationsmängd genom antingen läs- eller skrivbehörighet är att arkivansvaret ska placeras hos den myndighet som har skrivbehörighet. Under kartläggningen har vi emellertid fått beskrivet att det i dagens digitala miljöer inte längre är relevant att enbart tala om läs- och skrivbehörigheter. Den digitala informationshanteringen är betydligt mer komplex än så. Det har vidare framförts att det ibland krävs tid för att få till stånd en ny informationshantering som också är långsiktigt hållbar.

Företrädare för Riksarkivet har också pekat på vikten av att databaser hålls samman ur arkivsynpunkt. Nyttan av att bevara sammanhållna databaser är bl.a. att det ger överlägsna möjligheter att bedöma handlingars autenticitet och att söka och sammanställa uppgifter och handlingar. Även andra har framhållit riskerna med att fragmentera informationen vid arkivering genom att dela upp och gallra uppgifter efter olika myndigheters reglering. En sådan fragmentering leder till att det inte går att säkerställa kontinuitet och att informationen kan användas på samma sätt som i den gemensamma databasen efter arkivering. Det kan göra att det i efterhand kan vara komplicerat att avgöra vilken information som har legat till grund för ett beslut.

Särskilt från arkivarier har det framförts att det behövs en generell lagstiftning som styr informationshanteringen i en digital riktning för offentlig sektor. Det behövs med andra ord en gemensam riktning så att inte alla sitter med olika lösningar i olika utvecklingsarbeten. I nuläget är de krav som finns för informationshanteringen splittrade i olika regelverk. Exempelvis är gallringsbesluten starkt kopplade till myndigheternas organisation. En representant för en myndighet som använder ett it-system som är gemensamt med andra har beskrivit att gallringsbesluten hos de olika myndigheterna ser olika ut. Bedömningen av om en handling ska bevaras eller om den kan gallras görs nämligen bl.a. i förhållande till sitt sammanhang hos respektive myndighet. Det har emellertid framförts i kartläggningen

att när det saknas samordning av myndigheternas bevarande- och gallringsrutiner kan det leda till att information sparas på flera håll eller inte alls.

När myndigheter utkontrakterar sin informationshantering har vi vidare fått beskrivet för oss att det behöver finnas garantier för att systemleverantörerna verkligen utplånar uppgifterna ur systemen när de har fått i uppdrag att gallra. Men är det tekniskt möjligt att gallra uppgifter i molntjänster[41] med omedelbar verkan? Eller ska radering av en uppgift i molnet snarast ses som en markering om radering med följd att uppgiften skrivs över med ny information över tid?

Även utmaningar rörande förhållandet mellan arkivreglering och dataskyddsreglering har beskrivits för oss. Dataskyddsregleringens princip om lagringsminimering innebär att personuppgifter inte ska bevaras under längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.[42] I regel beskrivs det dock inte vara praktiskt möjligt att enbart gallra en eller ett fåtal uppgifter i ett system utan att det påverkar den kvarvarande informationsmängden på ett eller annat sätt. Av denna anledning är det angeläget att redan innan uppgifter samlas in ta ställning till om det finns ett relevant behov av dessa eller inte.

5.10 Upphandling, utkontraktering och avtal

5.10.1 Regelverk och teknisk utveckling

Under kartläggningsarbetet har flera aktörer framhållit att myndigheter i varierad grad har behov av att utkontraktera it-drift eller andra it-baserade funktioner till privata leverantörer. Representanter för myndigheter som utkontrakterar it-drift eller andra it-baserade funktioner till privata leverantörer framhåller dels att det är svårt att genomföra upphandlingar där den levererade tjänsten faktiskt motsvarar myndighetens behov, dels att avtalshanteringen är komplicerad.

[41] Molntjänster är tjänster som tillhandahålls med nätverksåtkomst och där resursdelning, möjlighet till snabb skalbarhet, självbetjäning och betalning efter användning eller volym är några av de centrala kännetecknen, se Pensionsmyndighetens rapport *Molntjänster i staten, en ny generation av outsourcing*, januari 2016, s. 9.
[42] Artikel 5.1. e dataskyddsförordningen.

Flera har uttalat att upphandlingsreglerna är komplicerade och att det är en utmaning att åstadkomma nödvändig flexibilitet vid upphandling av varor och tjänster relaterade till myndigheternas digitalisering. Ett mindre lyckat upphandlingsresultat kan leda till att verksamheten under flera år får en produkt eller tjänst som inte svarar mot verksamhetens behov. Problemet är bl.a. att det kan vara komplicerat att få till stånd en kravspecifikation som svarar mot myndighetens behov.

Vi har också fått förklarat för oss att det förekommer att leverantörer inte alltid är intresserade av att delta i de upphandlingsformer som kanske lämpar sig bäst för upphandling av it, nämligen konkurrenspräglad dialog och förhandlat förfarande. För leverantörerna kan de upphandlingsformerna innebära tidsödande arbete som inte alltid leder till något konkret och affärsmässigt resultat.

Någon aktör har särskilt pekat på att den snabba tekniska utvecklingen innebär särskilda utmaningar i upphandlingsarbetet. Myndigheters utvecklingsarbete bedrivs ofta i agila processer[43] och för att matcha sådana processer i upphandlingen behöver också upphandlingsprocessen kunna arbeta mot ett rörligt mål.

> Exempel: En innovationsupphandling görs vanligen i flera steg, t.ex. utredning, förstudie, utveckling och implementation. Eftersom myndigheten inte vet hur slutprodukten kommer att se ut är det i princip omöjligt att från början kravställa för hela kedjan. Upphandlingen sker i stället stegvis vilket innebär att den upphandlande myndigheten kan behöva byta leverantör mitt i innovationsprocessen och börja om på nytt med en ny leverantör. Bristande kontinuitet i leverantörsledet beskrivs hämma den digitala utvecklingen.

Utöver myndigheters skyldighet att efterleva upphandlingsreglerna ska myndigheterna se till att följa annan lagstiftning som reglerar myndighetens informationshantering. Om utkontrakteringen innebär att sekretessbelagda uppgifter kommer att lämnas ut till leverantören måste utlämnandet vara tillåtet enligt offentlighets- och sekretesslagen. Rör det sig om uppgifter som omfattas av sekretess och som rör rikets säkerhet gäller också kraven i säkerhetsskyddslagen.[44] Om informationsmängden som lämnas ut till leverantören inne-

[43] Se vidare kapitel 7.4.2 om begreppet ”agil”.
[44] Säkerhetsskyddslagen (1996:627). En ny säkerhetsskyddslag har föreslagits träda i kraft den 1 april 2019, se *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag*, prop. 2017/18:89.

håller personuppgifter måste myndigheten även säkerställa att regelverket kring dataskydd efterlevs. Består den utlämnade informationsmängden av allmänna handlingar behöver myndigheten kontrollera att det finns förutsättningar att uppfylla regleringen kring bevarande och gallring.

Under kartläggningsarbetet har vi förstått att myndigheter inte alla gånger anser sig själva besitta all den kompetens och den förmåga som krävs för att genomföra upphandling av it som svarar mot samtliga dessa rättsliga krav, och därtill de rättsliga krav som kan följa av andra regelverk som gäller för en myndighets verksamhet. Vi har särskilt uppfattat att små och medelstora myndigheter vill ha mer stöd. De samlade reglerna som ska följas är omfattande och kan ibland vara svåra att tolka och tillämpa. Om en myndighet missar att spegla samtliga relevanta rättsliga bestämmelser i sin kravställning kan det leda till att myndigheten i ett senare skede inte efterlever regelverket om informationen inte skyddas av leverantören på det sätt som krävs.

Vid samverkan mellan myndigheter som innebär att en myndighet utför arbete på uppdrag av en annan myndighet, dvs. som en form av utkontraktering, kan det så som kartläggningsarbetet visar, vidare uppstå osäkerhet i fråga om gränserna om när upphandlingslagstiftningen i stället ska tillämpas.

5.10.2 Sekretess och tystnadsplikt

Kartläggningsarbetet har visat att flera myndigheter, och andra aktörer, upplever osäkerhet om det i vissa situationer finns rättsligt stöd i sekretesslagstiftningen för att lämna ut uppgifter som omfattas av sekretess vid utkontraktering till privata leverantörer.

Flera myndighetsrepresentanter har beskrivit för oss att det finns en tvekan kring hur röjandebegreppet i sekretesslagstiftningen ska tolkas. Kan myndigheten lämna ut sekretessbelagda uppgifter utan att uppgifterna röjs för leverantören, genom att ställa upp avtalsvillkor som förhindrar leverantörens personal att ta del av myndighetens information?[45] Finns det lagringstjänster där leverantören inte behöver ta del av myndighetens sekretessreglerade uppgifter?

[45] Jfr *Outsourcing – en vägledning om sekretess och persondataskydd*, s. 16 f., eSam, januari 2016.

Eller behöver det mer eller mindre alltid finnas möjligheter för leverantörens personal att ta del av myndighetens uppgifter för att felsöka, korrigera felaktigheter eller ge annan support?

Under kartläggningen har det även framförts osäkerhet om hur den sekretessbrytande bestämmelsen i 10 kap. 2 § offentlighets- och sekretesslagen om nödvändigt utlämnande ska tolkas och i vilken utsträckning sekretessbelagda uppgifter kan lämnas ut med stöd av bestämmelsen i den situation som nu avses. Det har även framkommit att osäkerheten kring de rättsliga förutsättningarna för att utkontraktera it-drift eller andra it-baserade funktioner har lett till att myndigheter har avstått från att utkontraktera till privata leverantörer. I något fall har myndigheten i stället infört separata manuella rutiner för intern hantering av ett fåtal sekretessreglerade uppgifter i en större informationsmängd som i övrigt hanteras digitalt av en privat leverantör.

Frågor om förhållandet mellan den nya dataskyddsförordningen och nationella tystnadsplikter har också lyfts fram för oss under kartläggningsarbetet, särskilt vad gäller vård- och omsorgssektorn. Kartläggningen visar vidare att myndigheter hanterar sekretessproblematiken på olika sätt. Vissa myndigheter har beslutat att tills vidare inte anlita molntjänstleverantörer för informationshantering. Andra myndigheter menar att utlämnandet av sekretessbelagda uppgifter i vissa fall av utkontraktering till privata leverantörer är nödvändigt och därför omfattas av den sekretessbrytande regeln i 10 kap. 2 § offentlighets- och sekretesslagen. Flera myndigheter har påpekat att de generellt är tveksamma till att anlita privata leverantörer om det inte står klart att offentlighets- och sekretesslagen inte hindrar ett utlämnande av de uppgifter som ska hanteras av leverantören. Därtill menar flera att det finns behov av antingen ett vägledande uttalande i frågan eller en förtydligande reglering.

5.10.3 It-avtal

Flera av de myndighetsrepresentanter vi träffat anser att avtalsarbetet vid köp av it är resurskrävande och fordrar att avtalsansvariga tjänstemän har bred och hög kompetens. De menar att det är svårt att upprätta avtal som är väl avvägda och juridiskt hållbara ur alla aspekter. Avtalsinnehållet ska spegla de juridiska krav myndigheten

har att uppfylla men behöver också vara affärsmässigt gynnsamt. Myndigheten vill t.ex. kunna tillgodogöra sig den tekniska utvecklingen som sker under avtalets löptid. Har en myndighet inte tillräcklig kompetens eller resurser för att teckna ändamålsenliga och balanserade avtal kan det leda till att leverantören intar ett överläge, vilket kan resultera i att myndigheten ingår ett ofördelaktigt avtal som kan få ekonomiskt kännbara konsekvenser i ett senare skede.

Vi har fått förklarat för oss att det finns utmaningar i att formulera förutsebara avtalsvillkor, t.ex. sådana som leder till att det inte uppstår s.k. inlåsningseffekter. Det kan exempelvis vara komplicerat att utforma tydliga avtalsvillkor som ålägger leverantören att samarbeta vid ett framtida leverantörsbyte.

> Exempel: Om det saknas avtalsvillkor som förbinder leverantören att samarbeta vid ett framtida leverantörsbyte eller att överföra myndighetens information i ett användbart format vid avtalets upphörande kan det leda till svårigheter när myndigheten vill byta leverantör.

5.10.4 Personuppgiftsbiträdesavtal

När en myndighet uppdrar åt en extern leverantör att hantera myndighetens information blir leverantören ett personuppgiftsbiträde[46] åt myndigheten om informationen i fråga innehåller personuppgifter.[47] Dataskyddsförordningen ställer höga krav på transparens, insyn och kontroll när en behandling av personuppgifter överlämnas till ett personuppgiftsbiträde. Samtidigt kan vissa leverantörers driftsmodeller vara påfallande komplicerade och t.ex. involvera en mängd underleverantörer,[48] vilket kan verka hindrande för myndighetens möjlighet till insyn och kontroll. Några av de aktörer vi träffat påtalar att dataskyddsregleringens långtgående krav blir svåra att applicera på verkliga förhållanden.

Flera aktörer som har deltagit i kartläggningsarbetet upplever osäkerhet när det gäller personuppgiftsbiträdesavtal som tecknas med privata leverantörer. Det gäller särskilt när avtal ska tecknas

[46] Ett personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning, artikel 4.8 dataskyddsförordningen.
[47] Personuppgifter är varje upplysning som avser en identifierad eller identifierbar person, artikel 4.1 dataskyddsförordningen.
[48] Underleverantörer som behandlar personuppgifter som omfattas av den personuppgiftsansvariges ansvar är också personuppgiftsbiträden till den personuppgiftsansvarige. I det följande benämns de dock enbart som underleverantörer.

med en molntjänstleverantör. Hur säkerställs att myndigheten får kännedom om samtliga underleverantörer som kan komma att behandla personuppgifter åt myndigheten? Och hur säkerställs att underleverantörerna blir bundna av samma avtalsvillkor som stipuleras i personuppgiftsbiträdesavtalet? Hur ska myndigheten utöva kontroll över sina personuppgiftsbiträdens (leverantörens och alla underleverantörers) behandling av personuppgifter?

En generell uppfattning är att oproportionerligt mycket tid läggs ned på att utforma och förvalta personuppgiftsbiträdesavtal. Flera aktörer som har deltagit i kartläggningsarbetet menar att avtalshanteringen i högre utsträckning borde gå att standardisera om den alls ska vara nödvändig när offentliga aktörer biträder varandra. I myndighetssamarbeten är det vanligt att en myndighet agerar i rollen som personuppgiftsbiträde åt en annan myndighet. Ett sådant exempel är informationsöverföringstjänsten SSBTEK.[49] Inom ramen för den tjänsten har vi fått förklarat att de involverade aktörerna initialt bedömde att om samtliga aktörer skulle teckna separata personuppgiftsbiträdesavtal sinsemellan skulle antalet biträdesavtal komma att uppgå till över 800 stycken. En sådan omfattande avtalshantering ansågs vara orealistisk och inte medföra något mervärde varför en annan modell för avtalstecknande valdes som begränsade antalet separata personuppgiftsbiträdesavtal.

Vid användning av förvaltningsgemensamma tjänster är det inte ovanligt att det är personuppgiftsbiträdet, som också kan vara den part som utvecklar och förvaltar tjänsten i fråga, som utformar personuppgiftsbiträdesavtalen.

> Exempel: Inera AB[50] tillhandahåller tjänster till bl.a. hälso- och sjukvården. I dessa sammanhang agerar bolaget i rollen som personuppgiftsbiträde och respektive vårdgivare är personuppgiftsansvarig. Inera AB anlitar dessutom underleverantörer som i sin tur blir personuppgiftsbiträden till de personuppgiftsansvariga vårdgivarna. För att reglera personuppgiftsbehandlingen för alla inblandade parter har Inera AB tagit fram tre olika modeller av personuppgiftsbiträdesavtal. Ett avtal som tecknas mellan vårdgivaren som personuppgiftsansvarig och Inera AB som personuppgiftsbiträde. Ett annat avtal där landsting agerar personuppgiftsbiträde åt en personuppgiftsansvarig privat vårdgivare. Och

[49] Se vidare om SSBTEK i kapitel 5.11.5.

[50] Inera AB är ett bolag som ägs gemensamt av SKL företag AB och av landsting, regioner och kommuner. Ineras uppdrag är att utveckla gemensamma lösningar som bidrar till att effektivisera verksamheter t.ex. genom att tillhandahålla kvalitetssäkrade digitala tjänster, koordinering av digital utveckling och kompetens inom interoperabilitet.

slutligen ett tredje avtal som tecknas mellan Inera AB som personuppgiftsbiträde och privata leverantörer som underleverantörer. Avtalen mellan Inera AB och dess underleverantörer förhandlas fram var för sig, dvs. avtalen kan skilja sig åt innehållsmässigt med respektive avtalspart. Därtill tecknar Inera AB också separata ”kundavtal” med respektive vårdgivare. Att förhandla fram och förvalta samtliga dessa avtal är en mycket tidskrävande uppgift.

Även inom skolområdet finns frågor kring hur personuppgiftsbiträdesavtal ska hanteras. Hur ska varje skolhuvudman rimligen kunna säkerställa att det finns acceptabla personuppgiftsbiträdesavtal på plats för applikationer med digitala läromedel som laddas ned till elevernas mobila enheter? Dataskyddsförordningen ställer höga krav på innehållet i personuppgiftsbiträdesavtal oberoende av om det endast är ett fåtal indirekta personuppgifter eller en större mängd personuppgifter som behandlas.

5.10.5 Uppföljning av avtal

För att säkerställa att leverantörer följer de avtalsvillkor som har tecknats med en myndighet behöver myndigheten följa upp leverantörens avtalsefterlevnad. På det sättet säkerställs bl.a. att myndigheten efterlever rättsliga krav även när viss verksamhet utkontrakterats. Av de kontakter vi haft med leverantörssidan i vårt utredningsarbete har vi förstått att det inte är ovanligt att myndigheter saknar särskilda rutiner för uppföljning av avtal. I de fall uppföljning sker är det inte alltid myndigheten har gjort klart vad det närmare är som ska följas upp. Uppföljningen leder i sådana fall sällan till något konkret resultat.

I dataskyddsförordningen finns särskild reglering som ska underlätta för personuppgiftsansvariga att kontrollera att deras personuppgiftsbiträden, inklusive underleverantörer, efterlever de villkor som stipuleras i personuppgiftsbiträdesavtalen.[51] I vissa sammanhang har den personuppgiftsansvariga myndigheten ganska små möjligheter att faktiskt utföra nödvändiga kontroller. Så kan vara fallet när personuppgiftsbiträdet anlitar egna underleverantörer. I en sådan situation kan det vara mer rationellt att låta personuppgiftsbiträdet kontrollera och följa upp underleverantörernas efterlevnad av avtalsvillkoren i personuppgiftsbiträdesavtalen.

[51] Artikel 28.3 h dataskyddsförordningen.

5.11 Samverkan

5.11.1 Myndigheters uppdrag

Genom kartläggningen står det klart för oss att digitaliseringen driver på behovet av samverkan. Det gäller samverkan i myndighetsgemensamma utvecklingsarbeten, samverkan vid inköp av it och andra it-baserade funktioner från privata leverantörer, samverkan som snarast är att betrakta som utkontraktering mellan myndigheter och andra former av samarbeten såväl mellan myndigheter som med det privata näringslivet.

Under kartläggningsarbetet har flera framhållit att den svenska förvaltningsmodellen med fristående myndigheter och självstyrande kommuner kan vara svår att förena med det allt ökande behovet av myndighetsöverskridande samverkan. Det är vidare inte alltid tydligt vad som utgör den yttre ramen för den verksamhet en myndighet ska ägna sig åt och det gäller i synnerhet i gränsytorna mot andra aktörer. Även i utvecklingsarbeten måste myndigheterna hålla sig innanför gränserna för sina respektive myndighetsuppdrag. Om en förstudie eller annat arbete på idéstadiet leder till att en myndighet ska utföra nya uppgifter, t.ex. ansvara för utveckling och förvaltning av en ny digital tjänst, kan myndighetens uppdrag behöva breddas.

5.11.2 Myndigheters samverkan med varandra

Flera av dem vi träffat under kartläggningsarbetet efterfrågar tydligare styrning för att effektivare nå målen i digitaliseringsarbeten. Representanter från vissa myndigheter som deltar i flera eller breda samverkansarbeten pekar på svårigheter som kan uppstå till följd av att de deltagande myndigheterna styrs från olika departement i Regeringskansliet. Ökad samordning efterfrågas. Utmaningar i samverkansarbeten kan också uppstå på grund av att en myndighet som fått en samordnande roll har givits ett otydligt mandat. Även krav på konsensusbeslut i utvecklingsarbeten kan bli en hämsko.

Myndigheters samverkan i digitaliseringsarbeten sker också på frivillig basis, utan ett särskilt uppdrag från regeringen. Ibland träffas överenskommelser mellan parterna men sådan samverkan kan också ske utan mer formliga överenskommelser. Oavsett om samverkan sker frivilligt eller till följd av t.ex. ett särskilt regeringsuppdrag kan

det vara ett resurs- och tidskrävande arbete att ta fram närmare överenskommelser som styr samverkansarbetet.

I kartläggningsarbetet har det framkommit att tolkning och tillämpning av gällande rätt ofta är en komplex och tidsödande uppgift i myndighetsgemensamma utvecklingsinsatser. De skarpa myndighetsgränserna i kombination med sektorsspecifik reglering avseende t.ex. sekretess och dataskydd medför att myndigheterna måste lösa alla rättsliga frågor var för sig innan ett myndighetssamarbete kan resultera i gemensamma digitala processer. En utmaning i varje enskilt utvecklingsarbete är att myndigheternas jurister inte sällan gör olika tolkningar och bedömningar av samma rättsliga frågor.

När samverkan mellan myndigheter innebär att en myndighet utför arbete på uppdrag av den andra, dvs. närmast en form av utkontraktering, kan det så som kartläggningsarbetet visar, uppstå osäkerhet om när upphandlingslagstiftningen i stället ska tillämpas.

Den svenska förvaltningsmodellen med kommunalt självstyre där respektive kommun ansvarar för sådana angelägenheter som har anknytning till kommunens område eller dess medlemmar (lokaliseringsprincipen) kan också verka hindrande för digitala samverkansarbeten över kommungränserna. I dagsläget sker kommunala samarbeten i regel genom att en ny gemensam nämnd eller ett kommunalförbund inrättas.[52] Samarbete kan också äga rum inom ramen för gemensamt ägande, t.ex. Inera AB.

Samtidigt som önskemål om bättre förutsättningar för samverkan har förts fram under kartläggningen har det också påpekats att beslutsfattare bör vara medvetna om att digitala förfaranden som en gång har samordnats mellan flera myndigheter kan vara svåra att ändra.

> Exempel: Flera kommuner utvecklar i samverkan med varandra en gemensam plattform för en digital tjänst, t.ex. ansökan om förskoleplats. Om en av kommunerna sedan vill ändra reglerna för sin förskoleverksamhet genom att ta bort syskonförtur, kan detta vara ogörligt i den gemensamma plattformen.

[52] Se dock lagrådsremissen *En generell rätt till kommunal avtalssamverkan*, från den 22 februari 2018.

5.11.3 Myndigheters samverkan med privata aktörer

Kartläggningsarbetet visar att det blir allt vanligare att myndigheter samverkar med det privata näringslivet, även i andra former än vad gäller upphandling och inköp av varor och tjänster. Det kan gälla t.ex. sammankomster där myndighetsrepresentanter och representanter från privata näringslivet träffas och utvecklar kod i gemensamma plattformar (öppen källkod).

Myndigheter och privata aktörer har emellertid helt olika förutsättningar för samverkan. Myndigheternas verksamhet är regelstyrd och det gäller därför att hitta fungerande former för att samverka med det privata. I kartläggningen har vi fått höra om det arbete som läggs på att säkerställa att samverkan sker på ett konkurrensneutralt sätt och för att se till att upphandlingsreglerna inte träds för när. Även regleringen om otillåtet statsstöd har nämnts för oss i det sammanhanget som en faktor att hålla i åtanke. Myndigheterna behöver också ha kompetens och förmåga att ta fram välgrundade och genomtänkta avtal för att skydda sin verksamhet vid olika former av samverkan med det privata.

5.11.4 Arbetsro vid myndighetssamverkan

I ett utvecklingsarbete behöver ofta handlingar av den typ som internt inom en myndighet utgör arbetsmaterial delas mellan de samverkande aktörerna för att inhämta synpunkter inför fortsatt arbete. Enligt rådande rättspraxis anses det eventuella svaret med synpunkter bli en allmän handling. Det kan röra sig om utkast till rapporter, arbetsplaner eller delredovisningar som förmedlas mellan de samverkande myndigheterna eller som tas fram gemensamt. Om sådant arbetsmaterial i ofärdigt skick sprids beskrivs det kunna leda till missförstånd. Även om det inte rör sig om känslig information är arbetsutkasten inte färdigarbetade dokument. De utgör snarare arbetsmaterial på samma sätt som arbetsutkast som hittills i högre grad hanterats internt inom en myndighet och som anses utgöra arbetsmaterial och inte allmänna handlingar. Avsevärd tid läggs på att utreda hur myndigheter i samverkansarbeten ska hantera utkast och annat arbetsmaterial. Önskemål finns om att reglerna för när handlingarna blir att anse som allmänna borde vara desamma för

arbetsmaterial som hanteras i myndighetsgemensamma samverkansarbeten, som för arbetsmaterial som hanteras internt inom en myndighet.

5.11.5 Särskilda samverkansarbeten

Regeringens program Digitalt först

Digitalt först är regeringens program för digital förnyelse av det offentliga Sverige som genomförs under perioden 2015–2018. Inom ramen för programmet Digitalt först har ett antal myndigheter fått i uppdrag av regeringen att verka för digitalt först och leda digitaliseringen inom sina områden.

- Lantmäteriet, tillsammans med Boverket, har i uppdrag att utveckla en smartare samhällsbyggnadsprocess för att öka bostadsbyggandet.
- Jordbruksverket, tillsammans med Livsmedelsverket, har i uppdrag att öka tillväxten genom en smartare livsmedelskedja.
- Naturvårdsverket har i uppdrag att utveckla smartare miljöinformation för att nå miljömålen.
- SKL, tillsammans med Tillväxtverket och Bolagsverket, har i uppdrag att förenkla för restaurangföretagare genom verksamt.se.
- Tillväxtverket har i uppdrag att skapa enkla och digitala myndighetskontakter för företag.

Sammansatta bastjänster – SSBTEK och SSBTGU

Sammansatt bastjänst för ekonomiskt bistånd (SSBTEK) är en informationsöverföringstjänst som används av kommunerna vid handläggning av ärenden som rör denna form av försörjningsstöd. Genom SSBTEK kan kommuner få uppgifter utlämnande elektroniskt från Arbetslöshetskassornas samorganisation, Arbetsförmedlingen, CSN, Försäkringskassan och Pensionsmyndigheten. Åtkomsten till uppgifterna är reglerad och det är bara handläggare med ett pågående ärende som får hämta in uppgifter via tjänsten. En enskild kan alltså inte själv hämta uppgifter via SSBTEK. Tjänsten är

ett exempel på där digital utveckling i samverkan har vunnit såväl tidsbesparingar som ekonomisk framgång. I stället för att handläggare ägnar tid åt att med manuella medel samla in uppgifter kan samtliga relevanta uppgifter hämtas in sekundsnabbt. Samtidigt har kostnaden för användningen av tjänsten över tid kunnat minskas från 1 krona per invånare till 80 öre per invånare.

Sammansatt bastjänst för grunduppgifter för företag (SSBTGU) är en s.k. vidareförmedlingstjänst som hämtar uppgifter från den bästa källan (Bolagsverket, Skatteverket och Statistiska centralbyrån). Tjänsten används av den myndighetsgemensamma webbplatsen verksamt.se och av kommuner inom ramen för bl.a. Serveratprogrammet. En enskild som har skapat ett eget utrymme kan hämta in uppgifter från de anslutna myndigheterna genom fördefinierade frågor. Sammansatta svar förmedlas sekundsnabbt genom elektroniska utlämnanden. SSBTGU underlättar och förenklar ansöknings- och anmälningsförfaranden genom att enskilda kan ta del av företagsuppgifter från flera olika myndigheter och återanvända uppgifterna i andra myndigheters digitala tjänster. I denna tjänst är det i dagsläget den enskilde själv som har åtkomst till uppgifterna, medan andra myndigheter inte har det.

SSBTEK och SSBTGU är uppbyggda med samma tekniska lösning i grunden men riktar sig till olika användare och har utformats på olika sätt för att möta kraven i gällande reglering. Under kartläggningen har det framhållits för oss att det, även om tjänsterna har effektiviserat myndigheternas handläggning, finns en outnyttjad potential i tjänsterna som skulle kunna realiseras genom att öppna upp tjänsterna för nya användare och användningsområden. Om enskilda individer hade åtkomst till sina uppgifter i SSBTEK skulle de med stöd av den samlade informationen kunna avgöra om det över huvud taget är meningsfullt att ansöka om ekonomiskt bistånd. Det skulle i sin tur kunna minska arbetsbördan för kommunernas handläggare som behöver hantera färre ärenden som resulterar i avslag. Kommunerna skulle inom ramen för sin tillsynsverksamhet kunna vara betjänta av att hämta in företagsuppgifter direkt från SSBTGU. I dagsläget måste kommunerna förlita sig på att företagarna skickar in korrekta uppgifter alternativt köpa avgiftsbelagd information från den statliga myndighet som är bästa källan.

Tjänsterna SSBTEK och SSBTGU belyser hur det i och för sig varit tekniskt möjligt att utforma digitala tjänster inom ramen för

gällande lagstiftning, men där det beskrivits för oss att det finns potential för ännu större nyttor om tjänsterna vidareutvecklas. Det kan dock behövas författningsändringar.

Verksamt.se

Tillväxtverket, Bolagsverket och Skatteverket har inom ramen för ett myndighetssamarbete utvecklat tjänsten verksamt.se. Syftet med tjänsten är bl.a. att förenkla processen för enskilda att starta och driva företag. Inom ramen för verksamt.se tillhandahålls enskilda ett eget utrymme i tjänsten där de t.ex. kan skapa affärsplaner.

Den som vill använda verksamt.se för att starta ett företag dirigeras först till Bolagsverket för att i Bolagsverkets e-tjänst anmäla ett företag för registrering och få ett organisationsnummer. När Bolagsverket har fattat beslut kan den enskilde göra momsanmälan m.m. hos Skatteverket genom att logga in på nytt och dirigeras till Skatteverkets e-tjänst. Såväl sekretessregleringen som det förhållandet att varje myndighet ansvarar för sina egna informationssamlingar och bara har möjlighet att ge service inom sitt eget ansvarsområde har beaktats när tjänsten skulle utformas. Utgångspunkten i verksamt.se är att det inte ska förekomma något direkt uppgiftsutbyte mellan myndigheterna utan att den enskilde ska styra uppgiftsflödet. Inom ramen för kartläggningsarbetet har det dock uttryckts önskemål om rättsliga förutsättningar för att verksamt.se ska kunna ta ett steg vidare mot att bli en ännu bättre *hantera-ditt-företag-portal*.

En fråga som har diskuterats inom ramen för verksamt.se är vilka möjligheter det finns att närvara på sociala medier, t.ex. Facebook och Twitter. Sociala medier ger goda förutsättningar för snabb kommunikation med företagare och skulle också kunna vara ett sätt att marknadsföra tjänsten. Men eftersom verksamt.se inte är en egen juridisk person och inte agerar i rollen som personuppgiftsansvarig har bedömningen gjorts att det saknas förutsättningar att närvara på sociala medier när det inte tillräckligt tydligt framgår vilken myndighet som är avsändare.

Serverat

Inom ramen för regeringens Digitalt först-satsning driver SKL programmet Serverat tillsammans med Tillväxtverket, Bolagsverket och ett antal kommuner. Syftet med Serverat är att utveckla digitala lösningar för att förenkla för restaurangföretagare att starta och driva företag. Bolagsverkets uppdrag i programmet är att leverera företagsinformation från SSBTGU både på verksamt.se och i Serverats e-tjänster, dvs. de e-tjänster som tillhandahålls direkt av kommunerna för t.ex. ansökan om olika tillstånd. Tillväxtverkets roll är att på verksamt.se bygga en guide och checklista för att starta restaurang. SKL fokuserar på e-tjänsterna för de olika typer av kommunala tillstånd som krävs för att starta restaurang.

I det initiala arbetet har det uppmärksammats att många kommuner gör olika tolkningar av regelverket för olika tillstånd, t.ex. tillståndskrav för alkoholförsäljning. Det beskrivs vara en utmaning i arbetet att ensa tolkningarna och få en gemensam nationell tolkning och tillämpning av de styrande författningarna.

5.12 Kompetens och stödmaterial

I kartläggningsarbetet har flera av dem vi talat med pekat på att förmågan att samarbeta tvärfunktionellt behöver stärkas. Den digitala utvecklingen är inte en fråga som kan hanteras isolerat av en viss avdelning utan kräver att hela verksamheten involveras för att bästa resultat ska uppnås. Vissa framhåller behovet av fortsatt breddad kompetens för att få bättre förutsättningar att skapa förståelse över professionsgränserna. En förutsättning för gott samarbete över avdelningsgränser beskrivs vidare vara att de olika professionerna har förståelse för varandras uppdrag.

Likväl som jurister kan behöva bredda sin kompetens inom it och informationssäkerhet framhålls att även andra yrkesroller t.ex. it- och informationssäkerhetsspecialister, tekniker, upphandlare m.fl. behöver ha baskunskaper i det rättsliga regelverket som styr digitaliseringen. Att tolka dataskyddsbestämmelser i förhållande till befintlig teknik bör inte helt överlämnas till jurister som saknar djupare teknisk kunskap. Det finns med andra ord ett basbehov av kunskap i rättsinformatik, dvs. insikter om samband mellan materiell

it-rätt och metoder för att proaktivt integrera juridiken i digitaliseringsarbetet.

Under kartläggningsarbetet framkommer vidare att myndigheter generellt efterfrågar ett utökat rättsligt stöd i form av t.ex. uttalanden i förarbeten eller praxis. Myndigheternas rättstillämpare vill kunna känna sig trygga med rättsliga bedömningar och vägval i digitala utvecklingsarbeten. Dessvärre finns det sparsamt med förarbetsuttalanden och praxis som direkt går att applicera på dagens digitala miljöer.

Ett par myndighetsrepresentanter påtalar också att vägledningar bör utformas ur ett mer praktiskt perspektiv. Det är inte tillräckligt att veta *att* något ska göras. Myndigheterna måste också få ledning i *hur* det ska göras.

5.13 Den rättsliga begreppsapparaten

5.13.1 Äldre begrepp i digitala miljöer

Inom ramen för kartläggningen har flera myndigheter påtalat komplexiteten i att applicera bestämmelser med föråldrade begrepp på dagens digitala miljöer. Regelverket som styr den digitala förvaltningen innehåller en mängd begrepp som tankemässigt knyter an till analoga förhållanden. Som exempel kan nämnas ärende, handling, inkommen, upprättad, skriftlig och underskrift. Det finns också begrepp som knyter an till tekniska förfaranden men som är så ålderdomliga att de är svåra att tillämpa på dagens tekniker. Ett exempel är begreppet utlämnande på medium för automatiserad behandling. Begreppet saknar legaldefinition men vanligen avses ett överlämnande av elektroniskt lagrade uppgifter via t.ex. e-post eller genom filöverföring från ett datorsystem till ett annat.[53]

Den begreppsbildning som finns i tryckfrihetsförordningen har också beskrivits som komplicerad att sätta i relation till nutida teknikanvändning. Det gäller t.ex. lokutionen teknisk bearbetning eller teknisk lagring i 2 kap. 10 § tryckfrihetsförordningen.[54] Genom en ändring i offentlighets- och sekretesslagen den 1 januari 2018 har

[53] Se t.ex. *Patientdatalag m.m.*, prop. 2007/08:126, s. 77.
[54] Observera att ändringar i bl.a. 2 kap. tryckfrihetsförordningen föreslås i *Ändrade mediegrundlagar*, prop. 2017/18:49. Ändringarna innebär bl.a. ändrade beteckningar på lagrum.

sekretesskyddet ökats för uppgifter som tekniskt lagras eller bearbetas av en myndighet för någon annans räkning.[55] Även om ändringen välkomnas menar vissa att det fortfarande är oklart vad som är den faktiska innebörden av begreppen teknisk lagring och teknisk bearbetning i dagens digitala miljöer.

I 2 kap. 11 § första stycket 1 tryckfrihetsförordningen stadgas att brev, telegram eller annan sådan handling som har inlämnats till eller upprättats hos myndighet endast för befordran av meddelande inte anses vara allmän handling. Varken förarbeten eller praxis ger emellertid tillräcklig ledning om hur begreppet befordran av meddelande (post, telegram etc.) ska tolkas och tillämpas i förhållande till dagens teknikanvändning.

Någon av dem vi träffat har påpekat att när tolkning och tillämpning av otidsenliga begrepp på dagens digitala miljöer överlämnas till tjänstemän vid enskilda myndigheter blir en effekt att begreppen fylls med olika innebörd och räckvidd hos de olika myndigheterna, vilket kan bli problematiskt vid myndighetsöverskridande samarbeten.

5.13.2 En splittrad begreppsapparat

I kartläggningsarbetet har flera aktörer uppmärksammat behovet av en gemensam begreppsapparat i författningar. I dagsläget kan ett och samma begrepp användas med olika betydelser. Avsaknaden av en enhetlig begreppsapparat leder till att myndigheter behöver lägga tid och resurser på att lösa definitionsfrågor i varje enskilt utvecklingsarbete. Ska t.ex. en interoperabel tjänst för juridiska personer utvecklas behöver det finnas en entydig tolkning av begreppet *företag*. Eller kanske är det inte alls begreppet företag som ska användas utan *bolag*? Eller *organisation*? Skillnader i begreppsanvändningen riskerar att slå tillbaka i framtiden, när olika tjänster hos olika myndigheter ska kopplas ihop.

Det har vidare framhållits att begrepp som knyter an till digital arkivering och gallring behöver användas på ett enhetligt sätt. Begreppet *gallring* kan ha olika innebörd i olika författningar och ibland används andra begrepp t.ex. *radera*, *ta bort*, *utplåna* eller *förstöra* trots

[55] 11 kap. 4 a § och 40 kap. 5 § offentlighets- och sekretesslagen.

att det är gallring som avses. I Utredningen om 2016 års dataskyddsdirektiv[56] görs ett arbete för att rensa upp i begreppsfloran och hålla isär arkivregleringen från personuppgiftsregleringen. Konkret handlar det om att ta bort begreppet gallring från personuppgiftsregleringen och i stället reglera att en viss behandling av personuppgifter ska upphöra.

Det beskrivs vara önskvärt att åstadkomma ytterligare förbättrade processer vid författningsändringar som motverkar tvetydighet eller motstridighet i olika lagstiftningsprodukter. Den typ av tvetydighet eller motstridighet som ovan beskrivits kan annars hindra eller hämma utvecklingsarbeten som avser digitala informationsutbyten.

5.14 Samverkan kring författningsändringar

Samverkan i frågor som rör behov av författningsändringar med anledning av förvaltningens digitalisering äger rum såväl horisontellt dvs. mellan myndigheter, som vertikalt, dvs. mellan myndigheter och Regeringskansliet. Under kartläggningen har vi fått bilden av att myndigheter i allt högre grad samverkar med varandra och gemensamt hemställer om nödvändiga författningsändringar i t.ex. ett digitalt utvecklingsarbete som involverar informationsutbyte mellan myndigheterna. Generellt sett efterfrågar myndigheterna dock effektivare och smidigare processer för att kunna föra fram behov av ny eller förändrad reglering till lagstiftaren. I dagsläget finns det flaskhalsar där lagstiftningsarbetet riskerar att fastna. Det beskrivs vara värdefullt för myndigheter att få snabb återkoppling från departementen på gjorda hemställningar om författningsändringar. Är en beskrivning tillräckligt detaljerad eller saknas någon del i analysen? Det beskrivs också vara viktigt att lagstiftningsprocessen till stöd för den digitala förvaltningen bedrivs löpande och myndigheter efterfrågar en samordning eller gemensam kontaktpunkt för frågor som rör författningsändringar i anledning av utvecklingen mot en allt mer digital förvaltning.

En annan faktor som lyfts fram av flera myndigheter är tid. Författningsändringar tar lång tid att åstadkomma även när det rör

[56] *Brottsdatalag – kompletterande lagstiftning* (SOU 2017:74). Se även *Myndighetsdatalag* (SOU 2015:39), kapitel 14.

sig om förordningsändringar och än längre tid om det gäller lagändringar. I stället för att invänta en regeländring kan det leda till att myndigheter anpassar sig efter rådande reglering med följd att utvecklingsinsatsen inte blir optimal.

En följd av att nya digitala informationsutbyten mellan myndigheter i regel kräver författningsändringar är att departementen belastas med olika hemställningar om författningsändringar. Vid informationsutbyten mellan myndigheter berörs ofta fler än ett departement och det krävs samordning och likvärdig prioritering mellan departementen för att nödvändiga författningsändringar ska komma till stånd.

Några har framhållit att uppdragsgivaren ibland tenderar att förbise att vid myndighetssamverkan i den digitala förvaltningen behöver frågor om reglering kring digital informationshantering i princip alltid omhändertas. Rättsliga frågor behöver lösas i ett tidigt skede i utvecklingsprocessen för att åstadkomma rättsligt stöd för det digitala informationsutbyte som planeras. Av denna anledning är det önskvärt att departementen redan från början, när ett uppdrag bereds, tänker i digitala processer. Om så inte sker riskerar det att gå åt onödigt mycket tid för att i efterhand lösa rättsliga frågor om t.ex. förutsättningarna för digitalt informationsutbyte. Alternativt hindras effektiva och ändamålsenliga digitala processer eftersom de får brytas med manuella mellanled.

Flera av dem som deltagit i kartläggningsarbetet reagerar på att de nya författningar som tas fram sällan är anpassade till digitala processer. Man kan i någon mån hävda att lagstiftningsprodukter, trots att utgångspunkten är teknikneutralitet, i de flesta fall fortfarande utgår i från analoga förfaranden i stället för digitala.

6 Några inledande reflektioner över kartläggningsresultatet

6.1 Offentlig förvaltning i hela dess vidd

Utredningens uppdrag är inte begränsat till viss verksamhet, viss organisation eller viss information inom förvaltningen. Utan att här gå in i någon närmare beskrivning av den svenska förvaltningen i hela dess vidd finns det därför anledning att inledningsvis i korta ordalag beskriva den spännvidd som såväl kartläggningsresultatet som uppdraget i stort omfattar.

Den pågående och förmodade framtida digitaliseringen av offentlig förvaltning omfattar för det första vitt skilda verksamheter. De statliga myndigheternas respektive uppdrag är i flera avseenden av väsentligt skild karaktär och sträcker sig sammantaget över ett mycket brett område. Därtill har kommuner och landsting andra typer av uppdrag. Vid sidan av obligatoriska angelägenheter som t.ex. skolverksamhet och socialtjänst skiljer det sig också i viss utsträckning åt vilken verksamhet som bedrivs i olika kommuner. Såväl statliga som kommunala myndigheter och landsting samt regioner har för det andra också vitt skilda organisatoriska förutsättningar, inte minst när det gäller storlek och resurser. I den offentliga förvaltningen hanteras för det tredje information av vitt skilda slag. Det handlar om allt från uppgifter som rör rikets säkerhet, uppgifter som av annan anledning är särskilt skyddsvärda från verksamhetssynpunkt eller känsliga personuppgifter, till offentliga uppgifter av harmlöst slag. Ur ett förvaltningsrättsligt perspektiv berör digitaliseringen både myndigheternas ärendehantering, service gentemot privatpersoner, företag och organisationer liksom det faktiska handlande som utförs i verksamheten, exempelvis vid användande av trygghetstekniker i vården och omsorgen.

En allmän reflektion över kartläggningsresultatet är också att den teknikutveckling och teknikanvändning som pågår eller planeras hos myndigheterna också innefattar en stor spännvidd, allt från att vissa nu står i begrepp att gå ifrån en pappershantering vid ärendehandläggning till att undersöka tillämpningsområden för avancerad teknik med artificiell intelligens (AI).

Samtidigt som vi strävar efter att uppmärksamma problem och lämna förslag till åtgärder eller lösningar som är gemensamma för hela eller stora delar av den offentliga förvaltningen innebär den sammantagna spännvidd som här har beskrivits att såväl problembeskrivningar som bedömningar och förslag kommer att behöva nyanseras i olika delar av betänkandet. Här kan också nämnas att utredningen använder begreppet offentlig förvaltning med avseende på förvaltningsmyndigheter (statliga, kommunala och landstingskommunala) och domstolar. I de fall frågor rör andra aktörer eller hela den offentliga sektorn, dvs. all offentligt finansierad verksamhet, framgår det särskilt.

6.2 Detaljerad reglering

Av kartläggningen framgår det tydligt att myndigheter, och olika aktörer som i olika avseenden samverkar med myndigheter, ställs inför en mängd rättsliga frågor i samband med att digital teknik används eller införs på olika områden inom förvaltningen. Snabbheten i den tekniska utvecklingen och den förväntan på samhällsutveckling som följer med denna innebär att de rättsliga frågorna kopplade till förvaltningens digitalisering också ökar såväl i antal som i komplexitet och behöver besvaras i allt snabbare takt. Myndigheterna har också generellt sett en omfattande regelmassa att beakta i samband med varje digitaliseringsåtgärd.

Olika röster har i kartläggningsarbetet fört fram att regleringen i dag är detaljerad, och varken är anpassad eller hinner anpassas i den takt som behövs för att i tid svara upp mot de förväntningar som olika aktörer har på att förvaltningens verksamheter ska utvecklas i takt med teknik- och samhällsutvecklingen i övrigt. En inledande reflektion är att det allmänt sett synes vara problematiskt med rättslig styrning genom detaljerad reglering i lagform på områden som står under snabb utveckling.

Enligt såväl vår samlade erfarenhet som kartläggningsresultatet rör det sig påfallande ofta om dataskyddsregleringen eller om sekretessregleringen i mer vidsträckt bemärkelse, innefattande även de sekretessgenombrott eller uppgiftsskyldigheter som kan tillämpas myndigheter emellan, när det görs gällande att juridiken på ett onödigt sätt hämmar eller hindrar digital utveckling i förvaltningen. De rättsliga hinder eller svårigheter som har beskrivits för oss under kartläggningen ger inte på något sätt uttryck för att grundläggande skyddsbestämmelser i svensk grundlag, EU:s stadga om de mänskliga rättigheterna eller Europakonventionen skulle utgöra onödiga rättsliga hinder för digital utveckling. Det rör sig snarare om uttryck för att den nationella regleringen inom dessa rättsområden är detaljerad och att det i den specifika nationella rätten finns regler som förefaller vara onödigt begränsande eller hindrande.

För att lagstiftningen nu och fortsättningsvis inte i onödan ska hämma eller hindra en önskvärd utveckling är ett alternativ att öka takten i lagstiftningsarbetet för att i tid och vid varje tillfälle åstadkomma nödvändiga och önskvärda förändringar i en fortsatt detaljerad nationell lagstiftning. Ett annat alternativ är att försöka åstadkomma en mer generisk reglering inom de ovan beskrivna områdena, dvs. sträva mot en reglering som inte innehåller lika detaljerade bestämmelser. Vi återkommer till frågorna i kapitel 12.

Vi har under kartläggningen också tagit till oss det perspektivet att en omfattande mängd detaljerade regler som styr digital informationshantering inom förvaltningen medför, och måste medföra, ett resurskrävande arbete för att analysera varje digitaliseringsåtgärd i förhållande till den detaljerade och omfattande regleringen. Den tidsåtgången skulle också kunna minska med mer generella regler, bl.a. med hänsyn till att en högre grad av gemensamma förutsättningar för myndigheter skulle skapa bättre möjligheter för en mer enhetlig tolkning och tillämpning av regleringen. Här finns anledning att understryka att digital informationshantering, exempelvis digitala informationsutbyten mellan myndigheter, vanligen ställer krav på en väsentligt större exakthet redan från början än vad som har behövts i en manuell eller analog miljö, där rutiner och andra förfaranden har kunnat bestämmas och anpassas efter hand. I en samverkande digital förvaltning finns med andra ord ett begränsat utrymme för att tolkning och tillämpning av rättsregler ska kunna skilja sig åt mellan myndigheter eller verksamheter.

6.3 Teknikneutral reglering

De allra flesta författningar reglerar i dag områden som också på något sätt styrs av eller genomförs genom informations- och kommunikationsteknik. På området för digitalisering av den offentliga förvaltningen ligger det också i sakens natur att det förhåller sig på det sättet. Här finns inte utrymme för någon närmare redogörelse för hela den offentliga förvaltningens teknikanvändning men i den utsträckning det är relevant för utredningens överväganden och förslag återkommer vi i det följande till närmare beskrivningar av viss teknik.

Även om det finns ett samband mellan författningar och tekniska förutsättningar har riksdag och regering länge sökt utforma föreskrifter på ett sätt som är neutralt i förhållande till både den teknik som finns tillgänglig och används just vid tillfället för författningens tillkomst liksom okända framtida digitala lösningar. Fördelen med ett sådant förhållningssätt är att regleringen blir mer långsiktigt hållbar i den bemärkelsen att den inte behöver anpassas eller reformeras i samma tempo som den tekniska utvecklingen, vilket i många avseenden inte vore möjligt med tanke på den noggrannhet som lagstiftningsarbete kräver och den tidsåtgång som detta medför.

Här finns också anledning att särskilt belysa frågan om vad som egentligen avses med en teknikneutral reglering. En sådan reglering är ofta neutral i den bemärkelsen att den inte pekar ut en viss teknisk lösning, t.ex. e-post, i författningens ordalydelse. Under kartläggningen har emellertid vid ett flertal tillfällen uppkommit diskussioner om att en till synes teknikneutral reglering ofta innebär att traditionella förfaranden och processer som innefattar pappershantering utgör utgångspunkten för de handlingsdirektiv som författningen anger. Det kan bl.a. röra sig om att regleringen styr att viss information under ett visst skede ska överföras från en aktör till en annan, exempelvis genom att ange en process bestående av anmälan respektive ansökan eller att på annat sätt ange handlingsdirektiv om att information i ett visst skede ska överföras. Sådana bestämmelser kan visserligen sägas vara neutrala i förhållande till vilken teknik som används vid det förfarande som regleras. Informationshantering med digitala medel väcker emellertid frågor även rörande dessa typer av bestämmelser, eftersom den digitala tekniken

möjliggör en helt annan typ av hantering av information än vad som var möjligt när processerna reglerades.

Enligt vår bedömning kan en teknikneutral reglering nu och i framtiden inte utgå från att papper är informationsbäraren och att postgång används för förmedling av information. Även de gällande författningar som kan framstå som teknikneutrala kan därför behöva förändras i anledning av digitaliseringen. Behovet av att författningar som nu och i framtiden tas fram beaktar att den verksamhet som regleras kommer att stödjas eller utföras genom digitala eller automatiserade processer återkommer vi till i kapitel 7.10.

Det finns också nackdelar med en långtgående ansats att hålla författningsregleringen teknikneutral i så stor utsträckning som möjligt. Att en sådan teknikmässigt fristående författning medför svårigheter för tillämparen som ska applicera de neutrala reglerna på en många gånger komplex teknisk verklighet måste här framhållas som den största nackdelen med den teknikneutrala ansatsen i lagstiftningsarbetet. En alltigenom teknikneutral reglering riskerar också att försvåra dess förutsebarhet, till nackdel såväl för tillämpande myndigheter som för enskilda. Otydliga rättsliga förutsättningar för också med sig exempelvis risker för rättsosäkerhet när varje myndighet för varje utvecklingsarbete finner sina egna rättsliga lösningar. Det uppstår också risker för onödiga kostnader, eller avsaknad av effektiva lösningar, om eller när systemen i efterhand inte visar sig hållbara från rättslig synvinkel. Domstolspraxis skulle i viss utsträckning kunna läka de brister som en teknikneutral reglering innebär, men sådan praxis förekommer i påfallande låg utsträckning avseende den typ av rättsfrågor som här aktualiseras. Det finns dessutom sällan tid att invänta en eventuell framväxt av rättspraxis eftersom reformer eller andra regeringsuppdrag till myndigheter ofta förutsätter att det snabbt genomförs ett utvecklingsarbete i myndighetens it-system.

Samtidigt som teknikneutraliteten i författningar innebär att svåra rättsliga frågor lämnas åt enskilda rättstillämpare vid myndigheter som står inför ett digitaliseringsarbete, innebär sådan verksamhetsutveckling att avsevärda resurser läggs ned på utvecklingsinsatsen. Att under de förhållandena lämna det fulla ansvaret för att dra rättsliga slutsatser av en neutral lagstiftning ställer omfattande krav på den som har till uppgift att stå för juridiska bedömningar i

ett sådant digitaliseringsarbete. I kapitel 6.5 utvecklas vilka svårigheter som, bl.a. med hänsyn till den teknikneutrala regleringen, är förenade med inte minst juristens roll i digitala utvecklingsarbeten.

I våra fortsatta överväganden och förslag tas frågan om teknikneutralitet genomgående i beaktande. I de förslag som lämnas kommer utredningen att sträva efter att uppnå de fördelar som en teknikneutral reglering syftar till att åstadkomma. Den reglering som föreslås ska alltså vara långsiktigt hållbar och i princip inte innehålla detaljerade regler som knyter an till specifika tekniska lösningar som är kända och används i dag. Med andra ord ska förslagen inte vara fastlåsta vid dagens tekniska lösningar och därigenom hindra en fortsatt utveckling mot användandet av sådana trygga, innovativa och effektiva lösningar i förvaltningen som ännu inte är kända. Samtidigt strävar vi efter att uppnå målsättningen att lämna förslag och att motivera dessa på ett sätt som dels ska ge ett konkret rättsligt stöd till vägledning för tillämparen, dels tillvaratar enskildas intressen av bl.a. transparens och förutsebarhet.

6.4 Lagliga och lämpliga digitala tjänster

En allmän utgångspunkt är att förvaltningens digitaliseringsarbeten i första hand ska resultera i tjänster som är användarvänliga och som genererar nytta för privatpersoner eller företag eller för förvaltningens verksamhet. Med andra ord är det inte tillräckligt att det finns rättsliga förutsättningar för att ta fram digitala tjänster som uppfyller de krav som följer av reglering, det behöver finnas rättsliga förutsättningar för att ta fram lämpliga tjänster. Annars finns risk för att förvaltningen lägger tid och resurser på att utveckla tjänster som inte ger nytta.

Vilka tjänster som är lämpliga i den bemärkelsen att de genererar nytta för allmänheten och förvaltningens verksamheter kommer att förändras över tid. Det bör dock framhållas att flertalet sådana tjänster redan i dag utgör något helt annat än en ersättning för den kommunikation med och inom förvaltningen som tidigare och traditionellt sett har ägt rum genom pappershantering. I det följande (se kapitel 8) går utredningen närmare in på hur digitala tjänster skiljer sig från kommunikation genom pappershantering och potentialen för bl.a. ökad service gentemot privatpersoner och företag.

Därtill kommer att digitala tjänster skapar förutsättningar för ökad automation i förvaltningen (se kapitel 7), med de möjligheter till effektivitetssprång som detta innebär.

Om den fulla potentialen i förvaltningens digitaliseringsåtgärder ska kunna tas till vara behöver det därför finnas rättsliga förutsättningar för en informationshantering som utgår från nya möjligheter, inte från traditionella förfaranden som omsätts i en helt motsvarande digital informationshantering. Denna slutsats utgör en utgångspunkt för utredningens fortsatta analyser, bedömningar och förslag.

6.5 Juridisk metod i utvecklingsarbeten

Under utvecklingsarbeten behöver frågor av rättslig karaktär diskuteras på ett tvärfunktionellt sätt och angripas från olika perspektiv av arkivarier, jurister, säkerhetsansvariga, tekniker, verksamhetsutvecklare och flera andra professioner. Ur ett rent rättsligt perspektiv behöver frågor analyseras med flera (se bl.a. kapitel 4) författningar i åtanke. Det innebär att såväl specifika regler om myndigheters verksamhet som generella offentligrättsliga regler måste beaktas. Inte sällan behöver därför flera jurister med olika kompetens involveras i den rättsliga analysen. Ska tjänster upphandlas från privata leverantörer krävs därtill ofta ytterligare kompetens med avseende på kravställning och upphandling av it.

Det räcker emellertid inte att utgå från juristers bedömningar av vad som utgör gällande rätt vid de analyser som görs i samband med utvecklingsarbeten. Andra yrkeskategorier kan, som framgått ovan, från sitt perspektiv tillföra kunskap om att en digital informationshantering kan ordnas mer effektivt eller säkert med ett helt annat tillvägagångsätt än vad som varit utgångspunkten när gällande rätt togs fram. Befintliga regler som styr en verksamhet har nämligen, som framgått, många gånger tillkommit med utgångspunkt i en traditionell och pappersbaserad process för ärendehandläggning eller annan informationshantering. I den utsträckning det finns rättsregler som styr den processen kan dessa bestämmelser behöva förändras i anledning av digitaliseringen.

Det framgår av kartläggningen att det påfallande ofta därtill behövs en analys avseende om det befintliga legala stödet är tillräckligt när en myndighets verksamhet utvidgas. Som exempel kan nämnas att en myndighet står i begrepp att genom ett utvecklingsarbete ta på sig ett nytt åtagande att exempelvis tillhandahålla information till andra myndigheter. Den typen av åtaganden behöver på något sätt framgå av den skriftliga rättsordningen[1] för att grundläggande krav på bl.a. legalitet ska anses vara uppfyllda. Även sekretesslagstiftningen bygger på att myndigheters rutinmässiga utbyten av sekretessbelagda uppgifter normalt ska vara författningsreglerade.[2] Under pågående utvecklingsarbete är det vanligt förekommande att en eller flera samverkande myndigheters åtagande anges i ett regeringsuppdrag, t.ex. i myndigheternas regleringsbrev. När ett utvecklingsarbete är färdigt och resultatet ska övergå i drift och förvaltning hos någon myndighet eller flera i samverkan, men det inte sedan tidigare framgår i rättsordningen att myndigheten eller myndigheterna har det aktuella uppdraget, kan emellertid ett nytt legalt stöd för uppdraget behöva tas fram.

En sådan metod för rättslig analys under utvecklingsarbeten som här översiktligt har beskrivits ställer höga krav på såväl jurister som andra tjänstemän (eller konsulter) i andra yrkeskategorier. Den ställer också krav på samarbete mellan myndigheter och Regeringskansliet för att åstadkomma nödvändiga och önskvärda författningsändringar i takt med pågående utvecklingsarbeten. Utredningen återkommer därför i betänkandet till frågor om bl.a. organisatoriska förutsättningar för att bedriva rättsutveckling i takt med samhälls- och teknikutveckling (se kapitel 12). Det står också klart att det krävs noggranna överväganden inför bl.a. utkontraktering till privata leverantörer och tecknande av it-avtal. Utredningen återkommer till dessa frågor i kapitel 10 och 11.

[1] Jfr legalitetsprincipens krav på normmässig förankring för den verksamhet myndigheten bedriver. Det kan vara fråga om reglering i lag eller förordning, t.ex. myndighetens instruktion, men också om ett förvaltningsbeslut från regeringen, t.ex. i myndighetens regleringsbrev.

[2] Det förekommer emellertid att myndigheter rutinmässigt utbyter information utan att detta framgår uttryckligen av författning. Se även Lenberg m.fl., Offentlighets- och sekretesslagen (12 maj 2017, Zeteo), kommentaren till 10 kap. 27 § under rubriken Rutinmässigt utlämnande av uppgifter.

6.6 EU och utrymmet för nationell reglering

En allmän fråga som väckts inom ramen för utredningen är hur stort handlingsutrymme det egentligen finns att behålla eller införa nationella rättsregler för styrning eller stöd avseende förvaltningens digitala informationshantering och digitaliseringsåtgärder, med beaktande av de rättsakter och övriga initiativ som utarbetas inom EU. Under kartläggningen har det också lyfts fram att särskilda svårigheter vid digital samverkan, även nationellt mellan svenska myndigheter, kan uppstå när myndigheter i skilda verksamheter har att följa olika EU-rättsakter. Det finns därför anledning att här inledningsvis kort beskriva vissa utgångspunkter med anledning av EU-rätten.

Frågan om vilken kompetens EU har att anta rättsakter skiljer sig åt mellan olika områden. Enligt principen om tilldelade befogenheter[3] ska unionen endast handla inom ramen för de befogenheter som medlemsstaterna har gett unionen i fördragen för att nå de mål som fastställs där. Unionens befogenheter kan delas upp i exklusiva befogenheter, befogenheter som delas med medlemsstaterna och befogenheter att vidta åtgärder för att stödja, samordna eller komplettera medlemsstaternas åtgärder.[4] Här går vi inte närmare in på de olika områdena men konstaterar att det skiljer sig åt inom olika rättsområden vilket utrymme för lagstiftning som förbehålls EU respektive medlemsstaterna. Det finns även rättsakter som vilar på särskilda EU-rättsliga grunder. Det gäller exempelvis rättsakter om skydd för personuppgifter.[5] Rätten till skydd av personuppgifter har även fått status som en självständig rättighet i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna.[6]

Antagna EU-rättsakter ska tillämpas vid svenska myndigheter, antingen direkt i den mån regleringen antagits i form av en förordning eller efter genomförande i svensk rätt om rättsakten antagits i form av ett direktiv. Bland rättsakter av generell betydelse för den svenska och digitalt samverkande förvaltningen bör t.ex. nämnas

[3] Artikel 5.2 i fördraget om Europeiska unionen. EUT C 202, 7.6.2016, s. 18. EUR-Lex (FEUF).
[4] Se Fördelning av befogenheter inom Europeiska unionen. EUR-Lex. 23 mars 2010 (senast ändrad den 26 januari 2016).
[5] Artikel 16 FEUF.
[6] EUT C 83, 30.3.2010, s. 389.

NIS-direktivet[7] med bestämmelser om informationssäkerhet, dataskyddsförordningen[8] med bestämmelser om skydd för personuppgifter och eIDAS-förordningen[9] med bestämmelser om krav på ömsesidigt erkännande av anmälda e-legitimationer och krav på tillhandahållande av betrodda tjänster och en rättslig ram för sådana tjänster. Även Inspire-direktivet[10] och Tullkodexen[11] kan här nämnas som exempel på rättsakter som kräver vissa digitala förfaranden och som ska tillämpas av vissa svenska myndigheter eller verksamheter.

Utredningen har givetvis att förhålla sig till de givna förutsättningarna vad gäller fördelning av befogenheter mellan Sverige och EU när författningsändringar övervägs. Utrymmet för nationell rätt varierar därmed beroende på hur befogenheterna fördelas mellan EU och medlemsstaterna. I de avseenden vi i det följande överväger författningsändringar tar vi med oss det som ovan beskrivits om utrymmet för nationell rätt.

Utöver de rättsakter som antagits inom EU har också andra initiativ tagits med bäring på den digitala förvaltningen. Här bör särskilt EU:s handlingsplan för e-förvaltning nämnas.[12] I handlingsplanen anges ett antal principer, däribland ”Digitalt som standard”. Den principen innebär att offentliga förvaltningar bör leverera sina tjänster digitalt (inklusive maskinläsbara uppgifter) som förstahandsalternativ, samtidigt som andra kanaler hålls öppna för personer som inte är uppkopplade, av eget val eller av nödtvång. Offentliga tjänster bör också tillhandahållas via en enda kontaktpunkt (”one-stop-shop”) och via olika kanaler.

[7] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.
[8] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[9] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.
[10] Europaparlamentets och rådets direktiv 2007/2/EG av den 14 mars 2007 om upprättande av en infrastruktur för rumslig information i Europeiska gemenskapen (Inspire).
[11] Europaparlamentets och rådets förordning (EU) nr 952/2013 av den 9 oktober 2013 om fastställande av en tullkodex för unionen.
[12] Meddelande från kommissionen till europaparlamentet, rådet, europeiska ekonomiska och sociala kommittén samt regionkommittén av den 19 april 2016, EU:s handlingsplan för e-förvaltning för 2016–2020, Snabbare digital omvandling av förvaltningar (COM [2016] 179 final). Se även www.eu2017.ee/news/insights/tallinn-declaration-egovernment-ministerial-meeting-during-estonian-presidency

Ytterligare en av de principer som nämns i den EU-gemensamma handlingsplanen är ”The Once-Only Principle” (TOOP). Principen innebär att offentliga förvaltningar bör säkerställa att medborgare och företag endast behöver lämna samma uppgifter en gång på ett ställe i den digitala förvaltningen. Om myndigheten i fråga har rätt att vidareanvända dessa uppgifter internt ska de vidta åtgärder, med iakttagande av bestämmelser om dataskydd m.m., så att det inte medför några ytterligare bördor för medborgare och företag.

Även om handlingsplanen med bl.a. de angivna principerna inte har kommit till rättsligt bindande uttryck har den bäring även på svenska initiativ, varför den behöver tas i beaktande i våra överväganden.

6.7 Tydliga rättsliga hinder, rättslig osäkerhet eller avsaknad av reglering

Det finns flera aspekter i gällande rätt som kan anses hindrande eller hämmande för digital utveckling inom förvaltningen. I avsnitt 6.2 ovan beskriver vi översiktligt att kartläggningen visar på hindrande eller hämmande reglering bl.a. när det gäller sekretessregleringen och regleringen om skydd för personuppgifter. Även vad gäller exempelvis krav på undertecknande och vissa bestämmelser som kräver viss form när information hanteras i en ärendeprocess ger kartläggningsresultatet uttryck för att regleringen kan vara såväl tydligt hindrande som onödigt hindrande.

Gällande rätt kan emellertid hindra eller hämma digital utveckling inom förvaltningen även när det inte finns klara och tydliga rättsliga begränsningar. En påtaglig mängd av de rättsfrågor som redan har väckts med anledning av hittillsvarande utveckling av den digitala förvaltningen saknar givna svar i författning eller andra etablerade rättskällor. Med andra ord kan de rättsliga frågorna inte klart och entydigt besvaras med att det antingen finns tydliga och konkreta hinder i gällande rätt, som enkelt kan undanröjas i den mån de är onödiga, eller att åtgärden är klart och entydigt förenlig med gällande rätt. En sådan rättslig osäkerhet kan också hindra eller fördröja digitalisering inom förvaltningen. Som framgår i kapitel 5.11.2

visar det sig t.ex. inte sällan i myndighetsgemensamma utvecklingsarbeten att myndigheternas jurister gör olika tolkningar och bedömningar av samma rättsliga frågor när rättsläget är oklart.

Kartläggningen visar också att avsaknad av rättsregler leder till en avsevärd osäkerhet i tillämpningen. Med avsaknad av rättsregler menar vi dels frånvaro av styrande rättsregler som ger handlingsdirektiv för digitaliseringsåtgärder, dels även i någon utsträckning avsaknad av rättsregler som ger ett klart legalt stöd för vissa av förvaltningens digitaliseringsåtgärder. Som exempel kan här nämnas avsaknaden av reglering för styrning och stöd avseende vad målsättningen om digitalt som förstahandsval vid förvaltningens kommunikation med privatpersoner och företag egentligen innebär. Vi ser att även den osäkerhet som uppstår i frågor där rättsregler saknas kan hindra eller fördröja en digital utveckling som annars vore samhällsnyttig och önskvärd. Det förtjänar också att framhållas att flera aktörer som utredningen haft kontakt med, i kartläggningsarbetet och i övrigt, har resonerat kring och framhållit vikten av att privatpersoner och företag behöver känna tillit till den digitala förvaltningen.

Inför våra fortsatta överväganden och förslag tar vi med oss de ovan beskrivna aspekterna av på vilket sätt gällande rätt kan hindra eller hämma digital utveckling inom förvaltningen; dvs. genom tydliga rättsliga hinder, rättslig osäkerhet eller avsaknad av reglering.

6.8 De politiska målen

Politisk styrning innebär att tillgodose medborgarnas önskemål och preferenser genom att förverkliga politiska mål. Målen för förvaltningspolitiken och it-politiken är av särskilt intresse för oss. Den statliga förvaltningspolitiken bedrivs med målet en innovativ och samverkande statsförvaltning som är rättssäker och effektiv, har väl utvecklad kvalitet, service och tillgänglighet och som därigenom bidrar till Sveriges utveckling och ett effektivt EU-arbete.[13] Regeringens mål för digitaliseringen av den offentliga förvaltningen är en enklare vardag för medborgare, en öppnare förvaltning som stödjer

[13] *Offentlig förvaltning för demokrati, delaktighet och tillväxt*, prop. 2009/10:175, bet. 2009/10:FiU38, rskr. 2009/10:375.

innovation och delaktighet samt högre kvalitet och effektivitet i verksamheten.[14] Sverige ska också, enligt målet för it-politiken, vara bäst i världen på att använda digitaliseringens möjligheter.[15]

De angivna målen utgör enligt Utredningen om effektiv styrning av nationella digitala tjänster snarare mål för regeringens arbete och politiken som helhet, än sådana mål som myndigheterna förväntas uppnå. Utredningen har därför föreslagit att riksdagen ska anta ett nytt mål för den offentliga förvaltningens digitalisering som ska ligga till grund för regeringens redovisning till riksdagen och styrningen av de offentliga myndigheterna. Utredningen föreslår också ett digitaliseringsmål för de statliga myndigheterna.[16]

När det gäller den offentliga sektorns kontakter med privatpersoner och företag anser regeringen att digitalt ska vara förstahandsval. Detta är grunden i regeringens satsning Digitalt först. Digitalt som förstahandsval innebär att den offentliga förvaltningen, när det är lämpligt, ska välja digitala lösningar vid utformningen av sin verksamhet. Samtidigt ska säkerheten och skyddet för den personliga integriteten säkerställas. Med det i beaktande ska det vara enkelt att digitalt komma i kontakt med det offentliga Sverige.[17]

I kapitel 6.6 har den EU-gemensamma handlingsplanen för e-förvaltning presenterats. Den politiska inriktningen att åstadkomma en digitalt tillgänglig förvaltning har också nyligen stärkts inom EU genom en gemensam ministerdeklaration.[18] Genom deklarationen har medlemsstaterna förklarat att steg ska tas för att bl.a. säkerställa att privatpersoner och företag ska kunna komma i digital kontakt med förvaltningen. Regeringen har också i en skrivelse till riksdagen utvecklat den politiska inriktningen för hur Sverige ska bli bäst i världen på att använda digitaliseringens möjligheter.[19]

---

[14] *Budgetpropositionen för 2018*, prop. 2017/18:1, utg. omr. 2, 6.2 Mål.
[15] *Budgetpropositionen för 2012*, prop. 2011/12:1, utg.omr. 22, bet. 2011/12:TU1, rskr. 2011/12:87.
[16] Utredningen om effektiv styrning av nationella digitala tjänsters delbetänkande *digitalforvaltning.nu* (SOU 2017:23), s. 113 f., och slutbetänkande *reboot – omstart för den digitala förvaltningen* (SOU 2017:114).
[17] Prop. 2017/18:1, utg. omr. 2, 6.2 Mål.
[18] Se Tallindeklarationen om e-förvaltning av den 6 oktober 2017 på www.eu2017.ee/news/insights/tallinn-declaration-egovernment-ministerial-meeting-during-estonian-presidency
[19] Regeringens skrivelse *Hur Sverige blir bäst i världen på att använda digitaliseringens möjligheter – en skrivelse om politikens inriktning* (skr. 2017/18:47).

6.9 Behövs fler regler för styrning och stöd av den digitala förvaltningen?

Som framgår i kapitel 4 ska redan i dag ett stort antal författningar tillämpas i samband med digitalisering av verksamhet och anknytande informationshantering i den offentliga förvaltningen. Att mängden, ofta komplexa, regler i sig medför svårigheter för tillämpare och beslutsfattare framgår av den kartläggning som vi har genomfört och är också erfarenhetsmässigt känt. Det kan vidare med fog invändas att förvaltningen inte ska styras i detalj genom reglering, utan att tillit ska sättas till att myndigheter bäst själva utför sina respektive uppdrag och väljer formen för detta inom givna ramar. Mot den bakgrunden skulle det kunna invändas att det vore olämpligt att införa ytterligare bestämmelser som ska tillämpas i samband med förvaltningens digitaliseringsåtgärder liksom löpande användning av informations- och kommunikationsteknik.

En utgångspunkt för utredningen är emellertid att möjliggöra ett större steg mot en framtida trygg, innovativ och effektiv digital förvaltning. För detta krävs en viss rättslig stabilitet som den fortsatta utvecklingen av den digitala förvaltningen kan vila på. Att åstadkomma en sådan, ur rättssäkerhetssynpunkt, nödvändig stabilitet bedömer vi inte vara möjligt genom att enbart undanröja eller anpassa gällande regler. En begränsning till den typen av åtgärder och författningsändringar åstadkommer varken de handlingsdirektiv eller ger det rättsliga stöd som vi bedömer behövs. Det är också av stor vikt för tilliten till den digitala förvaltningen att enskilda genom lagstiftningen har möjlighet att få såväl en rättvisande bild av hur förvaltningen faktiskt sköts som insyn i densamma.

Den pågående digitaliseringen av förvaltningen med bl.a. ökande automation, kommer enligt vår bedömning att innebära påtagliga förändringar av själva verksamheten, inte bara det sätt som verksamheten utövas på. Även ur ett konstitutionellt perspektiv finns det därför enligt vår bedömning anledning att överväga hur ansvar och risker som hör samman med dessa förändringar bör fördelas och i vilken utsträckning det bör göras genom rättsregler. Samtidigt behöver vi givetvis beakta att den lagstiftning som ska tillämpas i samband med åtgärder som rör förvaltningens digitalisering inte ska hindra eller hämma fortsatt utveckling.

6.10 Betänkandets fortsatta disposition

Våra närmare analyser, bedömningar och förslag framgår i kapitel 7–13. I kapitel 7, 8 och 10 presenteras utredningens prioriterade områden för författningsförslag. Författningsförslagen rör god offentlighetsstruktur vid vissa automatiserade förfaranden i förvaltningen och ansatsen om Digitalt först vid förvaltningens kommunikation med enskilda. De rör också en tystnadsplikt för privata leverantörer som behandlar myndigheters uppgifter för enbart teknisk bearbetning eller lagring och en sekretessbrytande bestämmelse för att myndigheter i samband med utkontraktering av teknisk bearbetning eller lagring ska kunna lämna ut vissa sekretessbelagda uppgifter till privata eller offentliga leverantörer. Områdena har valts ut efter de närmare överväganden som beskrivs i respektive kapitel. Övergripande för dessa områden gäller dock att vi funnit dem centrala för att myndigheter fortsatt ska prioritera digitalisering av sin verksamhet och våga ta effektivitetssprång genom att använda ny teknik till gagn för såväl enskilda som samhället i stort. Samma områden är också centrala för att säkerställa transparenta, säkra och rättssäkra förfaranden, så att enskilda kan känna tillit till den digitala förvaltningen och välja enkla digitala lösningar för kontakter med förvaltningen. Förvaltningens digitalisering kan knappast heller diskuteras utan att frågor om informationssäkerhet belyses. Det gör vi i kapitel 9.

Ur olika perspektiv står frågor om samverkan i fokus för vårt uppdrag. Samverkan inom förvaltningen, mellan myndigheter och i förhållande till regeringskansli, inte minst när det gäller frågor om lagstiftning, är högst relevanta för denna utredning. Samverkan i förhållande till privata leverantörer av it-drift och andra it-baserade funktioner har också kommit att utkristallisera sig som ett fokusområde, när myndigheter inte alltid har möjlighet att med egen kompetens effektivt utveckla de digitala förfaranden som används eller som är påkallade för fortsatt digitalisering i förvaltningen. Förutom i kapitel 10 belyses detta närmare i kapitel 11 där vi behandlar några frågor om it-avtal och personuppgiftsbiträdesavtal.

De författningsförslag och andra förslag på åtgärder som lämnas inom ramen för denna utredning är emellertid endast att se som ett steg i det fortsatta arbetet med att åstadkomma en rättsutveckling

som möter den önskade digitala utvecklingen i förvaltningen. Åtgärder från såväl riksdag som regering pekar mot att förvaltningens digitaliseringsarbete nu ska genomdrivas med ökad intensitet. Det medför också behov av fortsatt lagstiftningsarbete. I kapitel 12 återknyter vi till frågor om fortsatt rättsutveckling liksom de analyser vi gjort när det gäller bl.a. lagstiftning som rör informationsförsörjning, informationsutbyten och ärendeprocesser, liksom frågor som rör tillhandahållande av öppna data och elektroniskt utlämnande av allmän handling.

Slutligen redovisas i kapitel 13 våra överväganden och förslag i den delen av uppdraget som rör rapportering av förvaltningens arbete med it och digitalisering.

7 Automation i förvaltningen

7.1 Kartläggningsresultatet och behovet av automation i förvaltningen

7.1.1 En ökad grad av automation

En fråga som ibland ställs gäller den närmare inriktningen för den digitala förvaltningen. Vart är vi på väg? En allmän reflektion efter att ha fått ta del av underlag och tankar från ett flertal myndighetsrepresentanter är att förvaltningen går mot en ökad grad av automation. Frågor om bl.a. digitalisering avseende informationsförsörjning eller informationsutbyten mellan myndigheter eller digital kommunikation med enskilda står i fokus för myndighetssamverkan, men utgör också ett medel för en ökad digitalisering av myndigheters kärnverksamhet, t.ex. ärendehandläggning.

Under kartläggningen har vi funnit att en påtaglig del av myndigheterna nu undersöker möjligheten att öka graden av automation i sina respektive verksamheter. Bland aktörer som strävar mot detta återfinns myndigheter som redan har automatiserat vissa ärendeprocesser och beslutsfattande och som nu överväger om detsamma är möjligt också inom andra områden. Möjligheter till exempelvis automatiserat beslutsfattande undersöks även hos myndigheter som hittills inte har använt den beslutsformen. Här finns möjligheter till effektivitetssprång i förvaltningen, men också risker som behöver belysas och hanteras rättsligt.

Att förvaltningen i flera avseenden behöver använda sig av kända tekniker, med beredskap för kommande, för att på ett tryggt och effektivt sätt fullgöra sin verksamhet står klart. Detta har bl.a. sin förklaring i att det på flera områden inte finns resurser för t.ex. mänsklig handläggning av ärenden inom de frister som behövs för att förfarandena ska vara rättssäkra ur en tidsaspekt. Behovet av att använda digitaliseringens möjligheter för att möta krav på att

myndigheters verksamhet bedrivs effektivt[1] kan enligt utredningen också förutses öka med tanke på digitaliseringen av samhället i stort.[2] Exempelvis har förvaltningen anledning att ha beredskap för att privata tjänster tas fram för att automatiserat inleda ärenden hos myndigheter.[3] Förvaltningen behöver mot denna kortfattade bakgrund ha rättsliga förutsättningar för att kunna använda de möjligheter till digitalisering inbegripande automation av förfaranden som kan förenas med, eller stärka, de centrala värdegrunder som beskrivits i kapitel 4.

Det finns anledning att framhålla att vi inom ramen för denna rättsligt orienterade utredning utgår från de politiska mål och inriktning som riksdag och regering givit (se bl.a. kapitel 6.8, 9.3.1 och 10.1.2). Både nationellt och inom EU förekommer därtill politiska initiativ med innebörd att den offentliga förvaltningen ska leda vägen för den digitala omvandlingen genom att möjliggöra tekniska genombrott och tidigt ta ny teknik i bruk.[4] Detta sätter ljuset på att det parallellt med den ökade digitaliseringen i form av automation i förvaltningen också kommer att finnas ett växande behov av ett stabilt informationssäkerhetsarbete som ett fundament i myndigheternas informationshantering (se vidare i kapitel 9).

Med automation inom förvaltningen[5] kan flera aspekter avses. Det finns därför anledning att inledningsvis beskriva några olika typer av automation (se kapitel 7.2). Viss teknikutveckling introduceras i kapitel 7.3.

7.1.2 God offentlighetsstruktur och rättssäkerhet

Såväl rättsliga hinder i gällande rätt som oklara rättsförhållanden kan komma att hindra eller hämma en utveckling mot en ökad grad av automation i en digital förvaltning. Under kartläggningen har ett

[1] 1 § första stycket lagen (1996:1059) om statsbudgeten och 3 § myndighetsförordningen (2007:515).
[2] Se bl.a. Digitaliseringskommissionens slutbetänkande *För digitalisering i tiden* (SOU 2016:89), s. 104 f. med där gjorda hänvisningar.
[3] I Sverige finns t.ex. redan en app för hjälp att överklaga felparkeringsbot. Se Göran Lindsjö, *En AI-redo statsförvaltning*, mars 2017, s. 23 på http://digitaltforst.se/wp-content/uploads/2017/03/En-AI-redo-statsförvaltning.pdf
[4] Se bl.a. regeringens digitaliseringsstrategi *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi*. Se även noter från Tallinn Digital Summit 29 september 2017, Conclusions of the Prime Minister of Estonia Jüri Ratas, på www.eu2017.ee/sites/default/files/inline-files/TallinnDigitalSummit_Conclusions_0.pdf
[5] I doktrin är förvaltningsautomation eller ”Verwaltungsautomation” vedertagna begrepp.

antal frågor och reflektioner framkommit som på en övergripande nivå kan sägas utgöra en rättslig osäkerhet avseende hur den allt mer digitala förvaltningen ska kunna säkerställa möjligheter till öppenhet och insyn, vilket ytterst kan sägas utgöra en garanti för att förvaltningens förfaranden både är och kan visas vara rättssäkra. Detta är, enligt såväl vår bedömning som vad flera gett till känna under kartläggningen, avgörande för att enskildas tillit till den digitala förvaltningen ska bestå vid en ökad grad av automation. Om insynsmöjligheterna efterhand visar sig brista riskerar detta inte bara leda till negativa konsekvenser för enskilda eller för samhället i stort, utan också hindra den fortsatta digitaliseringen. Den nu beskrivna rättsliga osäkerheten bedöms av oss ha en klart hämmande inverkan på förvaltningens fortsatta digitalisering.

Särskilt när digitala funktioner saknar sin direkta motsvarighet i en traditionell och manuell hantering har vi uppfattat att myndigheter upplever det svårt att var och en för sig bedöma rättsläget. Här kan som exempel nämnas att det vid ett automatiserat beslutsfattande, utöver den ärenderelaterade information som t.ex. ges in vid en ansökan och beslutet i sig, tillkommer algoritmer och datorprogram[6] med anknytande dokumentation av de krav som ställs på hur dessa implementeras i datormiljön. Rättslig tydlighet om vilka krav som ställs på myndigheter att upprätthålla bl.a. god offentlighetsstruktur i den digitala miljön efterfrågas även, och kanske särskilt, i de fall insynsintressen hamnar eller riskerar att hamna i konflikt med behov av säker slutenhet.[7] Här avses närmast den avvägning som behöver göras i förhållande till intressen av sekretess till skydd för bl.a. myndigheters verksamhet, intressen av skydd för personuppgifter och immaterialrättsligt skydd.

Svårigheterna att bedöma vad som krävs i fråga om att åstadkomma god offentlighetsstruktur vid automatiserade förfaranden förstärks när myndigheter inte har möjlighet att med egen kompetens utveckla de digitala förfaranden som används eller kommer att behöva användas för fortsatt digitalisering i förvaltningen. Inte sällan torde nämligen privata leverantörer komma att stå för dessa funktioner, vare sig det handlar om att myndigheter gör inköp eller

[6] Se kapitel 7.4.1 om begreppen.
[7] Jfr begreppets användning i Katastrofkommissionens betänkande *Tsunamibanden* (SOU 2007:44), s. 169.

om olika former av utkontraktering.[8] Utan tydlighet i regleringen blir det svårt för en myndighet att vid en upphandling ställa uttryckliga krav på att leverantören t.ex. måste tillgodose vissa insynsmöjligheter. Som ovan framgått riskerar också immaterialrättsliga intressen att komma i konflikt med insynsintressen, särskilt om avtalsförhållandena inte är klara på förhand.

De oklarheter som har uppmärksammats för oss gör att vi ser behov av en närmare analys av om gällande rätt nu och inför framtiden möjliggör en tillräckligt god offentlighetsstruktur för att säkerställa insyn i hur förvaltningens verksamhet bedrivs vid automatiserade förfaranden, särskilt när algoritmer och anknytande datorprogram får en allt mer framträdande roll i förvaltningens verksamhet. Analysen, liksom våra bedömningar och förslag, följer i kapitel 7.4–7.8. Ytterligare frågor som gäller den digitala förvaltningens öppenhet, bl.a. genom tillhandahållande av öppna data, analyseras i kapitel 12.

Kartläggningsresultatet visar även på myndigheters osäkerhet liksom uttryckliga hinder i fråga om rättsliga förutsättningar för övergång till förfaranden där stora datamängder används i förening med artificiell intelligens och maskininlärda algoritmer (se kapitel 7.3.2 för förklaring av begreppen). I kapitel 7.8 går vi närmare in på den tekniken.

7.1.3 Behov av automationsanpassad lagstiftning

För att det ska vara möjligt att fullt ut ta till vara på digitaliseringens möjligheter genom att t.ex. digitalisera ärendeprocesser har vi under kartläggningen fått presenterat för oss ett flertal exempel på rättsregler som behöver ändras. I förlängningen, om automationsgraden ökar i den utsträckning som vi förutspår, kommer det att finnas behov av anpassning av en påtaglig del av de rättsregler om bl.a. ärendeprocesser som förvaltningen tillämpar. Vi har med beaktande av omfattningen av kartläggningens resultat och tiden som stått till vårt förfogande av naturliga skäl inte haft utrymme att gå på djupet i alla de rättsliga frågor och exempel vi fått på lagstiftning som hindrar eller kan hindra digitalisering av bl.a. ärendehantering inom

[8] Här och i det följande har vi valt att i första hand använda det svenska begreppet utkontraktering i stället för begreppet outsourcing. Se vidare om begreppet i kapitel 10.1.1.

specifika sektorer, verksamheter eller myndigheter. I kapitel 12 återkommer vi dock till dessa frågor. I det sammanhanget överväger vi också frågan om hur det kan skapas bättre förutsättningar för att ta om hand sådana behov av författningsändringar i den tid och takt som är lämplig för att förvaltningens önskade digitala utveckling inte ska hindras eller hämmas i onödan av rättsliga skäl.

I vilken utsträckning gällande rätt med materiella bestämmelser som t.ex. tillämpas vid beslutsfattande bör ändras inför övergång till automatiserade förfaranden belyses i kapitel 7.9. I kapitel 7.10 diskuteras behovet av att bedöma konsekvenser för förvaltningens digitalisering när ny lagstiftning tas fram.

Här i kapitel 7 uppehåller vi oss särskilt vid rättsliga förutsättningar för automation i förvaltningen och i huvudsak dess ärendeprocesser, sett ur ett mer övergripande rättssäkerhetsperspektiv. Eftersom det ligger i vårt uppdrag att belysa hela förvaltningens förutsättningar är detta en naturlig utgångspunkt.

7.2 Förvaltningens verksamhet

7.2.1 Ärendehantering

Att anställda eller uppdragstagare i offentlig förvaltning använder datorstöd i form av ordbehandlingsprogram, e-post eller ärendehanteringssystem vid kommunikation med enskilda eller för dokumentation av uppgifter i ärenden och beslut framstår i dag som en självklarhet. Det är med andra ord numera få av oss som reflekterar närmare över den automation som den formen av it-stöd innebär för förvaltningen. Myndigheternas förfaranden vid ärendehandläggning är emellertid redan i dag påtagligt mer automatiserade än så. De myndigheter som tillhandahåller digitala tjänster för att privatpersoner och företag ska kunna inleda ett ärende har i samband härmed också skapat förutsättningar för att i vart fall inleda myndighetens handläggning av ärendet på ett helt automatiserat sätt. Ofta innebär detta att bl.a. diarieföring och första åtgärder för registrering av grundläggande uppgifter i myndighetens ärendehanteringssystem sköts helt automatiserat.

En inledande automatiserad ärendehandläggning kan, direkt eller i ett senare skede, övergå till att en mänsklig handläggare tar vid och med hjälp av ett maskinellt användarstöd fortsätter att hantera

ärendet och fatta beslut. Manuella förfaranden kan med andra ord kompletteras av automatiska. Beslut som fattas av människor kan exempelvis vara mer eller mindre tekniskt understödda, bl.a. när det gäller förvalda beslutsformuleringar. Det kan därför finnas anledning att tala om maskinellt understödda beslut även när mänskliga handläggare svarar för själva beslutsfattandet. Flertalet ärendetyper handläggs dock genom helt automatiserade förfaranden och avslutas med ett automatiserat beslutsfattande, bl.a. på skatte- och socialförsäkringsområdet. I de enskilda fallen tar alltså ingen enskild befattningshavare aktiv del i beslutsfattandet, utan förfarandet kan betecknas som ett helt automatiserat beslutsfattande. Att en ärendetyp som utgångspunkt handläggs automatiskt och avslutas med helt automatiserade beslut medför dock vanligen att funktioner behöver finnas för urval av vissa ärenden som inte kan hanteras helt automatiserat utan behöver övergå till manuell handläggning.

Vid automatiserade beslut finns normalt också automatiska funktioner för att underrätta parten om beslutet, men underrättelsen kan skickas antingen genom digitala förfaranden eller genom traditionell papperspost (se även kapitel 8.3.6). Även när en mänsklig handläggare står för beslutsfattandet förekommer det att användarstödet har mer eller mindre automatiserade funktioner för expediering.

7.2.2 Service

Att enskilda och företrädare för företag och organisationer själva kan söka efter information som myndigheter lämnar på sina webbsidor är ett numera högst vanligt tillvägagångssätt, men som ändå innebär att förvaltningen lämnar en form av automatiserad service.

Nya tekniker för lämnande av service som också väcker nya rättsliga frågor är emellertid högst aktuella. I kapitel 8.4.5 och 12.2.9 berör vi rättsfrågor om bl.a. språk, tolkning och översättning, liksom frågan om när handlingar blir att anse som allmänna i situationer där stöd och service lämnas till enskilda redan innan ett ärende hunnit inledas (t.ex. via ett eget utrymme, se vidare kapitel 8.4). Den service som lämnas redan i skedet innan en handling, t.ex. en ansökan, lämnas in till en myndighet kan dock samtidigt sägas vara en förutsättning för att uppgifterna i ärendet ska hålla en sådan kvalitet och

vara ordnade i sådan strukturerad form att den fortsatta handläggningen och beslutsfattandet i önskad grad kan automatiseras. Automationen kräver med andra ord att större vikt läggs vid myndighetens service gentemot enskilda innan ett ärende inleds, än vad som varit fallet vid traditionell handläggning av pappersbaserade anmälningar eller ansökningar.

Den ovan beskrivna vikten av att service ges redan innan ett ärende inleds i förvaltningslagens (2017:900) mening kan i sin tur väcka frågor om hur långt myndigheternas åtaganden enligt gällande rätt egentligen sträcker sig. Frågorna avser om eller när den service som myndigheten överväger att ge innan ett ärende inleds i något fall går utöver vad som är påkallat enligt gällande rättsordning, och därför skulle kräva särskilt stöd i författning eller genom t.ex. regeringsbeslut för att legalitetsprincipen ska vara uppfylld (se vidare kapitel 8.4.3 om legalitetsprincipen när digitala tjänster med eget utrymme används och kapitel 6.5 om metod för rättslig analys). Denna frågeställning kan aktualiseras vid utveckling av enkla och informativa tjänster för enskilda. I skedet innan exempelvis en bygglovsansökan ges in skulle det i tjänsten kunna lämnas förslag på hur en tomt kan bebyggas utan att den enskilde själv matar in egna uppgifter för beslutsunderlag. Någon generell lösning på denna typ av rättsfrågor har vi inte funnit inom de tidsramar som stått till utredningens förfogande utan stannar här vid att belysa att även ur denna aspekt kommer digitaliseringen och automationen i förvaltningen att föra med sig behov av överväganden om fortsatt rättsutveckling.

7.2.3 Faktiskt handlande

Myndigheternas faktiska handlande (i förvaltningsrättslig mening) har tidigare i stor utsträckning varit åtskilt från frågor om automation. Ett faktiskt handlande har nämligen till sin natur länge varit sådant att det endast kunnat utföras av en människa. Som exempel på faktiska handlanden kan nämnas en lärare som står i ett klassrum och undervisar eller en chaufför som kör en spårvagn, dvs. förfaranden som inte innefattar ärendehandläggning eller beslutsfattande i förvaltningsrättslig mening. Framtida tekniker förutspås emellertid i hög grad kunna ersätta mänskliga förfaranden. Det kan

röra sig om t.ex. självkörande fordon eller olika former av sensorer eller trygghetstekniker.[9]

I takt med ökad digitalisering och användning av nya tekniska möjligheter väcks det också nya rättsliga frågor, inte minst mot bakgrund av att ett automatiserat förfarande för med sig att hela den regelmassa som beskrivs översiktligt i kapitel 4 (om bl.a. god offentlighetsstruktur, informationssäkerhet, skydd för personuppgifter och sekretess för uppgifter) blir tillämplig.

Här kan som exempel nämnas frågor som uppstått i samband med användandet av digitala trygghetstekniker i socialtjänsten. En sådan teknikanvändning kan redan i dag i viss utsträckning sägas ersätta ett faktiskt handlande eller mänskliga ögon. Samtidigt har svåra rättsliga frågor lämnats till rättstillämpare, däribland frågan om regeringsformens skydd mot betydande intrång i den personliga integriteten[10] medför ett behov av särskilt lagstöd för användande av trygghetstekniker hos personer som själva inte är helt beslutsförmögna.

Vi ser inte möjlighet att prioritera närmare analys och eventuellt författningsförslag på det ovan beskrivna specifika området inom ramen för vårt uppdrag. Exemplet belyser emellertid väl de särskilda svårigheter som uppstår för rättstillämpare vid överväganden om automation på områden för faktiskt handlande inom förvaltningen, som hittills inte bedrivits på annat sätt än genom mänskliga förfaranden. Exemplet belyser också att lagstiftare och andra beslutsfattare i förvaltningen bör ha särskild beredskap och förståelse för att digitalisering och automation på områden för faktiskt handlande inom förvaltningen, som hittills förbehållits mänskliga förfaranden, i förlängningen kan kräva lagstiftningsåtgärder för att inte digitaliseringen ska hindras eller hämmas på grund av avsaknad av reglering.[11]

7.2.4 Ett kunskapsperspektiv

En förvaltning som är digital medför att de uppgifter som hanteras dels håller hög kvalitet även för statistik, dels kan länkas samman på

[9] Se bl.a. Digitaliseringskommissionens slutbetänkande *För digitalisering i tiden* (SOU 2016:89) s. 104 f. med där gjorda hänvisningar.
[10] 2 kap. 6 § andra stycket regeringsformen.
[11] Här kan nämnas att ”bruk av varslings- og lokaliseringsteknologi” har getts ett uttryckligt stöd i den norska loven om pasient- og brukerrettigheter.

nya sätt. I en digital förvaltning hanteras också stora digitala informationsmängder. Dessa förutsättningar ger i sin tur nya möjligheter att analysera informationen och därigenom få ny kunskap om förvaltningens verksamhet. Genom möjligheten att spåra och följa uppgifter kan t.ex. genomströmningstider och annan information om förvaltningens ärendehantering tas fram. Flödesstatistik av detta slag kan bland annat användas för att göra analyser av effektivitet. Den kan också ge mer tillförlitliga resultatmått. Sådan statistik kan tas fram både på nationell nivå och brytas ned på myndigheter eller mindre organisatoriska enheter, vilket bland annat ger ökade möjligheter att göra jämförelser. I förlängningen kan bl.a. bättre underlag skapas för regeringens styrning av förvaltningen. Det blir lättare att identifiera och bedöma var och hur resurserna ska användas och vilka konsekvenser eventuella resursförändringar kan förväntas få. Därigenom ökar möjligheterna att med träffsäkerhet genomföra reformer. Myndigheternas interna kvalitetsarbete och verksamhetsuppföljning underlättas också. Det kan även bli lättare att utvärdera lagändringar, till exempel hur en ny lag har tillämpats.

De uppgifter som samlas in och lagras i offentlig förvaltning kan också spela en central roll för den kunskapsutveckling som forskningen bidrar till. Nya tekniska möjligheter och stora datamängder kan användas för att få svar på frågor om samhällsförändring över tid och med stöd av analyser förutse framtida samhällsutveckling. Hur förutsättningarna för registerbaserad forskning kan förbättras analyseras inte närmare i denna utredning utan inom ramen för uppdraget i Forskningsdatautredningen.[12]

Genom att använda de möjligheter till analys som en strukturerad och digital informationshantering medger kan alltså kunskapen om förvaltningens verksamhet öka. Den kunskapen kan också återföras till verksamheten och användas för att stödja personal som har att hantera ärenden eller fatta beslut, eller på annat sätt vara till nytta för de enskilda som kommer i kontakt med förvaltningen. Här kan t.ex. det försäkringsmedicinska beslutsstödet nämnas. Beslutsstödet ger läkare stöd och rekommendationer vid sjukskrivningsbedömningar. Genom att beslutsstödet visar upp viss information direkt för användaren när en viss diagnoskod skrivs in i det system som läkaren använder får denne del av kunskap som han eller hon kanske inte

[12] *Personuppgiftsbehandling för forskningsändamål* (dir. 2016:65).

visste fanns eller annars hade fått ägna tid åt att eftersöka. Informationen kan därigenom sägas bli en del av läkarens kunskapsunderlag men det är fortfarande läkaren som avgör hur det enskilda fallet ska hanteras.

Ett annat exempel är s.k. learning analytics, som innebär att mäta, samla, analysera och rapportera data om bl.a. hur elever eller studenter lär sig och vad de lär sig. Genom analyserna kan underlag tas fram för att tidigare kunna ge stöd till de elever som behöver det. Sådana analyser kan också användas som underlag för att t.ex. utveckla nya läromedel.

Samtidigt som digital informationshantering i förvaltningen ger förbättrade möjligheter till kunskap uppkommer också nya rättsliga frågeställningar. Under kartläggningen har vi uppmärksammats på att det t.ex. inte alltid är så lätt att avgöra vad som är en statistikuppgift eller vad som är en personuppgift. När ny statistik behöver sammanställas av uppgiftsmängder som kommer från olika källor kan det exempelvis vara problematiskt att överblicka om det kan gå att härleda underlaget tillbaka till en viss person.

Frågor om förutsättningar för att använda stora datamängder gör sig bl.a. gällande vid överväganden om att skapa maskininlärda algoritmer (se närmare beskrivning i kapitel 7.3.2) och utföra avancerade analyser. Ibland kan uppgifter som har rensats från personuppgifter eller i vart fall rensats från direkta personuppgifter användas för analyserna, men ibland kan det vara just uppgifter om individer som är av intresse för forskning eller för att med stöd av de nya tekniska möjligheterna kunna förbättra för den enskilda individen ifråga. Vi återkommer till vissa av dessa frågeställningar i kapitel 7.8.

7.3 Teknikutvecklingen

7.3.1 Vårt uppdrag

Det ligger i vårt uppdrag att analysera den pågående digitala utvecklingen utifrån ett rättsligt perspektiv för att skapa en förståelse för vilka områden och företeelser som kommer att kräva lagstiftningsåtgärder så att förvaltningen ska kunna ta till vara digitaliseringens möjligheter. I våra direktiv beskrivs det också som angeläget att den offentliga förvaltningens verksamhet bygger på anpassade och långsiktigt hållbara rättsliga regler som ger stöd för digital utveckling,

samtidigt som de säkerställer behovet av informationssäkerhet och skydd av den personliga integriteten, liksom allmänhetens rätt till insyn och tillgång till god offentlig service.

Vi har inte möjlighet att inom ramen för utredningen lämna någon fullständig beskrivning av teknikutvecklingen. I det följande beskrivs emellertid kortfattat några områden för snabb teknikutveckling som är av betydelse för våra fortsatta rättsliga analyser, nämligen artificiell intelligens (AI) och maskininlärning, ”sakernas internet” (Internet of Things, IoT) och blockkedjeteknik. Teknikerna kan också i olika avseenden vara förenade med varandra.

7.3.2 Artificiell intelligens och maskininlärda algoritmer

Artificiell intelligens (AI) kan på en övergripande nivå beskrivas vara intelligens som uppvisas av maskiner. Det är också namnet på det forskningsområde som studerar hur man skapar datorer och datorprogram med intelligent beteende.[13] Inom AI finns flera olika delområden. Här bör bl.a. maskininlärning nämnas, där logiken inte längre är statisk, dvs. exakt programmerad på förhand, utan (förenklat beskrivet) tränas på stora datamängder med syfte att själv förstå samband mellan datapunkter. Allteftersom processorkraften ökar kan allt mer komplexa tillämpningar göras med artificiell intelligens. Vi återkommer i kapitel 7.8 till hur AI-system med maskininlärda algoritmer kan användas, bl.a. för att på nytt sätt analysera och bearbeta stora datamängder.

Vid tillämpning av AI och maskininlärda algoritmer kan vad som i kapitel 7.4.1 beskrivs vara olika former av indata hanteras i stor mängd och i många lager. Det kan röra sig om att det beslutsunderlag som processas och bedöms kan innehålla långt fler uppgifter (data) än vad en mänsklig handläggare kan hantera. Området för system som hanterar många lager av indata, ibland upp till miljontals datapunkter, och som med hjälp av maskininlärning uppdaterar sina algoritmer, benämns djupinlärning.[14]

Flera bakomliggande faktorer har samverkat för att utvecklingstakten inom AI nu ökat högst påtagligt. Förutom forskning har

[13] https://sv.wikipedia.org/wiki/Artificiell_intelligens
[14] Systemen i sig benämns neurala nätverk.

många yttre förhållanden möjliggjort framstegen, exempelvis tillgång till större beräkningskraft, större lagringsutrymmen och större datamängder. Framför allt har tillgången till mera data varit avgörande för utvecklingen av många tillämpningar. [15]

Kartläggningsarbetet visar att offentlig förvaltning i flera avseenden står i begrepp att använda AI i sin verksamhet. Tekniken kan användas t.ex. i form av en chatbot (dialogrobot) för att ge service till allmänheten genom fråga-svar-funktioner på en myndighets webbplats. AI har också potential att ge stor nytta om tekniken används vid urval eller som beslutsunderlag eller beslutsstöd vid ärendehandläggning eller faktiskt handlande. Det kan t.ex. röra sig om kvalificerade beslutsstöd vid diagnosticering inom sjukvården, stöd för korrekta utbetalningar från välfärdssystemen eller stöd i den brottsbekämpande verksamheten. Det synes också förekomma att myndigheter använder eller planerar att använda denna teknik för att fatta helt automatiserade beslut vid ärendehandläggning.

Med maskininlärda algoritmer tillkommer ett moment som inte motsvaras av programmering av traditionella algoritmer. För rättssäkra förfaranden krävs nämligen att en maskininlärd algoritm under en period *tränas*, innan den tas i drift för att leverera antingen beslut eller beslutsunderlag. Vi återkommer bl.a. i kapitel 7.8 till vilka ytterligare rättsliga dimensioner som den nya tekniken för med sig. Det förtjänar också att framhållas att det nu inte finns någon teknik för s.k. generell artificiell intelligens eller ”superintelligens” som klarar av att utföra vilken intellektuell uppgift som helst.

7.3.3 Sakernas internet

Med ”sakernas internet” (Internet of Things, IoT) menas föremål som har försetts med inbyggd teknik som sensorer, programvara och internetuppkoppling vilket gör att sakerna kan kopplas samman fysiskt eller via trådlösa nätverk med andra föremål eller system för att utbyta data.

Användning av uppkopplade föremål blir allt vanligare inom det offentliga. Det kan röra sig om digitala tekniker i äldrevården, exempelvis blöjor med fuktsensorer. Det kan också röra sig om sensorer som mäter luftkvalitet eller kartlägger rörelsemönster i stadsmiljö. I

[15] Göran Lindsjö, a.a. s. 3 f.

regel samlar föremålen in data i realtid vilket också innebär att det offentliga, med stöd av dessa uppgifter, får möjlighet att vidta relevanta åtgärder i realtid. Äldre kan med hjälp av den beskrivna tekniken med fuktsensorer slippa få sin nattsömn störd i onödan. Uppgifter om vilken kvalitet luften håller skulle t.ex. kunna användas för beslut om att det vid vissa tidpunkter är förbjudet för dieselfordon att köra på vissa gator i staden, medan förbudet direkt hävs när luftkvaliteten visar sig vara bättre. Sakernas internet har också potential att förenkla myndigheters tillsynsverksamhet. Inom livsmedelsbranschen skulle t.ex. smarta kylskåp och elmätare automatiskt kunna förmedla temperaturuppgifter till relevant tillsynsmyndighet, som efter analys av informationen skulle kunna besluta att vidta åtgärder. Det krävs dock att det finns ett förtroende för tekniken och att uppgifterna är korrekta.

Förutom frågor om hur en förvaltning som är uppkopplad mot digitala föremål kan säkerställa insyn vid den verksamhet som bedrivs, väcks, i den mån informationen som samlas in omfattar personuppgifter, frågor om bl.a. skydd för personuppgifter och personlig integritet. Frågor om insynsmöjligheter analyseras närmare i kapitel 7.6 och 7.7.

7.3.4 Blockkedjeteknik

Under kartläggningen och i anledning av utredningens hearing har vi uppmärksammats särskilt på teknikutvecklingen avseende s.k. blockkedjor.[16] Tekniken nämns ofta i samband med framtida betalningslösningar. Den första tillämpningen av blockkedjetekniken utgör också basen för den elektroniska valutan bitcoin. Blockkedjetekniken omtalas också i termer av att göra det möjligt att säkerställa att ett dokument inte förvanskats. Detta bör enligt vår bedömning vara av intresse för den digitala förvaltningen, både vid ärendehandläggning och i administrativ verksamhet.

Blockkedjetekniken kombinerar kända tekniska byggstenar från datavetenskap och kryptografi på ett nytt sätt. Förenklat beskrivet fungerar en blockkedja så att ett digitalt informationsinnehåll, t.ex. ett elektroniskt dokument, ges en unik kod (ett s.k. hashvärde) med

[16] Inte sällan används det engelska uttrycket Blockchain.

hjälp av en kryptografisk algoritm.[17] Det ursprungliga dokumentet kan bevaras i ett exemplar hos innehavaren samtidigt som denna unika kod (hashvärdet) som representerar data sparas och förmedlas vidare i en blockkedja. Koderna aggregeras matematiskt ihop i block som länkas samman i en kedja där efterföljande block matematiskt knyts ihop med den unika koden (hashvärdet) från det föregående blocket. Det blir därför omöjligt att lägga in ny information i tidigare block i kedjan utan att alla de efterföljande länkade blocken också ändras. Tekniken bygger även på att blockkedjan utgör en ”distribuerad bokföring” som är just distribuerad och kontrolleras på många platser (hos alla deltagande intressenter). En tillförlitlighet skapas genom att integriteten på den matematiskt länkade kedjan måste godkännas och kontrolleras i en vidare krets än hos en enstaka aktör om t.ex. nya tillägg ska göras.

Med blockkedjetekniken skapas även nya möjligheter till hantering och spårbarhet av original i digitala miljöer. Enligt vad som har uppgetts för oss kan en applikation använda en blockkedja för att lagra referenser till en ursprungsfil, lagra vem som är nuvarande ägare av den samt kontrollera alla förändringar av den. Förändringar kan t.ex. vara tillägg, makulering eller överlåtelse till ny innehavare.

Den teknik som beskrivits för oss innebär att alla som har tillgång till blockkedjan och får en kopia av ursprungsfilen, liksom ägarens unika kod, kan kontrollera och verifiera original och innehavare om eller när sådan kontroll efterfrågas. Tekniken medger däremot inte att det genom dessa unika koder går att återskapa innehållet i själva dokumentet. Det är med andra ord bara innehavaren av den ursprungliga filen med informationsinnehåll som kan läsa eller sprida innehållet i dokumentet.

De befintliga lösningar med användning av blockkedjeteknik som vi nu har fått beskrivna för oss innefattar också en digital underskrift med e-legitimation eller motsvarande för att verifiera kopplingen till den fysiska person som är utställaren av dokumentet. Detta bl.a. med tanke på att det straffrättsliga skyddet för urkunder ska tas till vara. Vid en internationell utblick förefaller också tekniken med blockkedjor i förening med biometriska förfaranden för att säkerställa koppling till fysisk person vara föremål för undersökning.

[17] Till exempel SHA-256. Den unika koden har också beskrivits som att varje dokument ges ett unikt digitalt fingeravtryck, se Lantmäteriets rapport *Framtidens husköp i blockkedjan* på www.lantmateriet.se/contentassets/6874bc3048ab42d6955e0f5dd9a84dcf/blockkedjan-framtidens-huskop.pdf

Vi återkommer till användningen av blockkedjeteknik främst i kapitel 11.6.1, där digitala avtal behandlas, och i kapitel 12, där bl.a. former för informationshantering i ärendeprocesser diskuteras.

7.4 Särskilt om automation av ärendehantering

7.4.1 Ärendeprocessen

I det förevarande kapitel 7 om automation i förvaltningen behandlas som framgått inte bara frågor som rör myndigheternas ärenden i förvaltningsrättslig mening. En betydande del av myndigheternas verksamhet cirkulerar emellertid kring ärendehandläggning och ärendehantering, varför det finns anledning att här uppehålla sig vid ärendeprocessen.

Ordet ”ärende” saknar en formell definition inom förvaltningsrätten. Under kartläggningen har framkommit att termen fortfarande, och kanske i ökad grad genom digitaliseringen, utgör en källa till missförstånd mellan olika yrkesgrupper. En registrator, en handläggare och en systemvetare menar ofta olika saker när de talar om ”ärenden”.

Enligt förvaltningsrättslig praxis anses ett typiskt myndighetsärende omfatta en kedja av aktiviteter som utmynnar i ett beslut med någon form av rättsverkan mot den som är part i ärendet. Även förvaltningslagens inriktning på att värna om den enskildes rättssäkerhet talar för ett sådant synsätt. Det är emellertid tydligt att gränsen mellan vad som är ärenden och vad som är annan förvaltningsverksamhet i viss mån är flytande.[18] Gränserna för vad som utgör ett specifikt ärende kan också behöva omprövas när nya möjligheter till informationshantering står till buds och ett specifikt ställningstagande hamnar i ett större sammanhang, dvs. sätts i en större kontext i en digitalt hanterad ärendeprocess jämfört med traditionell pappersaktshantering. Från den enskildes synpunkt kan det ”ärende” som privatpersonen eller företagaren önskar få behandlat vid en eller flera myndigheter också vara bredare än vad som avhandlas i ett enskilt beslut.[19] Digitaliseringen medför också behov

[18] Trygve Hellners och Göran Malmqvist, *Förvaltningslagen med kommentarer*, Norstedts Juridik, 2010, s. 38 f.
[19] E-delegationens slutbetänkande *En förvaltning som håller ihop* (SOU 2015:66), bl.a. i betänkandets bilaga 6.

av att reflektera särskilt över tidpunkten för när ett förvaltningsrättsligt ärende anses inlett (se vidare kapitel 8).

En del av svårigheten att definiera ordet ”ärende” består av att det används för att beteckna både de aktiviteter som utförs (själva ärendeflödet eller ärendeprocessen) och den dokumentation som uppstår till följd av aktiviteterna. Det finns dock anledning att skilja mellan ärendeprocessen och dokumentationen.[20]

En ärendeprocess i en digital miljö kan beskrivas som att ett visst beslutsunderlag, t.ex. uppgifter i en individuell ansökan (vanligen betecknade indata) matas in i ett it-system som styrs av datorprogram. Med ett datorprogram förstås en eller en serie av algoritmer som är kodade, dvs. funktioner för att visualisera det problem som algoritmen eller algoritmerna har löst och andra styrfunktioner för datorn. En algoritm är enligt en klassisk definition en noggrann plan eller metod för att stegvis göra något.[21]

Som framgår närmare i kapitel 8.2 kan vi å ena sidan skönja ett ökat intresse av att enskilda har kontroll över information som rör dem (ibland används begreppet ”My data” i detta sammanhang). Å andra sidan ser vi tendenser att vilja minska kraven på att den enskilde själv behöver lämna in olika uppgifter till myndigheter som beslutsunderlag. Detta dels av intresset att ge service till den enskilde (principen om ”en uppgift en gång”), dels av intresset att beslutsunderlag ska innehålla uppgifter av bästa möjliga kvalitet (genom att hämtas direkt från den ”bästa källan”). Att låta uppgifter av bästa möjliga kvalitet utgöra underlaget kan sägas vara en förutsättning för, eller i vart fall underlätta, fortsatt automatiserat förfarande vid ärendehandläggning och beslutsfattande.

Digitaliseringen och den ökade graden av automation kommer med andra ord att föra med sig att beslutsunderlag i minskad grad kommer att avse uppgifter som den enskilde själv har angett i ansöknings- eller anmälningsformulär. I ökad grad kommer i stället beslutsunderlaget att inhämtas från andra databaser som anropas och, i fall det finns, läser eller inhämtar sådant underlag (ytterligare indata). Det kan röra sig om anrop till andra databaser inom en myndighet eller externa databaser, tillgängliga via internet eller genom särskilda åtkomstmöjligheter. Tekniskt kan information

[20] Se även Johan Eriksson, *Öppna myndigheten, information och ärenden i e-förvaltningen*, SKL Kommentus AB 2014.
[21] www.csc.kth.se/utbildning/kth/kurser/DD1340/inda09/algorithms/algoritmer/

finnas även i andra typer av digitala källor än databaser, t.ex. i filer eller sensorsystem. Vi återkommer till ytterligare överväganden med anledning av den förskjutning avseende hur beslutsunderlag inhämtas som här kort beskrivits, bl.a. i kapitel 7.6.3.

När det sammantagna beslutsunderlaget, vare sig det inhämtats från den enskilde eller från andra källor, har processats, genereras ett beslut eller i andra fall kanske snarare ett beslutsstöd (utdata).

7.4.2 Dokumentation

Krav på dokumentation av beslutsunderlag finns bl.a. i förvaltningslagen (se kapitel 7.6.2.). Noterbart är dock de pågående förändringar i förvaltningens informationsförsörjning för att nå digitaliseringens fulla potential som kortfattat har beskrivits i det föregående avsnittet. Som framgått är det alltså inte givet att digitalisering av ett förfarande innebär att den digitala informationsförsörjningen helt kommer att motsvara t.ex. en pappersbaserad anmälan eller ansökan med uppgifter som lämnas av den enskilde. Vi ser i stället att graden av inhämtande av beslutsunderlag från andra digitala källor kan förutses öka. En särskild bestämmelse om dokumentation avseende beslutsunderlag som inhämtas från andra databaser finns i 4 kap. 3 § offentlighets- och sekretesslagen (2009:400). I kapitel 7.6.3 går vi närmare in på denna bestämmelse.

Ytterligare en reflektion kring vilka förändringar som digitaliseringen av förvaltningen för med sig är att det inte alltid är de uppgifter som i pappersmiljön har dokumenterats på särskilda handlingar som efterfrågas som beslutsunderlag när nya former för informationshantering övervägs. Det kan i stället vara andra uppgifter eller andra typer av uppgifter som nu får betydelse. Snarare än ett visst dokument kanske det är en enstaka uppgift, eller i stället en uppgift om att ett visst processteg har tagits, som är av intresse för en myndighets fortsatta åtgärder. Den förskjutningen får betydelse även ur ett rättsligt perspektiv. Vi återkommer till frågor om vilken rättsutveckling som kan behövas i anledning av detta, bl.a. i kapitel 12 när det gäller hur processer är reglerade.

Utöver beslutsunderlaget i ett specifikt ärende tillkommer i den digitala miljön ett antal dokument eller informationsbärare som saknar motsvarighet i den analoga miljön. Dessa typer av dokument

förhåller sig inte heller direkt till det enskilda ärendet.[22] Framtagande av algoritmer och anknytande datorprogram inleds vanligen med en kravspecifikation från beställaren, innefattande s.k. verksamhetsregler bestående av dels rättsregler, dels andra krav på användning av standarder och dylikt som ska följas, utöver den tekniska uppgift som ska lösas. Tekniska designdokument kan därefter tas fram med dels beskrivning av idéer för t.ex. problemlösning i form av algoritmer, dels hur dessa ska omsättas i programkod (ibland beskrivs även t.ex. val av programspråk). Det förekommer dock att dessa typer av designdokument saknas vid s.k. agil utveckling.[23] Genom kodning översätts algoritmen till ett givet programspråk och datorprogrammet tar sin form. Datorprogrammet, innefattande bl.a. de algoritmer som ingår, kan därmed beskrivas vara en dokumentation i sig.[24] Särskilda dokument som beskriver hur implementationen i algoritmer och datorprogram gått till, dvs. en särskild dokumentation med beskrivning av vad som faktiskt blev gjort, förekommer i varierad grad.

När det inledningsvis beskrivna beslutsunderlaget har processats och utmynnat i ett beslut ska detta beslut dokumenteras på särskilt sätt enligt författningskrav (se bl.a. kapitel 7.6.2), medan det däremot verkar finnas få rättsregler som ställer särskilda krav på dokumentationen avseende beslutsstöd (se dock kapitel 7.6.3 om krav på registrering och dokumentation av allmän handling i offentlighets- och sekretesslagen och arkivregleringen).

[22] Jfr förslag till skyldighet att hålla systemdokumentation tillgänglig för allmänheten i Datalagskommitténs betänkande *Integritet Offentlighet Kommunikationsteknik* (SOU 1997:39), s. 569 f.

[23] Agil systemutveckling är ett samlingsnamn för ett antal systemutvecklingsmetoder som kan användas vid programvaruutveckling, även kallade lättrörliga metoder eller iterativa metoder. Det engelska ordet ”agile” betyder smidig, vig, lättrörlig.

[24] Med ett datorprogram förstås, här enkelt beskrivet, en eller en serie av algoritmer, funktioner för att visualisera det problem som algoritmen eller algoritmerna har löst och andra styrfunktioner för datorn.

7.5 Rättssäkra automatiserade förfaranden i en öppen digital förvaltning

7.5.1 Rättsutveckling i takt med samhälls- och teknikutveckling

I kapitel 4 har vi konstaterat att rättssäkerheten kan stärkas med digitala medel. Vi har också tagit vår utgångspunkt i att god offentlighetsstruktur är en nödvändig grund för en öppen digital förvaltning, liksom att god informationssäkerhet krävs för att möta nya risker som digitaliseringen för med sig. Där har vi också översiktligt beskrivit att lagstiftningen behöver stå i samklang med den önskade utvecklingen och att såväl reglering om skydd för personuppgifter som sekretessreglering kan behöva anpassas.

Men hur ska förvaltningen i sin helhet, dvs. såväl tillämpande myndigheter som lagstiftande organ, gå till väga för att i samverkan med varandra åstadkomma rättssäkra automatiserade förfaranden i en öppen digital förvaltning? Vi gör inte anspråk på att inom ramen för denna utredning kunna komma med fullständiga svar på den frågan utifrån alla tänkbara situationer som kan uppstå eller kommer att uppstå när förvaltningen i olika avseenden övergår från manuella förfaranden till helt eller delvis automatiserade sådana. Vi strävar emellertid mot att både i de överväganden vi gör och i samband med att vi motiverar våra förslag till författningsändringar metodmässigt beskriva och bedöma behovet av rättsutveckling i takt med den teknik- och samhällsutveckling vi ser. Vår förhoppning är att den ansatsen ska kunna underlätta vid de överväganden som behöver göras även efter utredningens arbete och vara till nytta även i samband med fortsatt rättsutveckling.

Inledningsvis vill vi här belysa att vissa risker som förvaltningens automationsåtgärder kan medföra behöver adresseras och omhändertas ur ett rättsligt perspektiv så att de fördelar, även ur rättssäkerhetssynpunkt, som dessa automationsåtgärder för med sig kan tas till vara. I följande avsnitt (kapitel 7.6–7.9) belyser vi närmare dels de behov av författningsändringar som vi ser som nödvändiga i ett första steg, dels ytterligare åtgärder för att åstadkomma rättssäkra automatiserade förfaranden i en öppen digital förvaltning.

7.5.2 Omhändertagande av risker för rättsosäkerhet

Översättning av rättsregler till algoritmer eller datorprogram

Automation i samband med myndigheters ärendehantering kräver i hög grad ännu mänskliga direktiv i bemärkelsen att det är människor som, åtminstone initialt, i olika avseenden genom traditionell programmering styr hur datorerna ska fungera. För att möjliggöra ett automatiserat beslutsfattande krävs exempelvis att tjänstemän vid myndigheten, eller upphandlade konsulter, utifrån gällande författningar och andra styrdokument utformar en eller flera algoritmer som programkod. Den programmeringen föregås alltså av eller innefattar en översättning av rättskällor och, i varierad grad beroende på förhållandena, även annat underlag. Vid en sådan översättning tolkas författningstext, förarbeten, rättspraxis och doktrin och sätts samman till närmare regler som kan programmeras.

Datorrelaterad regelutformning i betydelsen omvandling av rättsregler till algoritmer med anknytande datorprogram är inte en nyhet i förvaltningen,[25] men fortfarande ett högst aktuellt exempel på när automationen riskerar att medföra rättsosäkerhet. Om den lagstiftning som ska tillämpas vid helt eller delvis automatiserat beslutsfattande är vag eller oprecis kommer en hög grad av utfyllnad att äga rum vid översättningen till programkod. Det innebär att det, i vart fall när det gäller hittills använd teknik, blir fråga om en fixering eller likriktning genom datorrelaterad reglering i stället för genom rättsregler.

Det har diskuterats om de datorprogram som här är aktuella därför borde ha en särskild förvaltningsrättslig status i form av förvaltningsbeslut som kan överklagas eller vara inordnade i normgivningshierarkin. De algoritmer eller datorprogram som används i förvaltningen vid helt eller delvis automatiserat beslutsfattande har emellertid såvitt känt för utredningen inte vid något tillfälle hanterats som sådana normer som följer av bemyndiganden och som ska kungöras eller publiceras i myndigheternas författningssamlingar. Den process som utförs när rättsreglerna ska tolkas och konkretiseras till algoritmer eller datorprogram behöver dock uppmärk-

[25] Se vidare t.ex. Magnusson Sjöberg, Cecilia, *Rättsautomation – Särskilt om statsförvaltningens datorisering*. Norstedts Juridik, 1992.

sammas i syfte att minimera risker för att regeringsformens bestämmelser om normgivningskompetens (se 8 kap. regeringsformen) träds för när i den processen.[26]

Nu står ny teknik som ovan beskrivits redan för dörren. Här avses närmast den form av artificiell intelligens som består av självlärande system. Både traditionellt programmerade algoritmer och maskininlärda sådana behöver därför hållas i åtanke vid våra fortsatta överväganden.

Möjligheter och utmaningar

Automatiserade förfaranden vid ärendehandläggning och beslutsfattande innebär inte enbart risker ur rättssäkerhetssynpunkt. I flera avseenden kan automatiserade förfaranden i stället skapa möjlighet till ökad rättssäkerhet, främst ur perspektivet förutsebarhet vid tillämpningen så till vida att ökad enhetlighet uppnås. Med automationen kan t.ex. risker för mänsklig godtycklighet undanröjas, liksom risker för att det inom en myndighet växer fram olika lokala kulturer där utfallen i besluten varierar beroende på av vem eller var inom organisationen de har fattats. På en övergripande nivå leder automatiserade förfaranden därför generellt sett till en mer likställd hantering jämfört med en manuell hantering av många olika handläggare vid en myndighet. Därför medför automationen i det avseendet en stärkt rättssäkerhet. Att automation medför snabbare förfaranden bidrar även detta till ökad rättssäkerhet för den enskilde.

Ett helt automatiserat beslutsfattande har såvitt känt för utredningen hittills främst kommit i fråga inom områden där den materiella rätten inte lämnar särskilt stort utrymme för bedömningar vid beslutsfattandet. En förklaring till detta är att de algoritmer som hittills används i svensk förvaltning till sin natur är deterministiska, dvs. de lämnar inte något utrymme för skönsmässiga bedömningar. Till exempel kan här nämnas beslutsfattande inom tandvårds- eller föräldrapenningsområdena där utfallet av beslut i princip inte skulle variera om besluten i stället hade fattats av mänskliga handläggare.

Automation inom områden där gällande rätt lämnar ett påtagligt utrymme för skönsmässighet vid beslutsfattande skulle emellertid i efterhand kunna visa sig vara till nackdel för en enskild, t.ex. om

[26] A.a.

denne hade kunnat åberopa vissa särskilda omständigheter vilka inte kunde beaktas av den statiska algoritmen. Om bedömningsutrymmet i den materiella rätten inte kan användas för flexibla bedömningar inom ramen för ett automatiserat förfarande riskerar därför utfallet av ett individuellt beslut att bli mindre rättssäkert trots den generellt sett ökade likställigheten. Den nu beskrivna risken för kvalitetsbrister i beslut som fattas automatiserat har adresserats på olika sätt i de förfaranden som hittills automatiserats i förvaltningen. I förordningen (2001:650) om vägtrafikregister finns exempelvis särskilda regler om omprövning av beslut som har fattats automatiserat.[27] I kapitel 7.9.1 belyser vi närmare vilka överväganden om anpassning av materiell rätt som vi bedömer bör göras vid övergång från manuella till automatiserade förfaranden, i första hand avseende beslutsfattande.

Användandet av ny teknik som t.ex. AI-system med maskininlärda algoritmer kan i framtiden komma att undanröja vissa av de ovan beskrivna riskerna för rättsosäkerhet vid tillämpning av automatiserat beslutsfattande, främst risken för att inte individuella faktorer kan beaktas vid ett enskilt beslut. När sådan teknik kommer att användas medför det emellertid också att nya typer av risker behöver hanteras för att rättssäkra förfaranden ska kunna garanteras. I detta sammanhang diskuteras inte minst risken för att maskininlärda algoritmer ”smittas” med felkällor eller felaktiga utgångspunkter, med risk för såväl rättsosäkra som diskriminerande förfaranden.[28] Även risker för att algoritmerna medvetet manipuleras för att orsaka ekonomisk eller personlig skada behöver beaktas.[29]

I takt med att förvaltningen tar i bruk allt mer tekniskt avancerade modeller för analys och stöd för mänskliga beslut kommer också frågan om ansvarstagande att behöva belysas, inte minst om eller när beslutsstöden blir så tekniskt avancerade att det snarare är ansvaret för funktionen i de algoritmer eller datorprogram som används som behöver diskuteras, än ansvaret för de enskilda besluten där de automatiskt genererade beslutsunderlagen används.

[27] 18 kap. 5 och6 §§ förordningen om vägtrafikregister (2001:650).
[28] Se Joyce Chou m.fl., *How to recognize exclusion in AI*, Microsoft 2017.
[29] Se Daniel Klinedinst m.fl., *2017 Emerging Technology Domains Risk Survey*, CMU/SEI-2017-TR-008, Software engineering institute, Carnegie Mellon University, October 2017, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2017_005_001_505319.pdf

De närmare åtgärder som av informationssäkerhetsskäl[30] behöver vidtas för att möjliggöra förvaltningens användning av den nya tekniken belyses inte närmare inom ramen för denna rättsligt orienterade utredning, men vikten av ett parallellt arbete med informationssäkerhet vid överväganden om ökad grad av automation i förvaltningen behöver framhållas. Vi belyser också frågor om de rättsliga förutsättningarna för en god informationssäkerhet i kapitel 9.

Säkerställande av möjligheter till insyn är dock enligt vår bedömning, ur rättsligt perspektiv, en av de grundläggande förutsättningarna för att förvaltningen ska kunna hantera rättsliga utmaningar i samband med automationsåtgärder och också kunna visa för allmänheten att de risker som finns tas om hand. På det sättet utgör god offentlighetsstruktur genom säkerställande av insynsmöjligheter en grundläggande förutsättning för att säkerställa rättssäkra automatiserade förfaranden inom förvaltningen.

7.6 Gällande rätt om insyn i algoritmer och beslutsunderlag

7.6.1 Dataskyddsförordningen

Automatiserat individuellt beslutsfattande, inbegripet profilering

Enligt dataskyddsförordningen har den enskilde rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, om beslutet kan ha rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar honom eller henne.[31] Sådant automatiserat beslutsfattande kan emellertid vara tillåtet, t.ex. enligt unionsrätten eller nationell rätt som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen.[32]

Profilering innebär varje form av automatisk behandling av personuppgifter när uppgifterna används för att bedöma vissa personliga egenskaper, i synnerhet för att analysera eller förutsäga

[30] För informationssäkerhet som avser digital information används ibland begreppet cybersäkerhet. Cybersäkerhetsbegreppet är vanligt förekommande i en internationell kontext. Här använder vi dock främst begreppet informationssäkerhet.
[31] Artikel 22.1, se även skäl 71.
[32] Artikel 22.2.b.

personens arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.[33]

Automatiserade beslut kan fattas med eller utan profilering. Omvänt kan profilering användas utan att det leder till ett automatiserat beslut. Ett beslut kan också grundas på profilering utan att beslutet enbart är baserat på automatiserad behandling, dvs. ett delvis automatiserat beslutsfattande.

Rättsliga frågor om innebörden av bestämmelsen om automatiserat beslutsfattande har i varierande utsträckning diskuterats sedan det tidigare dataskyddsdirektivet från 1995 trädde i kraft.[34] Diskussionerna har nu förts med förnyat intresse, bl.a. mot bakgrund av de sanktioner som kan följa om personuppgifter behandlas i strid med dataskyddsförordningen.

En av de frågor som har diskuterats är om sådana automatiserade processer som resulterar i ett stöd för beslut i individuella fall men inte genererar ett faktiskt beslut, med andra ord ett delvis men inte helt automatiserat beslutsfattande, faller utanför de ovan nämnda specifika krav som förordningen ställer upp beträffande automatiserade beslut. Det förefaller som att det finns få avgöranden i europeisk domstolspraxis där dessa frågor har belysts eller prövats i domstolar runt om i Europa trots att dataskyddsdirektivet varit i kraft i över 20 år.[35]

Mot den beskrivna bakgrunden är det välkommet att den s.k. artikel 29-gruppen[36] nu lämnat en särskild vägledning om automatiserat individuellt beslutsfattande, inbegripet profilering. I vägledningen anges att med beslut som enbart grundas på automatiserad behandling avses att det inte finns någon mänsklig inblandning i

[33] Artikel 4.4, se även skäl 72. Se även information på Datainspektionens webbplats www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/automatiserad-behandling/

[34] EG:s dataskyddsdirektiv (95/46), som genomförts i svensk rätt genom personuppgiftslagen (1998:204). Se även Wachter, Sandra m.fl., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, December 28, 2016. International Data Privacy Law, 2017. Available at SSRN: https://ssrn.com/abstract=2903469

[35] A.a.

[36] För att dataskyddsdirektivet (95/46) skulle tillämpas på ett enhetligt sätt i medlemsstaterna bildades den så kallade artikel 29-gruppen. Gruppen har fått sitt namn av artikel 29 i dataskyddsdirektivet och i artikel 30 finns bestämmelser om gruppens uppgifter.

beslutsprocessen. Den personuppgiftsansvarige[37] kan dock inte kringgå de särskilda reglerna om helt automatiserat individuellt beslutsfattande genom att införa en mänsklig inblandning som inte är meningsfull.[38]

I ett annex till vägledningen lämnar artikel 29-gruppen rekommendationer om hur personuppgiftsansvariga kan gå till väga för att möta de krav som följer av förordningen. I fråga om lämpliga skyddsåtgärder vid helt automatiserat beslutsfattande anges bl.a. att den personuppgiftsansvarige kan överväga regelbundna kvalitetskontroller av sina system för att säkerställa att enskilda behandlas rättvist och inte diskrimineras, tillsyn och tester av sina algoritmer som t.ex. utvecklats genom maskininlärning, särskilda åtgärder för dataminimering, anonymisering eller pseudonymisering av uppgifter och att den enskilde tillerkänns vägar för att uttrycka sin mening och få mänsklig kontakt.

I rekommendationerna anges också att personuppgiftsansvariga kan utforska möjligheter till certifieringsmekanismer eller uppförandekoder för tillsyn av processer som involverar maskininlärning, liksom översyn av etiska kommittéer eller liknande för att värdera risker och nytta med den profilering som avses.[39]

Information och tillgång till personuppgifter

Den personuppgiftsansvarige måste enligt dataskyddsförordningen informera de registrerade om att automatiserat beslutsfattande används. Denna *rätt till information* innebär bl.a. att den personuppgiftsansvarige ska lämna information om förekomsten av beslut som enbart grundas på automatiserad behandling. I dessa fall ska den personuppgiftsansvarige också lämna meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.[40]

En rättsfråga som diskuteras inom EU är vilka närmare explicita eller underförstådda krav förordningen egentligen ställer i fråga om

[37] Med personuppgiftsansvarig menas en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; se artikel 4.7 dataskyddsförordningen.
[38] Se artikel 29-gruppen, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 17 EN WP 251, Adopted on 3 October 2017 s. 9 f. om beslut som enbart grundas på automatiserad behandling.
[39] A.a. s. 30.
[40] Artikel 13.2.f och 14.2.g. Se även a.a. s. 23 f.

rätten för den enskilde att få en förklaring av ett individuellt beslut som fattats automatiserat. Vissa har menat att förordningens reglering medför en särskild rätt att få en förklaring av såväl det individuella beslutet som detaljer om det bakomliggande förfarande som lett fram till det, medan andra hävdar att enskilda enligt förordningen enbart har rätt att få övergripande information om logiken bakom besluten i generell bemärkelse.[41] Frågan har besvarats i linje med det sistnämnda alternativet av artikel 29-gruppen.[42]

Den enskilde har också bl.a. *rätt till tillgång* till personuppgifter och meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.[43] Rätten till tillgång är mycket snarlik den ovan beskrivna rätten till information, men en skillnad är att rätten till information ska tillgodoses innan en behandling av personuppgifter påbörjas medan rätten till tillgång ska mötas först efter den enskildes begäran. Även när det gäller rätten till tillgång har det förts diskussioner om hur långt denna rätt till tillgång egentligen sträcker sig, bl.a. när det gäller underliggande algoritmer och programkod, respektive hur den rättigheten förhåller sig till bl.a. immaterialrättslig skyddsreglering.[44]

Artikel 29-gruppen klargör i den ovan nämnda vägledningen att också rätten till tillgång innebär en mer övergripande rättighet, snarare än en rätt till en förklaring av ett specifikt beslut. Skälen i förordningen ger också uttryck för ett visst skydd för personuppgiftsansvariga vad gäller immateriella rättigheter eller affärshemligheter. Dessa rättigheter behöver dock sättas i förhållande till den aktuella kontexten och balanseras mot enskildas rätt till information.[45] Skyldigheten att ge den registrerade information om och tillgång till de personuppgifter som behandlas ska enligt förslaget till kompletterande dataskyddslag inte heller gälla personuppgifter som på grund av sekretess eller tystnadsplikt inte får lämnas ut till den registrerade.[46]

[41] Se Bryce Goodman och Seth Flaxman, *European Union regulations on algorithmic decision-making and a "right to explanation"*, augusti 2016, Oxford Internet Institute. Jfr Wachter, Sandra m.fl. a.a.
[42] A.a. s. 13 f.
[43] Artikel 13.2.f och14.2.g.
[44] Artikel 15.1.h och skäl 63.
[45] A.a. s. 24.
[46] Se förslag till 5 kap. 1 § lagen med kompletterande bestämmelser till EU:s dataskyddsförordning, *Ny dataskyddslag*, prop. 2017/18:105.

När det gäller *rätten till information* rekommenderar artikel 29-gruppen att den personuppgiftsansvarige kan överväga bl.a. visualisering eller ikoner som informerar den enskilde om profilering och automatiserat beslutsfattande. Meningsfull information om logiken som är involverad bör i de flesta fall innebära att den personuppgiftsansvarige tillhandahåller information om vilka kategorier av uppgifter som används i en profil, källan till de uppgiftsmängderna, hur profilen är uppbyggd (inklusive statistik som används i profilen), varför profilen är relevant för den automatiserade beslutsprocessen och hur den används för ett beslut som rör den enskilde.[47]

När det gäller *rätten till tillgång* rekommenderar artikel 29-gruppen bl.a. att det generellt sett kommer att vara mer relevant att lämna information om vilka kategorier av uppgifter som har använts eller kommer att användas vid profileringen eller beslutsprocessen och varför dessa tillämpas, än att tillhandahålla en komplex matematisk förklaring om hur algoritmer eller maskininlärning fungerar. Det sistnämnda bör dock också tillhandahållas om det är nödvändigt för att experter närmare ska kunna verifiera hur processen för beslutsfattande fungerar. Personuppgiftsansvariga kan vidare vilja överväga att implementera mekanismer som möjliggör för enskilda att kontrollera sin profil, inklusive detaljer om uppgifter och källor som använts för att utveckla den.[48]

Övrig dataskyddsreglering

Utöver de bestämmelser som presenterats ovan gäller även de generella reglerna i dataskyddsförordningen vid automatiserat beslutsfattande. Här kan bl.a. nämnas kraven på att behandlingen av personuppgifter ska vara laglig, korrekt och öppen,[49] att ändamålsbegränsningar ska beaktas,[50] principerna om dataminimering, korrekthet och lagringsminimering,[51] att rättslig grund krävs för behandling[52] och att laglig

[47] Se artikel 29-gruppen, a.a. s. 28.
[48] A.a. s. 29.
[49] Artikel 5.1.a.
[50] Artikel 5.1.b och 6.4.
[51] Artikel 5.1.c-e.
[52] Artikel 6.1, här framför allt c och e och förslag till 2 kap. 1 och2 §§ lagen med kompletterande bestämmelser till EU:s dataskyddsförordning, prop. 2017/18:105.

behandling av känsliga personuppgifter fordrar särskilt stöd,[53] rätten till rättelse, radering och begränsning av behandling,[54] rätten att göra invändning mot profilering,[55] vikten av att iaktta särskild restriktivitet när det gäller behandling av barns personuppgifter[56] och att konsekvensbedömning avseende dataskydd torde krävas vid varje form av automatiserat beslutsfattande, dvs. även när beslutsfattandet är delvis men inte helt automatiserat.[57]

Regeringen har vidare föreslagit att dataskyddsförordningen med vissa undantag ska gälla även utanför sitt egentliga tillämpningsområde, t.ex. i verksamhet som rör nationell säkerhet.[58]

Vid sidan av dataskyddsförordningen innehåller EU:s dataskyddsreform ett separat dataskyddsdirektiv som behandlar dataskyddet vid bl.a. brottsbekämpning, lagföring och straffverkställighet.[59] Direktivet innehåller reglering av samma eller liknande karaktär som dataskyddsförordningen men är anpassat för den särskilda verksamhet som bedrivs på området för brottsbekämpning och brottmålshantering. Utredningen om 2016 års dataskyddsdirektiv har föreslagit att direktivet i huvudsak ska genomföras i svensk rätt genom en ny ramlag, brottsdatalagen. Lagen kompletteras med en förordning som genomför vissa detaljbestämmelser i direktivet.[60] Utredningen har också föreslagit de anpassningar som krävs med anledning av ramlagen i de registerförfattningar som ingår i utredningens uppdrag, bl.a. polisdatalagen (2010:361). De särskilda registerförfattningarna på direktivets område föreslås gälla utöver brottsdatalagen. Det innebär att registerförfattningarna innehåller bestämmelser som är preciseringar, undantag eller avvikelser från bestämmelserna i brottsdata-

[53] Artikel 9 och förslag till 3 kap. 1 § lagen med kompletterande bestämmelser till EU:s dataskyddsförordning, a. prop.
[54] Artikel 16–18.
[55] Artikel 21.1.
[56] Skäl 38.
[57] Artikel 35.3.a och artikel 29-gruppen, a.a.s. 27.
[58] 1 kap. 2 § förslag till lag med kompletterande bestämmelser till EU:s dataskyddsförordning, a. prop.
[59] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (dataskyddsdirektivet).
[60] *Brottsdatalag* (SOU 2017:29).

lagen. Vidare innebär det att bestämmelserna i registerförfattningarna ska läsas tillsammans med regleringen i brottsdatalagen och tolkas i ljuset av denna reglering.[61]

I dataskyddsdirektivet på det brottsbekämpande området föreskrivs att det ska införas förbud mot automatiserade beslut, såvida inte sådana beslut är tillåtna enligt unionsrätten eller nationell rätt och det är föreskrivet lämpliga skyddsåtgärder för den enskilde.[62] Skyddsåtgärderna ska åtminstone ge den enskilde rätt till personlig kontakt med någon hos den personuppgiftsansvarige. Skyddsåtgärderna ska vidare innefatta särskild information till den registrerade och rätt till personlig kontakt för att möjliggöra för honom eller henne att framföra synpunkter, att få beslutet förklarat för sig och att överklaga beslutet. Automatiserade beslut får inte grundas på känsliga personuppgifter, om inte lämpliga skyddsåtgärder har vidtagits. Profilering som leder till diskriminering av fysiska personer på grundval av känsliga personuppgifter ska förbjudas.[63]

Utredningen om 2016 års dataskyddsdirektiv har anfört att det inom ramlagens tillämpningsområde i dag inte förekommer några automatiserade beslut, men att det med teknikutvecklingen inte kan uteslutas att det i framtiden kommer att finnas sådana. Den svenska ramlagen på direktivets område bör enligt utredningen innehålla en bestämmelse om automatiserade beslut eftersom direktivet sätter gränser för sådana beslut. Automatiserade beslut som enbart grundar sig på känsliga personuppgifter bör enligt utredningen förbjudas.[64]

Våra inledande överväganden

Som framgått ovan har det under lång tid förelegat en rättslig osäkerhet rörande dataskyddsregleringens bestämmelser om automatiserat beslutsfattande. Det är därför välkommet att artikel 29-gruppens vägledning klargör flera frågor inför att dataskyddsförordningen ska börja tillämpas. De rekommendationer som lämnas utöver vägledningen ger också en god bild över personuppgiftsansvarigas praktiska möjligheter att ordna sin personuppgiftsbehandling för att

[61] *Brottsdatalag – kompletterande lagstiftning* (SOU 2017:74), s. 328 f.
[62] Artikel 11 dataskyddsdirektivet.
[63] Skäl 38.
[64] 2 kap. 19 § förslag till brottsdatalag och SOU 2017:29 s. 287 f.

dels kunna följa förordningens krav, dels kunna visa att man följer dem. De rekommendationer som artikel 29-gruppen har lämnat är emellertid inte rättsligt bindande.

Det kvarstår vidare vissa frågor om hur den särskilda artikeln om automatiserat beslutsfattande ska tillämpas av svensk förvaltning. Det gäller t.ex. frågan om vad som i förordningens mening anses utgöra ett ”beslut”. Vad som utgör beslut enligt dataskyddsförordningen, med dess breda tillämpningsområde, är givetvis inte knutet till svensk förvaltningsrätt. Att i vart fall de slutliga beslut som fattas inom förvaltningen omfattas av begreppet ”beslut” bedömer vi stå klart. Vilka, om några, beslut under handläggningen som omfattas är däremot inte lika givet. Det är med andra ord oklart om förordningens särskilda artikel om automatiserat beslutsfattande ska tillämpas vid t.ex. förfaranden för automatiserat urval eller kontroll, med andra ord profilering, som inte renderar något slutligt beslut i förvaltningsrättslig mening.

Det är också oklart vilken räckvidd förordningens särskilda bestämmelse om automatiserat beslutsfattande har när personuppgifter i och för sig förekommer i samband med ett beslut som är slutligt, men där själva beslutsunderlaget utgörs av annan information än personuppgifter. Det kan t.ex. röra sig om ett beslut om fastighetstaxering som t.ex. innehåller personuppgifter i form av kontaktuppgifter och fastighetsbeteckning, men där uppgifterna som utgör beslutsunderlaget har ingen eller mycket liten koppling till den enskildes (dvs. den registrerades) personliga egenskaper eller förhållanden. Ett sådant, om än slutligt och automatiserat, beslut kan i vart fall inte sägas innefatta någon profilering. Den enskildes insynsintresse i fråga om den bakomliggande logik som har styrt beslutet kan dock vara lika stort oavsett om förordningens bestämmelse ska tillämpas eller inte. Frågan är emellertid om det insynsintresset tillgodoses med stöd av dataskyddsförordningen eller med stöd av annan nationell rätt.

Det finns också anledning att särskilt reflektera över räckvidden i dataskyddsförordningens bestämmelser. En central iakttagelse är att förordningens bestämmelser syftar till att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. De rättigheter till bl.a. insyn som stipuleras genom bestämmelserna om informationsskyldigheter och rätt till

tillgång till uppgifter tillerkänns därför enbart den eller de registrerade. Förordningen ger med andra ord inte stöd för en bredare insyn i hur förvaltningens verksamhet bedrivs. Möjligheter till insyn i förvaltningens verksamhet för journalistisk granskning, granskning av Riksrevisionen, Riksdagens ombudsmän (JO) och Justitiekanslern liksom allmänhetens möjligheter till insyn följer i stället av nationell rätt.[65]

Det står också klart att vid processer som inte innefattar behandling av personuppgifter blir förordningen inte tillämplig. Automatiserade förfaranden i förvaltningen som inte innefattar personuppgiftsbehandling kan t.ex. röra förvaltningsbeslut baserade på miljöinformation som varken direkt eller indirekt relaterar till någon enskild person. Inom exempelvis utvecklingsområdet ”smarta städer”[66] och samhällsbyggnadsprocessen torde det också komma att aktualiseras att myndigheter i sina automatiserade processer fattar förvaltningsrättsliga beslut baserat på data som inte relaterar till individer eller alls innefattar behandling av personuppgifter. Däremot är även den typ av beslut som rör stadens utformning och funktioner av påtaglig betydelse för utvecklingen av ett hållbart samhälle, och därmed också viktiga för många människor.

En utgångspunkt för utredningen är att den tekniska utvecklingen inom förvaltningen inte får leda till en försvagning av offentlighetsprincipen. Den utgångspunkten bottnar i tidigare gjorda rättspolitiska uttalanden.[67] Dataskyddsförordningens stärkta insynsmöjligheter för den enskilde som registrerats inverkar enligt oss inte på den utgångspunkten. Även allmänhetens insyn, dvs. möjligheten för alla och envar att få insyn i myndigheternas verksamhet behöver alltså fortsatt säkerställas och inte vara beroende av tekniken för informationshantering.[68]

[65] Artikel 85 och 86 dataskyddsförordningen.
[66] En smart och hållbar stad beskrivs bl.a. på www.smartastader.com vara en innovativ stad som använder informations- och kommunikationstekniker och andra medel för att förbättra livskvaliteten, effektiviteten hos stadsfunktioner och -tjänster och konkurrenskraften, samtidigt som den säkerställer att den uppfyller nuvarande och framtida generationers behov med hänsyn till ekonomiska, sociala och miljömässiga aspekter.
[67] Se bl.a. Offentlighets- och sekretesskommitténs delbetänkande *Ordning och reda bland allmänna handlingar* (SOU 2002:97), s. 94.
[68] Jfr även artikel 86 i dataskyddsförordningen.

7.6.2 Partsinsyn och förvaltningslagen

Partsinsyn

Den som är part i ett mål eller ärende hos en myndighet eller en domstol har en principiell rätt till partsinsyn i förfarandet och rätt att ta del av den information som tillförs målet eller ärendet under handläggningen. Myndigheter är i varierande utsträckning skyldiga att se till att en part får del av sådan information. Generella bestämmelser finns i förvaltningslagen.[69] Sekretess hindrar inte insyn från den som är part och som på grund av sin partsställning har rätt att ta del av handlingar och material i målet eller ärendet.[70] För att partens möjlighet till insyn enligt denna reglering ska gälla ska det emellertid vara fråga om uppgifter ”i” målet eller ärendet.[71] Insynen får bara begränsas under förutsättning att det av hänsyn till allmänt eller enskilt intresse är av synnerlig vikt att en sekretessbelagd uppgift i en handling i målet eller ärendet inte lämnas ut till parten. Sekretess hindrar dock aldrig en part från att ta del av en dom eller ett beslut i målet eller ärendet.

Förvaltningslagen om automatiserade beslut, dokumentation av beslutsunderlag och beslutsmotivering

I förvaltningslagen framgår det uttryckligen att ett beslut kan fattas automatiserat.[72] Det explicita författningsstödet är nytt i förhållande till 1986 års förvaltningslag. I propositionen med förslag till ny förvaltningslag konstaterade regeringen att automatiseringen av beslut under senare år kommit att bli en allt vanligare företeelse inom delar av den förvaltning som hanterar ett mycket stort antal ärenden årligen, t.ex. i Försäkringskassans verksamhet. Genom att det i förvaltningslagen slås fast att beslut kan fattas automatiserat tydliggörs att det inte behövs en reglering i en specialförfattning för att en

[69] 10 och 25 §§ förvaltningslagen. Se även t.ex. 10 och 12 §§ förvaltningsprocesslagen (1971:291) och 45 kap. 9 § rättegångsbalken som innehåller bestämmelser om partsinsyn.
[70] 10 kap. 3 § offentlighets- och sekretesslagen (2009:400).
[71] Eva Lenberg m.fl., Offentlighets- och sekretesslagen (12 maj 2017, Zeteo), kommentaren till 10 kap. 3 § offentlighets- och sekretesslagen.
[72] 28 § förvaltningslagen.

myndighet ska kunna använda denna beslutsform. Regeringen anförde vidare att regleringen därmed också skapar bättre förutsättningar för en fortsatt utveckling av den digitala förvaltningen.[73]

Utöver den nya regleringen om form för beslutsfattande, uppställer förvaltningslagen olika former av dokumentationskrav. Här bör särskilt nämnas kravet på anteckningar och andra typer av dokumentation när en myndighet får uppgifter på något annat sätt än genom en handling, om de kan ha betydelse för ett beslut i ärendet. Det ska framgå av dokumentationen när den har gjorts och av vem.[74] Det kan t.ex. vara fråga om information som någon ger muntligt eller som skaffas fram genom undersökningar eller besiktningar av personer, föremål, fastigheter eller miljöer.[75]

Det ovan beskrivna dokumentationskravet motiveras av att beslutsunderlaget i ett ärende måste vara komplett, identifierbart och lättillgängligt för att möta grundläggande krav på rättssäkerhet och effektivitet. En enskild ska genom att t.ex. använda sin rätt till partsinsyn kunna försäkra sig om att myndigheten inte bara har tagit ställning till allt material som har tillförts ett ärende utan att den också har bevarat det. För myndigheten är det viktigt att ha kontroll över beslutsunderlaget, bl.a. för att den ska kunna fullgöra sin kommunikationsskyldighet. Även utomstående som har bidragit med material måste kunna vara säkra på att materialet tagits om hand på ett korrekt sätt av myndigheten. Tillgång till allt material som har tillförts ett ärende är också en förutsättning för den prövning som en överinstans ska göra med anledning av ett överklagande av ett beslut eller för sådan tillsyn som utövas av t.ex. JO och Justitiekanslern.[76]

Här bör också nämnas att förvaltningslagen innehåller en bestämmelse med krav på en klargörande motivering av ett beslut som kan antas påverka någons situation på ett inte obetydligt sätt, om det inte är uppenbart obehövligt med sådan motivering.[77] Kravet på att en motivering av ett beslut ska vara klargörande innebär att en part ska ges möjlighet att förstå hur myndigheten har resonerat i det enskilda fallet.

---

[73] *En modern och rättssäker förvaltning - ny förvaltningslag*, prop. 2016/17:180, s. 179 f. Se även *Budgetpropositionen för 2018*, prop. 2017/18:1 Utgiftsområde 2 s. 94.
[74] 27 § förvaltningslagen.
[75] Prop. 2016/17:180 s. 314.
[76] A. prop. s. 174.
[77] 32 § förvaltningslagen.

Motiveringsskyldigheten innebär att myndigheten måste ange de skäl som har bestämt utgången i ärendet. Skälen måste presenteras på ett sådant sätt att de blir begripliga för den enskilde. Den klargörande motiveringen ska innehålla uppgifter om vilka föreskrifter som har tillämpats och vilka omständigheter som har varit avgörande för myndighetens ställningstagande. I beslutsmotiveringen ska alltså det författningsmässiga stödet för beslutet anges. Kravet på redovisning av omständigheter innebär ett krav på att redovisa vilka fakta som myndigheten har tillmätt betydelse och hur den har värderat dessa.

I förarbetena nämns bl.a. att motiveringsskyldigheten kan begränsas på grund av att motivering ibland är uppenbart obehövligt. Det kan t.ex. gälla när en myndighet meddelar ett beslut som helt tillgodoser den enskildes önskemål på grundval uteslutande av den enskildes egna uppgifter, och det inte finns någon enskild motpart som kan ha ett intresse av att ta del av en motivering för att överväga ett överklagande.[78] Vissa ytterligare undantag görs i frågan om när en motivering helt eller delvis får utelämnas, men som huvudregel ska en myndighet ändå kunna ge en motivering i efterhand om någon enskild begär det och det behövs för att han eller hon ska kunna ta till vara sin rätt.[79] Att skälen för ett avgörande ska framgå gäller också i dömande verksamhet.[80]

Våra inledande överväganden

Det saknas förarbetsuttalanden som anger hur bestämmelsen i förvaltningslagen om att beslut kan fattas automatiserat förhåller sig till dataskyddsförordningen. Mot bakgrund av regeringens tydliga avsikt att skapa bättre förutsättningar för en fortsatt utveckling av den digitala förvaltningen bedömer vi dock att det uttalade stödet för automatiserat beslutsfattande i förvaltningslagen som utgångspunkt borde innebära att automatiserat beslutsfattande inom förvaltningen även ska anses tillåtet enligt dataskyddsförordningen.[81]

[78] A. prop. s. 320 f.
[79] 32 § andra och tredje stycket förvaltningslagen.
[80] 17 kap. 7 § första stycket 5 och 30 kap. 5 § första stycket 5 rättegångsbalken, 30 § andra stycket förvaltningsprocesslagen och 28 § lagen (1996:242) om domstolsärenden.
[81] Här avses förhållandet till artikel 22.2.b i dataskyddsförordningen.

Några särskilda åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen med avseende på just automatiserade beslut har emellertid inte införts i förvaltningslagen.[82] Förvaltningslagen innehåller dock generellt tillämpliga bestämmelser om bl.a. rätt att lämna uppgifter muntligt i ett ärende, om det inte framstår som obehövligt, och bestämmelser om omprövning samt rätt att överklaga beslut.[83] I kapitel 7.9.1 återkommer vi till ytterligare överväganden om på vilket sätt reglering i den materiella rätt som ska tillämpas vid beslutsfattande kan inverka på frågan om det är tillåtet eller lämpligt att beslut fattas automatiserat.

Några ytterligare inledande reflektioner från vår sida är att förvaltningslagen varken kräver att datorprogram (inkluderande algoritmer) som används vid automatiserat beslutsfattande dokumenteras, tillförs beslutsunderlaget i de enskilda förvaltningsärenden där de kommer till användning eller framgår av beslutsmotiveringen. Dessa tillkommer i stället snarast som ett eget lager av funktionalitet mellan å ena sidan de författningar med anknytande källmaterial som tillämpas och å andra sidan det beslutsunderlag i form av fakta som har tillförts ärendet (se beskrivning i kapitel 7.4.2). I linje med detta tillerkänns inte part någon särskild rätt att få insyn i hur myndigheten använder bakomliggande algoritmer med anknytande datorprogram enligt den uttryckliga rätten till partsinsyn (jfr dock kapitel 7.6.3 om handlingsoffentlighet och våra där gjorda överväganden om datorprogram som allmän handling).

Vad som däremot kan utläsas av förvaltningslagen och dess förarbeten är vikten av ordning och reda när det gäller beslutsunderlag i enskilda fall, såväl när det gäller sakliga uppgifter som när det gäller möjlighet att spåra var de kommer ifrån. Detta framgår bl.a. genom en bestämmelse om att det ska framgå vem som har dokumenterat uppgifterna när en myndighet får uppgifter på något annat sätt än genom en handling.[84]

[82] Jfr artikel 22.2.b dataskyddsförordningen.
[83] 24 och 36–48 §§ förvaltningslagen.
[84] 27 § förvaltningslagen.

7.6.3 Handlingsoffentlighet och arkivlagstiftning

Vad utgör en allmän handling?

I såväl offentlighets- och sekretesslagen som arkivlagen (1990:782) finns regler om att myndigheterna på olika sätt ska registrera och beskriva sina allmänna handlingar.[85] Bestämmelsernas syfte är att garantera allmänhetens rätt att få tillgång till allmänna handlingar. För att offentlighetsprincipen praktiskt sett ska kunna fungera på det sätt som är avsett i tryckfrihetsförordningen har det ansetts nödvändigt att myndigheterna håller sina allmänna handlingar registrerade eller i vart fall så ordnade att det går att konstatera vilka allmänna handlingar som finns.[86]

Vad som är allmän handling framgår av 2 kap. tryckfrihetsförordningen.

Med *handling* förstås framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel.[87] Framställningar i skrift eller bild utgör handlingar i traditionell bemärkelse, dvs. framställningar som kan uppfattas visuellt utan tekniska hjälpmedel. Det är alltså fråga om alla former av pappersbaserade skriftliga uppteckningar, t.ex. tabeller, blanketter och protokoll, men även kartor, ritningar och olika slags bilder t.ex. fotografier eller röntgenbilder. En *upptagning* innebär att informationen i en framställning inte kan uppfattas eller förstås utan tekniskt hjälpmedel.

Handlingen är *allmän*, om den förvaras hos en myndighet och är inkommen till eller upprättad hos myndigheten.[88] Termen *förvaras* har i tryckfrihetsförordningens bemärkelse en betydelse som skiljer sig från ordets innebörd enligt vanligt språkbruk. Utgångspunkten är att handlingen ska finnas inom myndighetens lokaler, men exempelvis en handling i form av ett färdigt dokument som finns i en tjänstemans förvar utanför myndighetens väggar anses även den förvarad av myndigheten. För upptagningar gäller att de endast anses

[85] Se särskilt 4 kap. 2 § och 5 kap. 1 § offentlighets- och sekretesslagen, 6 § 2 arkivlagen, 6 kap. 5 § RA-FS 2008:4 och 5 kap. RA-FS 2009:1.
[86] Avsnittet bygger i stor utsträckning på Alf Bohlin, *Offentlighetsprincipen*, Norstedt Juridik, 2015, *Tsunamibanden* (SOU 2007:44), s. 83 f. och *Ordning och reda bland allmänna handlingar* (SOU 2002:97), s. 57 f.
[87] 2 kap. 3 § första stycket tryckfrihetsförordningen. Observera att ändringar i bl.a. 2 kap. tryckfrihetsförordningen föreslås i *Ändrade mediegrundlagar*, prop. 2017/18:49. Ändringarna innebär bl.a. ändrade beteckningar på lagrum.
[88] 2 kap. 6 § och 2 kap. 7 § första stycket tryckfrihetsförordningen.

förvarade av en myndighet om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. För sammanställning av uppgifter ur en upptagning för automatiserad behandling, där upptagningen utgör allmän handling, gäller därutöver inskränkningen att sammanställningen endast anses förvarad hos myndigheten om myndigheten kan göra den tillgänglig med rutinbetonade åtgärder.[89]

Genom formuleringen av sistnämnda inskränkning har lagstiftaren uttryckt att en så kallad *färdig elektronisk handling* anses förvarad hos myndigheten oavsett om den kan tas fram med rutinbetonade åtgärder eller om det krävs mer omfattande åtgärder. Med uttrycket färdig elektronisk handling avses sådana elektroniska handlingar där utställaren, myndigheten eller den som lämnat in handlingen till myndigheten, har gett dem ett bestämt, fixerat, innehåll som går att återskapa gång på gång. Som typiska exempel på sådana handlingar kan, förutom e-postmeddelanden, nämnas promemorior och protokoll i elektronisk form.

I förarbetena till lagändringen[90] anförde regeringen att det inte var tillfredsställande att en sådan handling skulle anses förvarad hos en myndighet endast om den kunde tas fram med rutinbetonade åtgärder. Det skulle i praktiken innebära att det kunde finnas färdiga elektroniska handlingar hos myndigheterna som inte rättsligt sett ansågs förvarade, och därför inte ansågs vara allmänna, därför att myndigheterna organiserat sina datasystem på sådant sätt att det inte gick att återfinna handlingen med rutinbetonade åtgärder. Detta ansågs av regeringen oacceptabelt från offentlighetssynpunkt. Om en färdig elektronisk handling ska anses förvarad hos en myndighet eller inte bör enligt förarbetsuttalandet i stället avgöras utifrån om den rent faktiskt är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar, oavsett om det krävs endast rutinbetonade åtgärder för att ta fram den eller mer omfattande insatser från myndighetens sida.

[89] 2 kap. 3 § andra stycket tryckfrihetsförordningen. Ytterligare en begränsning gäller för en elektronisk sammanställning innehållande personuppgifter, dvs. all slags information som direkt eller indirekt kan hänföras till en fysisk person. En sådan sammanställning anses inte alls förvarad hos myndigheten om myndigheten saknar befogenhet enligt lag eller förordning att göra den tillgänglig (2 kap. 3 § tredje stycket tryckfrihetsförordningen).
[90] *Offentlighetsprincipen och informationstekniken*, prop. 2001/02:70, s. 18 f.

Sammanställningar av uppgifter ur dataregister, som inte av utställaren getts en bestämd, fixerad form som kan återskapas gång på gång, är i stället ett typexempel på vad som inte brukar omfattas av begreppet färdiga elektroniska handlingar. Skyldigheten för myndigheter att tillhandahålla sådana sammanställningar bör enligt samma förarbetsuttalande även i fortsättningen begränsas utifrån vad som är möjligt att åstadkomma med rutinbetonade åtgärder.

För att en handling som anses förvarad hos en myndighet ska vara allmän fordras som nämnts att den antingen har inkommit till myndigheten eller upprättats där. En handling anses *inkommen* till en myndighet när den har anlänt till myndigheten eller kommit behörig befattningshavare till handa. I fråga om en upptagning gäller i stället att den anses inkommen när annan har gjort den tillgänglig för myndigheten på sätt som innebär att myndigheten kan ta del av den med tekniskt hjälpmedel.[91] Handlingar som utväxlas inom samma myndighet anses inte inkomna till myndigheten, om inte avsändande respektive mottagande organ utgörs av olika verksamhetsgrenar inom myndigheten och kan anses självständiga i förhållande till varandra.[92]

Även termen *upprättad* har i tryckfrihetsförordningen fått en innebörd som avviker något från vanligt språkbruk. En handling anses enligt tryckfrihetsförordningen upprättad först när den antingen expedierats eller när det ärende till vilket den hänför sig har slutbehandlats hos myndigheten. Hör inte handlingen till något visst ärende, anses den upprättad när den har justerats av myndigheten eller på annat sätt färdigställts.[93] Innan sådana handlingar föreligger i sitt definitiva skick utgör de alltså myndighetsinternt material. För diarier, journaler och sådana register eller andra förteckningar som förs löpande gäller däremot att de anses upprättade redan när de har färdigställts för anteckning eller införing.[94] Gemensamt för dessa handlingar är därför att de blir allmänna på ett mycket tidigt stadium, under förutsättning att de också anses förvarade hos myndigheten. E-postloggar har t.ex. ansetts vara sådana handlingar som utgör denna typ av register.[95]

[91] 2 kap. 6 § tryckfrihetsförordningen.
[92] 2 kap. 8 § tryckfrihetsförordningen.
[93] 2 kap. 7 § första stycket tryckfrihetsförordningen.
[94] 2 kap. 7 § andra stycket 1 tryckfrihetsförordningen.
[95] RÅ 1998 ref.44.

Det förtjänar att kort nämnas att det även för allmänna handlingar gäller begränsningar i insynsrätten. Uppgifter i allmänna handlingar kan omfattas av sekretess, vilket innebär att de inte är offentliga i denna del.

Våra inledande överväganden

Den ovan redovisade presentationen gör inte anspråk på att vara fullständig men kan förhoppningsvis tjäna som en illustration av den typ av komplicerade rättsliga överväganden som måste göras för att avgöra om, och i så fall när, ett visst elektroniskt material är att anse som allmän handling eller inte. Något slutligt och för hela förvaltningen i alla situationer allmängiltigt ställningstagande i t.ex. frågan om datorprograms (inkluderande algoritmers) offentligrättsliga status kan därför inte presenteras. Ett datorprogram som tagits i bruk inom en myndighet måste dock anses utgöra en upprättad handling, som är att anse som allmän om det också förvaras hos myndigheten.[96]

Gränsdragningen mellan vad som är en färdig elektronisk handling respektive en sammanställning är emellertid många gånger problematisk. Det gäller vare sig det rör sig om sakliga uppgifter (data) eller beståndsdelar i ett program såsom en algoritm. Sannolikt skulle en algoritm i något fall kunna anses ha fått en bestämd, fixerad form av utställaren och därmed anses utgöra en färdig allmän handling i sig. I andra fall skulle en algoritm som beskrivs i programkod kunna vara att anse som en osjälvständig del av programmet, som därmed endast vid förfrågan skulle kunna bli aktuell att sammanställa som en allmän handling under förutsättning att det är möjligt att åstadkomma med rutinbetonade åtgärder.

Till det anförda måste läggas en särskild problematik som uppstår med tolkning och tillämpning av termen *förvarad* när en myndighet anlitar en utomstående leverantör. Avtalen med tjänsteleverantören om vad som ska finnas tillgängligt för en myndighet, i kombination med faktiska tekniska förutsättningar, synes kunna få avgörande betydelse för frågan om vad som ska anses utgöra allmän handling vid utkontraktering.[97]

[96] Jfr RÅ 2004 ref. 74.
[97] Jfr t.ex. kammarrättens dom av den 27 november 2013 i mål nr 2823-13, i fråga om uppgifter som en myndighet inte, enligt kontraktet, hade rätt att få tillgång till.

Sammantaget kan det konstateras att det fortfarande finns besvärliga definitionsproblem vad gäller handlingsoffentligheten i digitala miljöer, inte minst vad gäller datorprograms mindre beståndsdelar.[98] Rätten att ta del av allmän handling ger emellertid enligt vår bedömning inte en heltäckande möjlighet till insyn i förvaltningens verksamhet när datorprogram, inbegripet algoritmer, används vid automatiserade förfaranden.

Offentlighets- och sekretesslagen om beskrivning och registrering av allmänna handlingar

I såväl offentlighets- och sekretesslagen som arkivlagen finns flera regler om att myndigheterna på olika sätt ska registrera och beskriva sina allmänna handlingar.[99]

Allmänna handlingar ska som huvudregel enligt offentlighets- och sekretesslagen registreras så snart de har kommit in till eller upprättats hos en myndighet.[100] Skyldigheten att registrera allmänna handlingar är inte ovillkorlig. Om det inte gäller sekretess för uppgifter i de allmänna handlingarna får en myndighet i stället för registrering välja att hålla handlingarna så ordnade att det utan svårighet kan fastställas om en handling har kommit in eller upprättats. En ovillkorlig registreringsskyldighet omfattar därmed bara de handlingar som det gäller sekretess för.

När elektroniska handlingar skapas i tekniska system finns det normalt olika former av automatiserade funktioner, t.ex. loggar, eller kataloger, för att kunna finna handlingarna. Beroende på om de automatiserade funktionerna skapar register som uppfyller kraven i offentlighets- och sekretesslagen kan dessa funktioner vara tillräckliga också för att uppfylla registreringskraven.[101] De uppgifter som ska framgå av registreringen är datum då handlingen[102] kom in eller upprättades, diarienummer eller annan beteckning handlingen

[98] Se motsvarande slutsats i SOU 2007:44 och jfr t.ex. SOU 1997:39.
[99] Se särskilt 4 kap. 2 § och 5 kap. 1 § offentlighets- och sekretesslagen, 6 § 2 arkivlagen, 6 kap. 5 § RA-FS 2008:4, 5 kap. RA-FS 2009:1.
[100] 5 kap. 1 § första stycket offentlighets- och sekretesslagen.
[101] Eva Lenberg m.fl., a.a., kommentaren till 5 kap. 1 § offentlighets- och sekretesslagen.
[102] Här synes i digitala miljöer fortfarande avses färdiga elektroniska handlingar, vår anmärkning. Jfr SOU 1997:39.

fått vid registreringen, i förekommande fall uppgifter om handlingens avsändare eller mottagare och i korthet vad handlingen rör. Uppgifter om avsändare eller mottagare och i korthet vad handlingen rör ska utelämnas eller särskiljas om det behövs för att registret i övriga delar ska kunna hållas tillgängligt för allmänheten.[103]

Här bör även nämnas att Datalagskommittén år 1997 lämnade ett förslag till bestämmelse om skyldighet för myndigheter att hålla systemdokumentation tillgänglig för allmänheten. Systemdokumentationen skulle beskriva hur sådana program som fattar automatiserade beslut är konstruerade. Bestämmelsen borde enligt förslaget införas i dåvarande sekretesslagen (1980:100) där övriga regler om myndigheternas skyldigheter att registrera och dokumentera fanns. Myndigheterna borde däremot inte åläggas en skyldighet att lämna ut datorprogram i elektronisk form, särskilt med beaktande av säkerhetsaspekter och upphovsrätt.[104] Utredningens föreslog att den aktuella bestämmelsen skulle ha följande lydelse.

Systemdokumentation

12 §
En myndighet som i sin myndighetsutövning använder tekniska hjälpmedel för att fatta automatiserade beslut skall hålla systemdokumentation tillgänglig för allmänheten. Av dokumentationen skall framgå
1. ändamålet med systemet,
2. vilka uppgifter som används i systemet,
3. varifrån och hur de uppgifter som används i systemet hämtas,
4. hur aktuella rättsregler har omvandlats till logiska regler i systemet,
5. vem som hos myndigheten kan lämna närmare upplysningar om hur systemet fungerar.
Dokumentationen får dock inte innehålla upplysningar som kan leda till att sekretessbelagda uppgifter om systemet röjs.

Förslaget har inte lett till lagstiftning.

Dokumentation enligt arkivlagen

Även arkivregleringen innehåller krav på dokumentation.[105] Riksarkivets föreskrifter innebär relativt detaljerade dokumentationskrav vad gäller elektroniska handlingar. Med elektronisk handling

[103] 5 kap. 2 § offentlighets- och sekretesslagen.
[104] SOU 1997:39 s. 569 f.
[105] Se särskilt 2 § arkivlagen, 6 kap. 5 § RA-FS 2008:4 och 5 kap. RA-FS 2009:1.

avses i Riksarkivets föreskrifter en upptagning för automatiserad behandling i enlighet med 2 kap. 3 § tryckfrihetsförordningen.

En myndighet ska enligt Riksarkivets föreskrifter bl.a. dokumentera sina elektroniska handlingar för att handlingarna ska kunna framställas, överföras, hanteras, förvaras och vårdas på ett tillfredsställande sätt under den tid som de ska bevaras.[106] Dokumentationens disposition, omfattning och detaljnivå ska anpassas till den typ av elektroniska handlingar som avses. Om det krävs för förståelsen ska dokumentationen förses med innehållsförteckning, läsanvisning samt beskrivning av den eller de metoder som har använts vid framtagning av dokumentation. Dokumentationen ska fortlöpande kompletteras och hållas aktuell. Sambanden mellan elektroniska handlingar och dokumentation ska upprätthållas över tid.[107]

Dokumentationen ska bl.a. innehålla en översiktlig beskrivning, redogörelse för informationsinnehåll, redogörelse för indata och utdata, redogörelse för registrerings- och uttagsmöjligheter, beskrivning av relationer mellan olika delar, beskrivning över hur koder och förkortningar har använts, beskrivning av rutiner och funktioner, beskrivning av lagrade data såsom struktur, samband och definitioner, redogörelse för ändringar, redogörelse för informationskvalitet, redogörelse för användningen av standarder samt i förekommande fall avvikelser från standarder, dokumentation av strategi för bevarande, dokumentation av test och utvärdering vid driftsättning, dokumentation rörande informationssäkerhet och dokumentation rörande den gallring som sker av elektroniska handlingar. [108]

Våra inledande överväganden

Vi noterar inledningsvis att såväl offentlighets- och sekretesslagens krav på beskrivning och registrering som arkivlagstiftningens krav på dokumentation, här främst redovisat genom en kort redogörelse av Riksarkivets föreskrifter, hänför sig till allmän handling som utgångspunkt för det som ska registreras respektive dokumenteras. De svårigheter som vi ovan redogjort för vad gäller att avgöra den offentligrättsliga statusen för sammanställningar av uppgifter ur

[106] 5 kap. 1 § RA-FS 2009:1.
[107] 5 kap. 2och3 §§ RA-FS 2009:1.
[108] 5 kap. 4 § RA-FS 2009:1.

elektroniska handlingar i digital miljö blir därmed av betydelse även i fråga om dessa registrerings- och dokumentationsskyldigheter. Det föreligger alltså fortfarande en rättslig osäkerhet med avseende på vad som utgör en allmän handling när det gäller datorprogram och i än högre grad när det gäller dess mindre beståndsdelar i form av algoritmer.

Som framgått ovan kan algoritmer eller datorprogram i vissa fall utgöra färdiga elektroniska handlingar, som träffas av befintliga krav på registrering eller dokumentation enligt offentlighets- och sekretesslagen eller arkivregleringen. I andra fall kan en algoritm som beskrivs i programkod kunna vara att anse som en osjälvständig del av programmet, som därmed endast vid förfrågan skulle kunna bli aktuell att sammanställa som en allmän handling (under förutsättning att det är möjligt att åstadkomma med rutinbetonade åtgärder). De sistnämnda algoritmerna träffas inte direkt av de befintliga registrerings- och dokumentationskraven. Kraven kan nämligen inte förstås på annat sätt än att de enbart träffar färdiga elektroniska handlingar. Som ovan framgått förstärks också problematiken när det är fråga om algoritmer eller anknytande datorprogram som tillhandahålls av utomstående leverantörer.

Till detta bör läggas att Riksarkivets föreskrifter inte är direkt bindande i förhållande till kommuners hantering av allmänna handlingar.[109] Under kartläggningen har det därtill blivit känt för oss att föreskrifterna som rör arkiv inte heller alltid beaktas från början när ett nytt it-system eller datorprogram tas i bruk, trots de olägenheter som uppstår när frågor om möjligheter till långtidsbevarande inte omhändertas redan när ett nytt system planeras.

7.6.4 Offentlighets- och sekretesslagen om beslutsunderlag

Dokumentation av beslutsunderlag

I 4 kap. 3 § offentlighets- och sekretesslagen finns en särskild bestämmelse om dokumentation av beslutsunderlag som tillkom i mitten på 1970-talet. Den anger att om en myndighet för handläggning av ett mål eller ärende använder sig av en upptagning för automatiserad behandling, ska upptagningen tillföras handlingarna i

[109] Samverkan äger dock rum mellan Riksarkivet, Sveriges Kommuner och Landsting (SKL) kommuner och landsting, bl.a. genom samrådsgruppen för kommunala arkivfrågor.

målet eller ärendet i läsbar form, om det inte finns särskilda skäl mot det. Bestämmelsen innebär med andra ord en huvudregel om skyldighet att överföra uppgifter som en myndighet hämtar från t.ex. ett visst register till handlingarna i det enskilda målet eller ärendet. Regeln tar även sikte på sådana upptagningar som inte innefattar upplysning om enskild person. Som skäl för bestämmelsen anfördes att man inte i efterhand kan göra klart för sig vilka uppgifter som påverkade beslutet i ett mål eller ärende om inte alla uppgifter som hade betydelse för avgörandet ingår i akten. Det angavs vidare att eftersom ADB-register[110] ofta ändras kontinuerligt, kunde deras innehåll vid viss tidpunkt vara svårt att fastställa. Bestämmelsens betydelse för att tillgodose offentlighetsprincipen framhölls också i förarbetena till densamma.[111]

Efter att ursprungligen varit placerad i dåvarande datalagen (1973:289) har bestämmelsen flyttats till den tidigare sekretesslagen och överförts till den nuvarande offentlighets- och sekretesslagen.[112]

Redan när den aktuella bestämmelsen infördes pekade flera remissinstanser på ekonomiska konsekvenser och att åtskilligt av vinsterna med nya datasystem skulle gå förlorat om myndigheterna tvingades överföra informationsmängder till akter (som då var pappersbaserade). Av det skälet infördes möjligheten till undantag. Det ankommer på myndigheten själv att avgöra i vilka fall man bör kunna underlåta att överföra en upptagning till handlingarna i målet eller ärendet i läsbar form. Det krävs dock att särskilda skäl föreligger. Som exempel på sådana skäl angavs i förarbetena att upptagningen finns lätt tillgänglig, t.ex. via bildskärm. Departementschefen förtydligade också att bestämmelsen endast avser upptagning som används i mål eller ärende. Till denna kategori borde normalt inte räknas exempelvis framställning av statistikprodukt.[113]

Förarbeten till 1986 års förvaltningslag hänvisar till den aktuella bestämmelsen. Där anges också att bestämmelsen ska tillämpas framför förvaltningslagens paragraf om skyldighet att dokumentera

[110] ADB står för automatiserad/automatisk databehandling.
[111] Se bl.a. *Kungl. Maj:ts proposition med förslag till ändringar i tryckfrihetsförordningen, m.m.*,prop. 1973:33,s. 141.
[112] *Personuppgiftslag*, prop. 1997/98:44 s. 112 och *Offentlighets- och sekretesslag*, prop. 2008/09:150, s. 365.
[113] Prop. 1973:33 s. 141 f. Se även prop. 1997/98:44 s. 112 f. och prop. 2008/09:150 s. 365, där formuleringen ”upptagning för automatiserad behandling” valdes i stället för begreppet ”ADB-register” som ansågs föråldrat.

information om uppgifter som en myndighet får på annat sätt än genom en handling och som kan ha betydelse för utgången i ärendet.[114]

Våra inledande överväganden

Den särskilda bestämmelsen i offentlighets- och sekretesslagen om överföring av upptagning för automatiserad behandling i läsbar form i vissa fall har i stor utsträckning lämnats oförändrad sedan dess tillkomst i mitten på 1970-talet. Den förändring i lydelse som gjordes vid ikraftträdande av offentlighets- och sekretesslagen, när termen ADB-register utmönstrades till förmån för lydelsen upptagning för automatiserad behandling, kan i någon mån ha grumlat betydelsen av bestämmelsen eftersom det inte framgår lika tydligt att bestämmelsen syftar till att träffa situationer när information hämtas eller läses från andra register eller databaser.

Under senare tid har sammanlänkningen av databaser och andra delar av it-system inom förvaltningen i allt högre grad ökat, liksom nyttorna med att använda stora datamängder (med en annan term ”Big Data”) till underlag för beslut och för framtagande av t.ex. beslutsstöd för delvis automatiserat beslutsfattande. Detta och den allt mer samordnade informationsförsörjningen inom förvaltningen gör att bestämmelsen enligt vår bedömning fortfarande är högst relevant.[115]

Undantagsmöjligheten från kravet på att beslutsunderlag ska tillföras målet eller ärendet motiverades ursprungligen av kostnadsskäl med avseende på kostnader för att ta fram och bevara pappershandlingar i ärendeakter över uppgifter från olika datoriserade register. Kostnadsaspekten är enligt vår bedömning fortfarande av vikt vid val av hur uppgifter (data) bör lagras i förvaltningen. I nutid gäller det särskilt frågan om kostnader för att lagra stora volymer i varje enskilt ärende jämförd med kostnaden för lagring vid en central källa. Samtidigt behöver även bl.a. informationssäkerhetsaspekter beaktas vid val av lagringsplats. Behovet av att använda bestämmel-

[114] Regeringens proposition 1985/86:80 om *ny förvaltningslag*, s. 66.
[115] Tidigare har bestämmelsens relevans i förhållande till dokumentationsskyldighet enligt förvaltningslagen m.fl. författningar ifrågasatts, se bl.a. *Elektronisk dokumenthantering* (SOU 1996:40) s. 262 f.

sens undantagsmöjligheter för att undvika lagring av samma uppgifter på flera håll inom en myndighet eller i förvaltningen torde emellertid enligt vår bedömning snarare öka än minska. Fortfarande behöver det dock, särskilt av rättssäkerhetsskäl men också av allmänt insynsintresse, finnas möjligheter till insyn i de uppgifter som relaterar till ett enskilt mål eller ärende. Vi ser därför ett behov av att göra en närmare analys avseende om, och i förekommande fall hur, möjligheten till insyn i beslutsunderlaget i enskilda mål eller ärenden behöver klargöras eller stärkas.

7.7 God offentlighetsstruktur för insyn i förvaltningens ärendehantering

7.7.1 Behövs ny eller anpassad reglering?

Utredningens bedömning: En anpassning bör göras i den reglering som säkerställer insynsmöjligheter när vissa automatiserade förfaranden används. Det gäller regler som säkerställer möjligheter till insyn dels i hur den digitala förvaltningen använder vissa algoritmer eller datorprogram vid mål- eller ärendehantering, dels i underlaget i enskilda mål eller ärenden.

En sådan anpassning undanröjer en rättslig osäkerhet som nu hindrar eller hämmar digitaliseringen samtidigt som offentlighetsprincipen säkerställs och rättssäkerheten stärks.

Skälen för utredningens bedömning

Insyn i den digitala förvaltningens verksamhet

Vår utgångspunkt är att graden av digitalisering och automation i förvaltningen ökar för att möta framtida samhällsutmaningar och för att upprätthålla en förvaltning som är trygg, innovativ och effektiv även i fortsättningen. För att tilliten till den digitala förvaltningen ska bestå vid en ökad grad av automation är det emellertid avgörande att möjligheter till öppenhet och insyn även i fortsättningen kan säkerställas.

En första fråga att ta ställning till är om insynsmöjligheterna förändras när manuella förfaranden automatiseras, och i sådant fall på vilket sätt.

Även vid automatiserade förfaranden gäller bestämmelserna i bl.a. förvaltningslagen som kräver att en myndighet måste ange de skäl som har bestämt utgången i ett enskilt ärende och att skälen måste presenteras på ett sådant sätt att de blir begripliga för den enskilde.[116] Det kan hävdas att det oavsett teknik är detta resultat av myndigheternas regeltillämpning som är det viktiga, och att det är denna regeltillämpning som allmänheten med stöd av offentlighetsprincipen behöver kunna få insyn i och kontrollera. Det finns inte heller någon särskild mekanism för insyn för att kontrollera hur ett manuellt framställt beslut har tillkommit annat än i den mån det framgår av beslutsmotiveringen. De rutiner och hjälpverktyg som den enskilde tjänstemannen i övrigt använder vid regeltillämpning är t.ex. sällan föremål för allmänhetens insyn.[117]

Vid en manuell handläggning kan emellertid frågor ställas i efterhand till ansvarig tjänsteman, t.ex. vid tillsyn och myndigheters interna egenkontroller. Det är också möjligt att kontrollera t.ex. vilken utbildning den ansvarige beslutsfattaren har haft eller i övrigt vilka förutsättningar som förelåg när tjänstemannen fattade beslutet. För att säkerställa, och också visa, att inga ovillkorliga hänsyn tas i samband med mänskligt beslutsfattande finns också flertalet bestämmelser om jäv.[118]

I den mån datorprogram som används vid myndigheters automatiserade förfaranden innehåller felkonstruktioner vilket leder till felaktiga resultat skulle det kunna hävdas att de befintliga rättssäkerhetsgarantierna där oriktiga beslut kan angripas på vanligt sätt, t.ex. genom överklagande, fortfarande är tillräckliga. Under kartläggningen har vi emellertid fått exempel på fall där det visat sig svårt att i efterhand dels alls upptäcka, dels tränga in i och närmare kontrollera dessa felaktigheter. Det behöver vara möjligt för den enskilde som berörs av ett visst beslut, för tillsynsmyndigheter, journalister eller andra intressenter hos allmänheten och inte minst för myndighetens egen personal att finna eventuella brister i de

[116] 32 § förvaltningslagen och prop. 2016/17:180. Se även 17 kap. 7 § första stycket 5 och 30 kap. 5 § första stycket 5 rättegångsbalken, 30 § andra stycket förvaltningsprocesslagen och 28 § lagen om domstolsärenden.
[117] Se motsvarande resonemang i SOU 1997:39 s. 567.
[118] Se t.ex. 16–18 §§ förvaltningslagen.

algoritmer eller anknytande datorprogram som används. Annars blir de formella möjligheterna att angripa fel genom överklagande av beslut kraftigt kringskurna.

Förvaltningens automationsåtgärder föranleder alltså vissa förändringar i möjligheten till insyn som behöver adresseras och belysas ur ett rättsligt perspektiv för att säkerställa fortsatt rättssäkra förfaranden.

Av våra inledande överväganden i kapitel 7.6 framgår sammanfattningsvis att den rätt till insyn i bl.a. logiken bakom ett automatiserat förfarande som föreskrivs i dataskyddsförordningen inte är heltäckande, vare sig när det gäller att tillgodose insynsintressen i enskilda ärenden eller allmänhetens generella insynsintressen. Den särskilda rätt till partsinsyn som följer av bl.a. förvaltningslagen ger inte heller rätt till insyn i de datorprogram (inklusive algoritmer) som används vid helt eller delvis automatiserat beslutsförfarande, eller särskilt upprättade krav- eller designdokument i den utsträckning sådana har tagits fram inom myndigheten.

Rättsläget är vidare i viss utsträckning oklart när det gäller den offentligrättsliga statusen för datorprogram och i än högre grad när det gäller dess beståndsdelar i form av framför allt algoritmer. Bedömningen av vad som utgör allmän handling i digital miljö får samtidigt helt avgörande betydelse för de nu gällande registrerings- och dokumentationsskyldigheterna som förvaltningen har att fullgöra i syfte att möjliggöra allmänhetens insyn. Särskilt när det är fråga om algoritmer eller anknytande datorprogram som tillhandahålls av utomstående leverantörer ger nuvarande rättsliga förutsättningar enligt vår bedömning inte fullgoda möjligheter till insyn för att följa förvaltningens verksamhet. För flera myndigheter behövs samtidigt samverkan med privata aktörer, vare sig det rör inköp eller utkontraktering, för att kunna ta tillvara digitaliseringens möjligheter eftersom vissa funktioner kräver specialistkompetens som inte varje myndighet kan sörja för på egen hand.

Den rättsliga osäkerhet gällande insynen i den allt mer automatiserade förvaltningen som beskrivits för oss under kartläggningen, och som vi i kapitel 7.1.2 bedömt ha en hämmande inverkan på förvaltningens fortsatta digitalisering med avseende på automationsåtgärder har sammanfattningsvis fog för sig även efter en analys av gällande rätt.

Därtill kan det enligt vår bedömning finnas skäl att stärka skyddet för enskilda genom att fastställa lämpliga skyddsåtgärder i nationell rätt på det sätt som föreskrivs i dataskyddsförordningen om automatiserat beslutsfattande. Våra ställningstaganden och förslag i det följande ska alltså också ses i förhållande till dataskyddsförordningens reglering om lämpliga åtgärder till skydd för enskilda.[119]

Sekretess

Det bör framhållas att det inte sällan kommer i fråga att någon form av sekretess gäller för myndigheters algoritmer eller datorprogram, liksom för särskild dokumentation kring framtagande av dessa i den mån sådana dokument skulle vara att anse som allmänna handlingar.

Det kan röra sig om sekretess för uppgifter som skulle kunna missbrukas om de blev allmänt kända, t.ex. uppgifter som ska hållas hemliga med hänsyn till myndighetens verksamhet för inspektion, kontroll eller annan tillsyn.[120] Om en algoritm eller ett datorprogram som utgör allmän handling innehåller uppgifter som avslöjar de kontrollmetoder som myndigheten använder, t.ex. vilka uppgifter som jämförs för att kontrollera skattskyldiga eller hur urvalet av bidragsberättigade som ska granskas görs, kan den aktuella sekretessbestämmelsen vara tillämplig.

Det kan också röra sig om sekretess för uppgifter som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser system för automatiserad behandling av information.[121] Även annan sekretessreglering kan aktualiseras.

Det förhållandet att sekretess kan gälla för algoritmer eller datorprogram inverkar emellertid inte på behovet av att upprätthålla god offentlighetsstruktur till gagn för en grundläggande möjlighet till insyn i förvaltningens förfaranden. Tvärtom gäller ovillkorliga krav på registrering av allmänna handlingar som omfattas av sekretess[122] med hänsyn till den särskilda vikten av att sådana handlingar hålls ordnade hos myndigheterna. Att sekretess kan gälla för de algoritmer eller datorprogram som vi nu närmare analyserar, stärker därför

[119] Artikel 22.2.b dataskyddsförordningen, se även våra inledande överväganden i kapitel 7.6.2.
[120] 17 kap. 1 § offentlighets- och sekretesslagen.
[121] 18 kap. 8 § 3 offentlighets- och sekretesslagen.
[122] 5 kap. 1 § tredje stycket offentlighets- och sekretesslagen.

snarare än försvagar behovet av god offentlighetsstruktur. En sådan god struktur bidrar också till goda möjligheter för tillsyn och egenkontroll, särskilt i de situationer när allmänhetens möjligheter till insyn begränsas av sekretess.

Immaterialrätt

De immaterialrättsliga förutsättningar som kan finnas, framför allt i fråga om upphovsrätt för datorprogram, behöver också tas i beaktande vid överväganden om vilka möjligheter till insyn som finns och ska finnas i en digital förvaltning.

Upphovsmannens och rättighetsinnehavarens intressen skyddas av upphovsrättslagstiftningen och andra lagar som ansluter till upphovsrättens område.[123] Upphovsrättsligt skydd förhindrar normalt sett inte ett utlämnande av allmänna handlingar.[124] Utlämnandet betyder dock inte att den som tar del av handlingen kan vidareutnyttja den fritt, t.ex. tillgängliggöra handlingen på webben eller sälja kopior av handlingen, eftersom upphovsrätten kvarstår efter ett utlämnande. I offentlighets- och sekretesslagen finns vidare sekretessreglering som träffar uppgift i ett upphovsrättsligt skyddat verk som inte kan antas sakna kommersiellt intresse.[125] De förslag som utredningen lämnar behöver därför stå i god balans med intresset av att värna även det immaterialrättsliga skyddet. Den balansen diskuteras i kapitel 11.4.3 om it-avtal, där också bl.a. lagen (1990:409) om skydd för företagshemligheter uppmärksammas.[126]

Myndigheters ansvar och möjligheter till egenkontroll

Som framgått i kapitel 7.5.2 följer också nya risker med modern teknik. Om brister i insynsmöjligheter består samtidigt som förvaltningen tar ett tekniksprång finns en påtaglig risk för att fel i bakomliggande funktioner inte alls uppmärksammas. Några situationer där felaktigheter visat sig förekomma i samband med automatiserade

[123] 1 kap. 8 § tryckfrihetsförordningen.
[124] 26 b § upphovsrättslagen (1960:729).
[125] 31 kap. 23 § offentlighets- och sekretesslagen.
[126] Regeringen har i lagrådsremiss *En ny lag om företagshemligheter* av den 8 februari 2018 föreslagit ny lagstiftning.

förfaranden har också beskrivits för oss under kartläggningen.[127] Samtidigt har vi förstått att det inte alltid varit möjligt för en myndighet att på egen hand kontrollera fel i bakomliggande beräkningar, på grund av att myndigheten inte haft tillgång till det datorprogram som använts eller för egen del haft tillräcklig möjlighet till insyn i den bakomliggande funktionaliteten. Det kan t.ex. ha berott på att myndigheten inte ställt särskilda krav i förhållande till leverantörer på att viss insynsmöjlighet ska finnas (se även kapitel 11.4.3 om it-avtal).

Vad som anförts ovan om bristande möjligheter för myndigheter att för egen del kunna ta del av hur de algoritmer eller datorprogram som används i verksamheten fungerar aktualiserar frågan om hur en myndighet kan säkerställa att ansvar kan tas för ärendehandläggning och beslutsfattande vid automatiserade förfaranden. Det gäller särskilt i de fall algoritmer med anknytande datorprogram som används tillhandahålls av annan.

Ytterligare en av de frågor som har lyfts för oss under kartläggningen är vem på myndigheten som kan eller bör anges som ansvarig för beslut som fattats automatiserat. Ytterst är myndighetschefen ansvarig för den verksamhet som bedrivs vid myndigheten. Men de ovan nämnda frågeställningarna visar på vikten av att det i myndigheten finns en tydlig, och i förhållande till enskilda och allmänhet, transparent fördelning avseende vem som har att ta ställning till om, och på vilket sätt, automatiserade förfaranden ska införas och hur de ska utformas. Den ansvarige vid myndigheten, ytterst myndighetschefen om delegation inte framgår av arbetsordning eller på annat sätt, behöver därförsäkerställa att det kommer att finnas tillräckliga möjligheter till insyn i den funktionalitet som ligger bakom automatiserade förfaranden så att det är möjligt att utöva ansvaret för den verksamhet som bedrivs och de beslut som fattas.

Här bör också nämnas att ansvarsfrågor rörande ökat automatiserat beslutsfattande i förvaltningen kan komma att angränsa till regeringsformens krav på att en förvaltningsuppgift som innefattar myndighetsutövning endast får överlämnas åt kommuner, andra juridiska personer och enskilda individer med stöd av lag.[128] Detta utgör också ett skäl till varför myndigheter för egen del behöver ha förmåga att fullgöra sitt eget ansvar och inte passera gränsen för vad

[127] Se t.ex. förvaltningsrätten i Uppsalas dom av den 28 juni 2017 i mål nr 1333-17.
[128] 12 kap. 4 § regeringsformen.

som utan särskilt författningsstöd är tillåtet att överlämna till en utomstående aktör.

Utöver allmänhetens intresse av insyn i förvaltningens verksamhet kan mot den beskrivna bakgrunden också läggas intresset av att verksamhetsansvariga har fullgoda möjligheter att ta ansvar för den verksamhet som bedrivs, och de beslut som fattas, också genom automatiserade förfaranden. Vad som här diskuteras om behov av anpassad reglering för att säkerställa förmåga att ge tillräcklig insyn i den digitala förvaltningen bör därför även ses i ljuset av att skapa goda förutsättningar för förvaltningens egenkontroll och ansvarstagande vid automatiserade förfaranden, särskilt med ny teknik i åtanke.

Författningsändringar eller andra alternativ

Inför fortsatta ställningstaganden har vi övervägt om den rättsliga analys som ovan beskrivits i sig skulle kunna bidra till att myndigheter säkerställer insyn i den digitala förvaltningens verksamhet genom att bl.a. ställa krav på utomstående leverantörer och avtala om insynsmöjligheter. Kan med andra ord tillräckligt god offentlighetsstruktur och möjligheter till insyn i den digitala förvaltningen åstadkommas, utan att någon ny reglering föreslås vid sidan av den som gäller enligt t.ex. dataskyddsförordningen till skydd för den registrerade?

Det finns flera situationer där en sådan god offentlighetsstruktur med insynsmöjligheter behövs, under förutsättning att det inte gäller sekretess. Behovet gör sig gällande i alla typer av utvecklingsarbeten, vid helt myndighetsinterna sådana såväl som vid myndighetssamverkan. Behovet visar sig också vid inköp eller utkontraktering av olika slag. Det gör sig vidare gällande i såväl enskilda ärenden, som mer generellt när det gäller den bakomliggande funktionaliteten vid automatiserade förfaranden. Vi bedömer det dock sammantaget som osannolikt att krav som inte härrör från författning alltid skulle prioriteras i utvecklingsarbeten, vid inköp eller utkontraktering, särskilt inte om de i något fall kan komma att medföra kostnadsökningar utan att genast ge verksamhetsnytta.

Under kartläggningen har vi också, å ena sidan, fått kännedom om att i vart fall delar av förvaltningen nu intar en försiktig hållning

och avvaktar med automationsåtgärder givet det oklara rättsläget. Detta även efter de ändringar i förvaltningslagen om automatiserat beslutsfattande som genomförts i syfte att underlätta förvaltningens fortsatta digitalisering. Här märks med andra ord en vilja att juridiska överväganden och fortsatt lagstiftningsarbete ska gå före innan nya automatiserade förfaranden sjösätts. De hittillsvarande diskussionerna om automatiserat beslutsfattande var rättsenligt utan uttryckligt författningsstöd har också visat på att förekomsten av rättslig osäkerhet kan hindra eller fördröja en digital utveckling inom förvaltningen, på ett sätt som nu i efterhand har visat sig onödigt när förvaltningslagen ändrats och ger ett generellt stöd åt den automatiserade beslutsformen.

Å andra sidan ser vi också en risk för att andra incitament eller styrmedel än rättsregler snabbt kan driva utvecklingen i offentlig verksamhet vidare. En faktor som talar för detta är det tekniksprång som nu äger rum, bl.a. genom AI-system med maskininlärda algoritmer som har annan funktionalitet än de traditionellt programmerade algoritmerna. Om det inte står klart att grundläggande krav på god offentlighetsstruktur och möjlighet till insyn i verksamheten kan tillgodoses vid automation i förvaltningen samtidigt som t.ex. effektivitetsskäl driver utvecklingen snabbt framåt, finns risker för att nya funktioner byggs som i efterhand visar sig svåra eller kostsamma att ändra om rättsliga problem framkommer först efter hand.

Enligt vår bedömning bör inte grundläggande frågor om garantier för allmänhetens insyn och rättssäkra förfaranden vid förvaltningens automation lämnas åt enskilda rättstillämpare vid respektive myndighet att hantera. I linje med vad regeringen tidigare anfört[129] behöver förvaltningen från offentlighetssynpunkt garantera i vart fall förmåga att tillhandahålla viss information om bakomliggande funktionalitet vid automatiserade förfaranden. Särskilt när nu sådana förfaranden blir av allt större betydelse för förvaltningens verksamhet och ärendehandläggning.

Enligt vår bedömning är tiden mogen för att genom en proaktiv reglering ge ledning genom tydliga rättsregler som följer det konstitutionella förfarandet. På det sättet drivs utvecklingen framåt samtidigt som det undviks att funktioner och förfaranden tas fram som senare visar sig inte gå att förena med centrala rättsliga värden,

[129] Prop. 2001/02:70 s. 18 f.

med onödiga kostnader och väsentliga risker för såväl det allmänna som enskilda som följd.

Frågan om anpassning av regleringen om god offentlighetsstruktur för att ge möjlighet till insyn bör prioriteras. Den har potential att stödja den fortsatta digitaliseringen av den offentliga förvaltningen som helhet, genom att undanröja en rättslig osäkerhet som hindrar eller hämmar digitaliseringen samtidigt som offentlighetsprincipen säkerställs och rättssäkerheten stärks.

Varje myndighet som överväger att öka graden av automation i sin verksamhet behöver också överväga nyttan med åtgärden. På en övergripande nivå bedömer vi dock att en ny reglering som klargör vissa frågor om god offentlighetsstruktur för säkerställande av insynsmöjligheter också medför goda möjligheter till såväl effektivitetssprång i förvaltningens verksamhet som innovation i samhället i stort. Bland de områden som enligt vår bedömning kommer att präglas av en ökad grad av automation i framtiden, och som kommer att gagnas av den rättsliga tydlighet som här diskuteras, kan nämnas effektiva kontroller av utbetalningar i välfärdssystemen.

Det finns som beskrivits ovan en god rättslig struktur att utgå från när det gäller reglering som säkerställer insyn i hur förvaltningens verksamhet bedrivs. Vi ser inte anledning att frångå den strukturen eller göra några större eller genomgripande förändringar i regleringen. En anpassning bör dock göras i den reglering som säkerställer insynsmöjligheter när vissa automatiserade förfaranden används. Det gäller för det första, och som här ovan främst har berörts, möjligheterna till insyn i hur den digitala förvaltningen använder vissa algoritmer med anknytande datorprogram vid mål- eller ärendehandläggning. Det gäller för det andra även insynsmöjligheter i underlaget i enskilda mål eller ärenden.

7.7.2 Förmåga att ge insyn i vissa automatiserade förfaranden

Utredningens förslag: Det ska regleras i författning att en myndighet ska se till att information kan lämnas om hur myndigheten vid handläggning av mål eller ärenden använder algoritmer eller datorprogram som, helt eller delvis, påverkar utfallet eller beslutet vid automatiserade urval eller beslut.

Skälen för utredningens förslag

Stärkt förmåga att ge insyn

Som framgått av de ovan redovisade bedömningarna (se kapitel 7.6 och 7.7.1) har allmänheten inte någon generell rätt eller möjlighet att få reda på hur förvaltningen använder algoritmer eller anknytande datorprogram. I stora delar av förvaltningen kanske det hittills inte heller har varit särskilt relevant att undersöka dessa funktioner närmare. Från offentlighetssynpunkt är det givetvis inte intressant hur ett ord- och textbehandlingsprogram eller ett registreringsprogram är funktionellt uppbyggt. Där är det normalt endast själva texten eller siffrorna som behandlas, eller med andra ord de sakliga uppgifterna som hanteras, som är intressanta att få insyn i. Det intresset tillgodoses också i gällande rätt.

Enligt vår bedömning är det främst av intresse att nu säkerställa att myndigheter kan lämna information om hur de vid handläggning av mål eller ärenden använder vissa algoritmer eller datorprogram som närmast ersätter mänskliga handläggare vid bedömningar i samband med ärendehantering (se vidare nedan för närmare avgränsning av vilka algoritmer eller datorprogram som avses). Ett sådant säkerställande av offentlighetsprincipen och förstärkning av rättssäkerhetsgarantierna i den digitala förvaltningen bedömer vi vara ett rättsligt fundament för att förvaltningen nu ska kunna ta effektivitetssprånget mot en ökad automation, och också kunna dra nytta av ny teknik som t.ex. AI-system med maskininlärda algoritmer. Det handlar med andra ord om att förvaltningen även i fortsättningen ska ha förmåga att kunna svara på frågor om hur verksamheten bedrivs, också när den inte längre sköts av mänskliga handläggare som själva kan svara på frågorna.

Intresset av att stärka förmågan att kunna ge insyn i hur förvaltningen använder sig av algoritmer med anknytande datorprogram gäller i och för sig redan för traditionellt programmerade algoritmer och datorprogram, där programutvecklaren har omvandlat rättsliga regler till logiska formler i programmet och i det sammanhanget varit tvungen att tolka vissa av reglerna.[130] Det kan i dagsläget vara fråga om algoritmer eller datorprogram som t.ex. räknar ut skatter eller avgifter, eller som räknar ut hur mycket pengar en bidragsberättigad

[130] Se Magnusson Sjöberg, Cecilia, a.a., s. 35.

person har rätt att få. Att proaktivt väga in detta intresse när användande av ny teknik övervägs i förvaltningen, samtidigt som en ökad grad av verksamheten kan förutspås bli automatiserad, är dock enligt oss ett än tyngre vägande skäl varför tiden nu är mogen för den reglering som diskuteras i detta kapitel.

I det föregående och nedan resoneras också om att förhållandet till dataskyddsförordningens reglering om automatiserade beslut är ett ytterligare skäl för utredningens förslag.

God offentlighetsstruktur genom förmåga att ge insyn i vissa automatiserade förfaranden

Intresset av att kunna kontrollera och få insyn i myndigheternas verksamhet även när den automatiseras motiverar enligt oss att allmänheten som utgångspunkt ska ha möjlighet att få svar på frågor om hur viss verksamhet vid myndigheterna bedrivs när den sköts av algoritmer eller datorprogram. Intresset av att kunna kontrollera och få insyn gör sig gällande även beträffande sådana algoritmer eller datorprogram som enligt gällande rätt inte skulle anses utgöra allmän handling. Det kunde därför vara aktuellt att undersöka ändringar i grundlagens reglering om handlingsoffentlighet för att säkerställa att algoritmer eller datorprogram som används vid vissa automatiserade förfaranden kommer att kunna granskas av allmänheten.

Det ligger emellertid inte inom ramen för vårt uppdrag att föreslå grundlagsändring. En grundlagsändring tar därtill särskild tid att genomföra, och vår bedömning är att den komplettering av gällande rätt som vi nu undersöker bör åstadkommas i närtid. En ändring i grundlagen bedöms inte heller vara nödvändig för att åstadkomma den goda offentlighetsstruktur som kan säkerställa att myndigheter förmår ge nödvändig insyn för granskning även av automatiserade förfaranden.

Även om utgångspunkten är att allmänheten ska ges insyn i förvaltningens verksamhet, kommer vidare som framgått ovan sekretess inte sällan att gälla för dessa algoritmer eller datorprogram liksom för särskild dokumentation kring framtagande av dessa i den mån det skulle vara fråga om allmän handling. Behovet av att åstadkomma god offentlighetsstruktur stärks emellertid snarare än minskar när det också finns intressen av slutenhet (se kapitel 7.7.1

om sekretess och upphovsrätt). I sammanhanget bör det även beaktas att de algoritmer eller datorprogram som vi nu diskuterar normalt kommer att vara komplexa och inte i första hand enkla för var och en ur allmänheten att sätta sig in i och förstå.

Den förmåga att även i fortsättningen säkerställa möjligheter till granskning och insyn i förvaltningens verksamhet som vi strävar efter att åstadkomma behöver därför enligt vår bedömning i viss utsträckning kunna kompletteras av en myndighets egenkontroll av de automatiserade förfarandena, av revision, tillsyn eller andra former av utomstående kontroll eller andra åtgärder för att kunna visa allmänheten att förfarandena är rättssäkra även när det inte är möjligt för var och en att ta del av själva algoritmerna eller programmen. Vi återkommer till den frågan i kapitel 7.8.3 när det särskilt gäller AI-system.

Vilka automatiserade förfaranden avses?

De algoritmer eller datorprogram som är särskilt intressanta ur insynssynpunkt är i första hand de som används vid helt automatiserat beslutsfattande, dvs. beslut som fattas helt utan mänsklig inblandning. Algoritmer eller datorprogram som lämnar förslag till beslut, så kallade beslutsstöd eller delvis automatiserade beslut, kommer emellertid såvitt vi bedömer att få en allt ökande betydelse i den digitala förvaltningen. Gränsdragningen mellan vad som kommer att anses som helt automatiserade förfaranden och sådant beslutsfattande som fattas av människor med understöd av datorgenererade förslag kommer inte att vara helt skarp. Enligt vår bedömning finns det också ett intresse av att säkerställa förmåga till insyn i de beslutsstöd som kommer att ligga till grund för beslutsfattande.

Det har inte legat inom ramen för denna utredning att kartlägga i vilken omfattning förvaltningen tillämpar särskilda automatiska förfaranden för urval och kontroll som t.ex. syftar till att i förväg bedöma vilken sannolikhet det finns för att en individ ska agera felaktigt. Här analyseras inte heller närmare hur sådana kontroller kan utföras på ett effektivt sätt utan att stå i konflikt med grundläggande bestämmelser om diskrimineringsförbudet i regeringsformen och om integritetsskydd i dataskyddsförordningen och i de

registerförfattningar som är aktuella.[131] Vi ser dock behov av att också de algoritmer eller datorprogram som används vid den typen av urval, oavsett om det resulterar i något förvaltningsrättsligt beslut eller inte, omfattas av de här diskuterade möjligheterna att ge insyn.

Vi bedömer sammanfattningsvis att intresset av att myndigheter fortsatt ska säkerställa en förmåga att kunna lämna information om hur verksamheten bedrivs, även när den automatiseras, är särskilt angeläget vid handläggning av mål eller ärenden när myndigheter använder algoritmer eller datorprogram som påverkar automatiserade urval eller beslut.

Ett krav på funktion snarare än viss dokumentation

Den centrala frågan i sammanhanget är hur god offentlighetsstruktur kan åstadkommas som säkerställer grundläggande insynsmöjligheter, vilka i sin tur skapar tillit till den digitala förvaltningen vid de ovan beskrivna automatiserade förfarandena.

Vi ser inte behov av att i detalj reglera nya administrativa rutiner om vilken dokumentation som krävs för att tillgodose intressen av insyn i myndigheternas verksamhet när automatiserade förfaranden används. En sådan ansats skulle riskera att bli allt för administrativt betungande för myndigheterna. Det skulle vidare kunna bli kostsamt i onödan om krav på ingående dokumentation måste fullgöras och om detaljeringsgraden inte är anpassad för den enskilda situationen. Risken finns också att en detaljerad reglering om dokumentation i förlängningen inte visar sig gå i takt med teknikutvecklingen, på ett sätt som gör att det övergripande syftet med regleringen i form av att fortsatt upprätthålla goda insynsmöjligheter inte heller uppnås.

Det finns snarare behov av att säkerställa att en myndighet alltid har förmåga att kunna redogöra för hur den vid handläggning av mål eller ärenden använder vissa algoritmer eller datorprogram som är av avgörande betydelse, än behov av en viss specifik dokumentation i sig. Till skillnad från det förslag som lämnades av Datalagskommittén i *Integritet Offentlighet Informationsteknik*[132] ser vi alltså inte anledning att föreslå någon generell bestämmelse som ålägger

[131] Jfr förslagen i Integritetskommitténs slutbetänkande *Så stärker vi den personliga integriteten* (SOU 2017:52), s. 142 f.
[132] SOU 1997:39.

myndigheterna att ta fram och hålla viss specifik systemdokumentation tillgänglig. Vi inriktar oss i stället på att myndigheter även när förfaranden automatiseras ska ha fortsatt förmåga att kunna ge insyn i verksamheten. Det handlar alltså snarare om att en sådan funktion ska upprätthållas, än att viss dokumentation måste finnas.

Med beaktande av det ovan anförda bör det regleras att myndigheter alltid ska se till att ha förmåga att, på förfrågan, kunna lämna information om hur de vid handläggning av mål eller ärenden använder aktuella algoritmer med anknytande datorprogram. En sådan förmåga och funktion måste kunna krävas av den digitala förvaltningen för att säkerställa tilliten till automatiserade förfaranden. Vi föreslår därför att det ska komma till klart uttryck i författning att myndigheter ska kunna lämna sådan information om någon frågar efter den.

Regleringen bör dock inte utformas som ett mer vidsträckt krav än nödvändigt. Det är tillräckligt att en myndighet ser till att ha eller skaffar sig förmåga att kunna lämna övergripande redogörelser för hur de algoritmer med anknytande datorprogram som omfattas av den nya regleringen används av myndigheten vid frågor från t.ex. allmänheten. Samtidigt bör även här understrykas att sekretess kan hindra att myndigheten alls svarar på allmänhetens frågor som rör användningen av algoritmer eller datorprogram. I de situationerna är det tillräckligt att myndigheten innehar förmåga att lämna information för att kunna svara t.ex. tillsynsmyndigheter eller i samband med att myndigheten utövar egenkontroll avseende de aktuella algoritmerna eller datorprogrammen.

Sammanfattningsvis föreslår vi alltså att det i författning bör framgå att en myndighet ska se till att information kan lämnas om hur myndigheten vid handläggning av mål eller ärenden använder algoritmer eller datorprogram som, helt eller delvis, påverkar utfallet vid automatiserade urval eller beslutet vid automatiserade beslut.

Vårt förslag omfattar såväl algoritmer eller datorprogram som är att anse som allmänna handlingar, som sådana som annars inte utgör allmän handling. Vi föreslår inga ytterligare ändringar av gällande rätt i fråga om dokumentation genom beskrivning och registrering av allmänna handlingar (se kapitel 7.6.3), varför dessa bestämmelser alltjämt ska tillämpas i de fall algoritmer eller datorprogram utgör allmän handling.

Närmare om förslagets innebörd

I de fall en myndighet själv utvecklar eller handhar driften av de algoritmer med anknytande datorprogram som här avses kommer myndigheten normalt sett, genom sina tjänstemän, också ha förmåga att kunna redogöra för hur dessa används i myndighetens verksamhet. Om utomstående leverantörer anlitas kan det emellertid behöva ställas särskilda krav i förhållande till dessa, så att myndigheten får den information som behövs för att i sin tur ha förmåga att kunna redogöra för hur myndigheten använder algoritmerna eller datorprogrammen i sin verksamhet. Se också vidare i kapitel 11 i fråga om praktiskt stöd i bl.a. denna fråga när it-avtal tecknas.

En myndighets information bör vidare kunna vara mer eller mindre detaljerad, beroende på den aktuella situationen. En övergripande beskrivning av hur de algoritmer med anknytande datorprogram som omfattas av regleringen används av myndigheten ska emellertid alltid kunna lämnas. I de fall varken sekretess eller immaterialrättsliga förhållanden uppställer hinder kan därtill t.ex. programkoden med fördel hållas öppen (s.k. öppen källkod), till gagn för såväl insyn som de innovationsmöjligheter detta kan föra med sig. Vårt förslag innebär dock inte någon rättighet för allmänheten att ta del av programkod. I andra fall kan det röra sig om att de tekniska designdokument som tagits fram i samband med implementeringen av algoritmer och datorprogram också kan fungera som underlag när myndigheten fullgör den nu diskuterade bestämmelsen om förmåga att kunna lämna information. Detsamma gäller dokumentation som tagits fram för att möta offentlighets- och sekretesslagens eller arkivlagens bestämmelser om beskrivning eller registrering av allmän handling, i de fall algoritmer eller datorprogram anses utgöra sådan. Något absolut krav på att ta fram särskilda designdokument eller annan dokumentation är det dock inte fråga om, varför förslaget inte bedöms kunna hamna i konflikt med tillämpningen av agila metoder för utvecklingsarbete. Även affärsmässiga överväganden kan påverka på vilket sätt en myndighet väljer att fullgöra den nu aktuella förmågan att ge insyn i hur myndigheten använder algoritmer med anknytande datorprogram som tillhandahålls av utomstående leverantörer (se vidare kapitel 11.4.3 om it-avtal).

Det bör mot den beskrivna bakgrunden enligt vår mening lämnas åt tillämparen att närmare avgöra hur långtgående information som

bör kunna lämnas om användningen av en viss algoritm eller anknytande datorprogram. På så sätt riskeras inte heller att den reglering vi föreslår kommer i konflikt med upphovsrätt eller andra immateriella rättigheter, eller skapar konkurrensmässiga nackdelar eller onödiga hinder mot utkontraktering. På det sättet kan det också säkerställas att kravet på att kunna ge information i varje särskild situation balanseras mot exempelvis krav på säker slutenhet som kan föreligga av t.ex. sekretesskäl.

Förmågan att kunna lämna information om hur myndigheten använder algoritmer eller datorprogram vid mål- eller ärendehandläggning bör emellertid inte ses så snävt som att det alltid handlar om att kunna redogöra för den exakta tekniska utformningen av algoritmer eller datorprogram som sådana. I flera fall torde det vara av större eller lika stort värde att inneha förmåga att kunna svara på frågor om t.ex. vilka kategorier av indata som används vid det automatiserade förfarandet. Är det uppgifter som hämtats från enskilda, från internetbaserade källor, från databaser på annat håll inom förvaltningen eller från sensorer utplacerade i en viss stad? Detta för oss också vidare till frågan om vikten av att säkerställa möjligheten till insyn i beslutsunderlag i enskilda ärenden, se kapitel 7.7.3.

Syftet med den nu föreslagna författningsregleringen är att stärka den goda offentlighetsstrukturen vid myndigheternas användning av vissa automatiserade förfaranden. Behovet bottnar i att beslutsfattande och urvalsförfaranden i ökad grad sker helt eller delvis automatiserat med stöd av nya tekniker i stället för av mänskliga handläggare som själva kan svara på frågor om hur verksamheten bedrivs. För att uppnå det syftet krävs dock inte enligt oss att det införs några nya förfaranden med t.ex. möjlighet till domstolsprövning.

Förhållande till dataskyddsregleringen

I den utsträckning en myndighet använder algoritmer med anknytande datorprogram vid automatiserat individuellt beslutsfattande, inbegripet profilering, som omfattas av dataskyddsförordningen, utgör den av oss föreslagna regleringen om förmåga att kunna lämna information också en lämplig åtgärd till skydd för den registrerades

rättigheter, friheter och berättigade intressen.[133] Vårt förslag tillkommer därför som en ytterligare säkerhetsåtgärd i förhållande till de allmänna rättssäkerhetsgarantierna som anges i t.ex. förvaltningslagen, vilket enligt vår bedömning stärker förvaltningens generella förutsättningar att använda sig av den automatiserade beslutsformen vid beslutsfattande. Se dock även överväganden i kapitel 7.9.1 om gällande rätt med materiella bestämmelser, om eventuella ytterligare behov av säkerhetsåtgärder i vissa fall.

7.7.3 Insyn i beslutsunderlaget i enskilda ärenden

Utredningens förslag: Uppgifter som utgör underlag i ett mål eller ärende ska som huvudregel tillföras handlingarna i det målet eller ärendet, även när underlaget kommer från databaser eller andra digitala källor. En myndighet behöver dock inte tillföra underlaget till handlingarna i målet eller ärendet om det finns särskilda skäl mot det.

När en myndighet inte tillför underlaget till det enskilda målet eller ärendet ska myndigheten se till att information kan lämnas om vilken eller vilka databaser eller andra digitala källor som innehåller ett underlag för handläggningen av målet eller ärendet.

Skälen för utredningens förslag

Huvudregel om att underlag tillförs det enskilda målet eller ärendet

Vår utgångspunkt är att det finns anledning att hålla fast vid huvudregeln i 4 kap. 3 § offentlighets- och sekretesslagen om att uppgifter som utgör underlag i ett mål eller ärende ska tillföras handlingarna i det målet eller ärendet, även när underlaget kommer från olika databaser eller andra digitala källor, t.ex. filer eller sensorsystem, via automatiserade förfaranden. Detta torde fortfarande normalt krävas för att myndigheten ska kunna bereda part insyn i utredningsmaterialet enligt 25 § förvaltningslagen. Regleringen i 4 kap. 3 § offentlighets- och sekretesslagen är vidare inte begränsad till att ge part insyn utan avser att säkerställa en allmän insynsmöjlighet i det

[133] Artikel 22.1 och 22.2 b dataskyddsförordningen.

underlag som ligger till grund för myndigheters mål- och ärendehandläggning.

När huvudregeln tillämpas är det enligt oss inte aktuellt att överväga några ytterligare klargöranden avseende hur det ska vara möjligt att spåra uppgifternas härkomst, utan det bör också i fortsättningen anses tillräckligt att de sakliga uppgifter som utgör beslutsunderlag tillförs akten, som kan vara digital, i det mål eller ärende som handläggs.

Möjlighet till undantag

Huvudregeln bör enligt vår bedömning även fortsättningsvis kunna frångås om det finns särskilda skäl mot att tillföra underlag till handlingarna i målet eller ärendet i läsbar form. Som ett sådant särskilt skäl bör alltjämt kunna räknas att det finns andra tekniska möjligheter som gör att underlaget finns tillgängligt, så att exempelvis part kan se eller få tillgång till uppgifterna utan att en dubblett lagras i det enskilda ärendet.[134]

I tidigare förarbetsuttalanden har det uttalats att åtskilligt av vinsterna med nya datasystem skulle gå förlorade om myndigheterna skulle tvingas till en betydande och dyrbar hantering av kopior, då i pappersform. Argumentet gör sig fortfarande gällande, varför möjligheten till undantag också fortfarande behöver kunna användas om alternativet vore att myndigheterna skulle vållas betydande kostnader för dubbel elektronisk lagring av uppgifter.[135]

Behovet av att använda undantagsmöjligheten torde komma att öka i linje med att graden av inhämtande av beslutsunderlag från digitala källor kan förutses öka.[136] Strävan går i flera avseenden mot att förenkla för enskilda så att dessa inte själva ska behöva fylla i och tillhandahålla alla uppgifter som behövs för att pröva en ansökan eller anmälan, utan i högre grad ges service genom att uppgifter samlas in från andra källor och presenteras digitalt på ett sätt som också underlättar för det fortsatta automatiserade förfarandet vid

[134] Jfr prop. 1973:33 s.143. Se i detta sammanhang även våra bedömningar i kapitel 8.3.7 och 12.2.4 om att det, i samband med utarbetande av nya former för informationsförsörjning inom förvaltningen, finns skäl för att vissa grundläggande uppgifter inte ska behöva kommuniceras med enskilda enligt 25 § förvaltningslagen i varje enskilt ärende.
[135] Se a. prop. s. 141 f.
[136] Jfr dock även vad som angetts i kapitel 7.6.4 om behovet av att överväga lagringsplatser även utifrån t.ex. informations- och cybersäkerhetsintressen.

ärendehandläggning och beslutsfattande. I vissa ärenden torde det dessutom bli allt vanligare med stora datamängder som beslutsunderlag, t.ex. när det gäller geografisk information eller miljöinformation. Användande av ny teknik med möjlighet till hantering av stora datamängder får inte leda till onödiga kostnader för dubbel lagring av information.

Spårbarhet till beslutsunderlag

Vi ser inte anledning att frångå den bedömning som regeringen tidigare gjort om att den nu aktuella bestämmelsen i offentlighets- och sekretesslagen har företräde framför förvaltningslagens krav på dokumentation av beslutsunderlag.[137] Konsekvensen blir emellertid att det enligt gällande rätt inte följer några uttryckliga krav på att kunna härleda beslutsunderlag från upptagningar för automatiserad behandling som inte tillförs det enskilda målet eller ärendet.

Även när underlag från en sådan upptagning som här avses inte tillförs dokumentationen i det enskilda målet eller ärendet behöver en myndighet alltid kunna redogöra för var beslutsunderlaget finns, för att rättssäkra förfaranden och insyn i handläggningen av mål och ärenden ska kunna garanteras. Det bör därför enligt vår bedömning framgå klart i författning att myndigheter ska kunna upprätthålla spårbarhet till ett beslutsunderlag. Vi föreslår för tydlighets skull att detta kommer till uttryck genom ett tillägg till befintlig reglering som anger att myndigheten i den aktuella situationen ska se till att information kan lämnas om vilken eller vilka databaser eller andra digitala källor, t.ex. sensorer, filer eller andra lagringsplatser, som innehåller ett underlag för handläggningen av målet eller ärendet. Vi föreslår också att det görs språkliga justeringar i nuvarande 4 kap. 3 § offentlighets- och sekretesslagen för att förtydliga att det är just möjligheterna till insyn i underlag i mål eller ärenden som behöver säkerställas.

Den förändring som vi föreslår bör enligt vår bedömning även fungera som en god grund för fortsatta överväganden om en modernisering av informationsförsörjningen i den digitala förvaltningen, där uppgifter i högre utsträckning kan lämnas en gång och återanvändas inom förvaltningen.

[137] Se prop. 1985/86:80 s. 66.

Vi ser inte anledning att föreslå några detaljerade eller betungande krav om på vilket sätt myndigheter ska säkerställa spårbarhet till beslutsunderlag, utan bedömer att det lämpligen även i fortsättningen bör lämnas till tillämpande myndigheter att bestämma formerna för hur förmågan att spåra ett beslutsunderlag ska upprätthållas. Det finns också anledning att även här påminna om att uppgifter om vilken eller vilka databaser eller andra digitala källor som innehåller ett underlag för handläggningen av målet eller ärendet, kan omfattas av sekretess. I sådant fall ska information inte lämnas, även om myndigheten har förmågan att göra det.

Förhållande till dataskyddsregleringen

Den nu aktuella bestämmelsen i 4 kap. 3 § offentlighets- och sekretesslagen är inte begränsad till upptagningar för behandling av personuppgifter. Dataskyddsförordningen innehåller emellertid också reglering som rör rätten för den enskilde att få information om bl.a. varifrån personuppgifter kommer, och i förekommande fall om de har sitt ursprung i allmänt tillgängliga källor, i de fall uppgifterna inte har erhållits från den registrerade.[138] Den information som lämnas innan en personuppgiftsbehandling påbörjas bör omfatta uppgift om bl.a. vilken eller vilka databaser eller andra källor som kommer att användas. Givetvis går det inte att i förväg informera om utfallet av själva informationssökningen och huruvida denna har lett till beslutsunderlag i det enskilda fallet eller inte. En registrerad kan emellertid med stöd av rätten till tillgång i efterhand begära att få tillgång till sådan information.[139]

I viss utsträckning kommer rätten till information och rätten till tillgång enligt dataskyddsförordningen och det säkerställande av insynsmöjligheter som vi nu föreslår att bli överlappande i förhållande till varandra. Vår utgångspunkt är emellertid behovet av att

[138] Artikel 14.2 f.

[139] Artikel 15.1 g och h. Motsvarande bestämmelse i personuppgiftslagen (26 §) är begränsad genom att en registrerad enbart har rätt att få information efter ansökan en gång per kalenderår. Dataskyddsförordningen innehåller ingen direkt motsvarande begränsning men en personuppgiftsansvarig kan, om en begäran är uppenbart ogrundad eller orimlig, särskilt på grund av dess repetitiva art, ta ut en rimlig avgift för att tillhandahålla informationen eller vägra tillmötesgå begäran. Enligt 5 kap. 3 § förslaget till ny lag med kompletterande bestämmelser till EU:s dataskyddsförordning får regeringen meddela föreskrifter om ytterligare begränsningar av vissa rättigheter och skyldigheter enligt artikel 23 i dataskyddsförordningen, se prop. 2017/18:105.

säkerställa allmänhetens möjlighet till insyn i myndigheters beslutsunderlag, oavsett om det är personuppgifter som behandlas i ett visst beslutsunderlag eller inte, och inte enbart en rätt till insyn för en enskild registrerad.

Om det i någon situation skulle bli aktuellt att med stöd av den nu aktuella bestämmelsen i offentlighets- och sekretesslagen låta bli att tillföra uppgifter till den enskilda akten vid automatiserat individuellt beslutsfattande, inbegripet profilering, kan det säkerställande av möjligheter till insyn som vi föreslår också utgöra en lämplig åtgärd till skydd för den registrerades rättigheter, friheter och berättigade intressen.[140] Möjligheten att låta bli att tillföra beslutsunderlag till akten i enskilda mål eller ärenden kommer emellertid såvitt vi nu kan bedöma i högre grad att aktualiseras i andra typer av ärenden, t.ex. där stora datamängder används som beslutsunderlag såsom exempelvis i plan- och byggprocesser.

Rensning, arkivering, gallring eller bevarande av uppgifter vid källan

Det ligger i sakens natur att det via den spårbarhet som här är aktuell ska vara möjligt att få tillgång till beslutsunderlaget i den databas eller annan digital källa som har legat till grund för ärendehandläggningen. Detta aktualiserar i sin tur frågor om förutsättningar för rensning, arkivering, gallring eller bevarande av uppgifter vid källan.[141]

Under kartläggningen har flera aktörer tagit upp frågor som avser vikten av att vid myndighetssamverkan som rör informationsförsörjning också träffa överenskommelser om arkivansvar för att säkerställa att de uppgifter som är tillgängliga för flera myndigheter och som behöver bevaras inte endast momentant finns tillgängligt för insyn. Flera har också belyst svårigheterna med att i tillräcklig grad uppmärksamma dessa frågor vid utvecklingsarbeten.

Regeringen har nyligen gett en särskild utredare i uppdrag att göra en bred översyn av arkivområdet.[142] Det övergripande syftet med utredningen är att säkerställa samhällets tillgång till allmänna handlingar både nu och i framtiden. Utredaren ska bl.a. översiktligt

[140] Artikel 22.1 och 22.2 b dataskyddsförordningen.
[141] För gällande rätt om arkivering, se särskilt 3 § första stycket andra meningen arkivlagen och 4 § arkivförordningen (1991:446).
[142] *Översyn av arkivområdet* (dir. 2017:106).

beskriva arkivsektorn samt beskriva och analysera hur samhällsutvecklingen har påverkat och kan förväntas påverka förutsättningarna för arkivverksamheten och olika arkivinstitutioner. Utredaren ska också se över arkivlagstiftningen och närliggande lagstiftning och vid behov lämna förslag på hur lagstiftningen kan anpassas till utvecklingen på området. Med beaktande av arbetet i den nämnda utredningen finner vi inte anledning att här gå djupare i analyser eller författningsförslag som avser rensning, arkivering, gallring eller bevarande av beslutsunderlag, utan stannar vid att påtala vikten av att även dessa frågor får sin lösning.

7.7.4 Placering och tillämpningsområde

Utredningens förslag: De föreslagna bestämmelserna som rör god offentlighetsstruktur för insyn i förvaltningens ärendehantering vid vissa automatiserade förfaranden ska placeras i offentlighets- och sekretesslagen och följa den lagens tillämpningsområde.

Skälen för utredningens förslag: Den för förvaltningen gemensamma regleringen om god offentlighetsstruktur finns företrädesvis i offentlighets- och sekretesslagen. Det är också i den lagen som den nu gällande 4 kap. 3 § om överföring av beslutsunderlag till akten i det enskilda målet eller ärendet finns.

Vi har övervägt om det borde skapas en särskild lag för att där bl.a. införa de bestämmelser om god offentlighetsstruktur vid vissa automatiserade förfaranden som föreslagits i detta kapitel. Vi har dock stannat vid att regler om god offentlighetsstruktur i den digitala förvaltningen bör hållas samlade med de regler som redan gäller. Vi föreslår därför att den nya bestämmelsen om god offentlighetsstruktur genom förmåga att ge insyn vid vissa automatiserade förfaranden införs i offentlighets- och sekretesslagen och att 4 kap. 3 § i samma lag anpassas. Av den föreslagna placeringen i offentlighets- och sekretesslagen följer att den lagens tillämpningsområde gäller.

7.7.5 Konsekvenser av förslagen

På en övergripande nivå bedömer vi att förslagen om god offentlighetsstruktur för säkerställande av insynsmöjligheter i förvaltningens verksamhet när vissa automatiserade förfaranden används medför goda möjligheter till såväl effektivitetssprång i förvaltningens verksamhet som innovation i samhället i stort. Bland de områden som enligt vår bedömning kommer att präglas av en ökad grad av automation i framtiden, och som kommer att gagnas av den rättsliga tydlighet som förslagen medför, kan nämnas effektiva kontroller av utbetalningar i välfärdssystemen. Samtidigt som förslagen innebär att skyddet för enskilda stärks kan förslagen, om automationsåtgärder också vidtas, antas bidra till att minska brottsligheten genom brottspreventiv verkan eller öka uppklarningen av brott.

Genom att i ett första steg genomföra dessa förändringar bedömer vi också att det finns goda förutsättningar för dels fortsatt utvecklingsarbete i den digitala förvaltningen, dels fortsatt rättsutveckling för att möta den önskade verksamhetsutvecklingen.

Förslagen innebär inte några skyldigheter för myndigheter i förvaltningen att införa automatiserade förfaranden med algoritmer eller datorprogram i sin verksamhet. Förslagen har särskilt utformats för att inte i onödan vara betungande för myndigheter samtidigt som de stärker offentlighetsprincipen för allmänheten och rättssäkerheten för enskilda. Vårt förslag beträffande den goda offentlighetsstruktur som behövs för att kunna lämna information förutses därför inte leda till några beaktansvärda merkostnader. Eventuella merkostnader ska ses i förhållande till den effektivisering och kostnadsbesparing som övergången från manuella till automatiserade förfaranden medför. Om merkostnader uppkommer till följd av att förslagen omfattar även förfaranden som redan har automatiserats vid tidpunkten för ikraftträdande förutsätts dessa bli marginella och ska finansieras inom befintliga ramar.

Utvecklingen i fråga om vilka insynsmöjligheter som ska gälla i förvaltningen följer nu gällande ordning, där offentlighets- och sekretesslagens krav gäller också för kommunala och landstingskommunala myndigheter. Förslagen vi lämnar får därmed inte i sig någon nytillkommen konsekvens för den kommunala självstyrelsen.

Förslagen har också utformats så att inte några negativa konsekvenser ur konkurrenssynpunkt i förhållande till kommersiella

aktörer ska uppkomma. Möjligheterna till samverkan med det privata näringslivet för att utveckla innovativa och effektiva lösningar stärks. Förslagen har också utformats för att vara väl avvägda i förhållande till eventuellt immaterialrättsligt skydd i form av bl.a. upphovsrätt för datorprogram som kan föreligga, varför några negativa konsekvenser i dessa hänseenden inte kan förväntas.

Förslaget till anpassning av bestämmelsen om beslutsunderlag i enskilda ärenden bedöms kunna förenkla vid överväganden om hur myndigheters informationshantering i den digitala förvaltningen ska gå till. Enligt vår uppfattning bör de föreslagna anpassningarna ge en god grund för fortsatt arbete med att utveckla förvaltningsgemensamma lösningar där uppgifter i högre grad lämnas en gång till förvaltningen och återanvänds från den bästa källan.

Förslagen kan härutöver inte förväntas leda till andra konsekvenser än de generella konsekvenser av våra förslag som redovisas i kapitel 14.2.

7.8 Ytterligare överväganden för en AI-redo förvaltning

7.8.1 Samspelet mellan rättsutveckling och teknikutveckling

De tendenser vi ser är att användandet av artificiell intelligens (AI) kommer att bli allt mer centralt i samhällets digitalisering, och därmed även i förvaltningens förändringsarbete. Flera länder genomför just nu stora satsningar inom området.

Det står redan klart att AI används och har potential att användas för viktiga förbättringar i samhället och även inom den svenska förvaltningen. Här kan inte alla möjligheter med användandet av den tekniken presenteras. Övergripande handlar det emellertid om att förvaltningens verksamhet och service gentemot enskilda kan effektiviseras och förbättras inom sektorer som t.ex. hälso- och sjukvård, utbetalningar från välfärdssystemen eller brottsbekämpning liksom när det gäller effektiva förfaranden vid olika myndigheters ärendehantering och vid service. Ett konkret exempel på områden där användande av artificiell intelligens kan komma förvaltningen och enskilda individer till nytta rör användande av tekniken för att ta fram beslutsstöd åt läkare vid diagnosticering av sjukdomar.

Att den nya tekniken också är förenad med att nya risker behöver hanteras har vi kort presenterat i kapitel 7.5. Viktiga frågor behöver besvaras för att användandet av AI inom förvaltningen inte ska skapa nya problem. Användningen av den nya tekniken kräver med andra ord ett flertal överväganden, även av rättslig karaktär. Det bör framhållas att vi inom ramen för vårt uppdrag endast har att utreda de rättsliga förutsättningarna för digitalisering inom just förvaltningen, och inte för samhället i stort.

Inom bl.a. forskningen har det under flera år pågått en debatt om flera av dessa frågor. En debatt som rör såväl den tekniska utvecklingen som etiska och rättsliga aspekter på densamma. Så här långt har den utmynnat i att vissa organisationer eller grupperingar har antagit eller fastslagit ett antal principer.[143] Principerna innehåller även rättsliga ställningstaganden. Bland annat synes det så här långt i en internationell kontext råda enighet om att det ska föreligga en öppenhet såtillvida att all inblandning av autonoma system i rättsligt beslutsfattande ska erbjuda en tillfredsställande förklaring som är reviderbar av en myndighet med mänskliga förfaranden.

I takt med att den nya tekniken tas i tillämpning i samhället och inom förvaltningen räcker det emellertid inte med principiella uttalanden. Det behövs ställningstaganden om vad som ska vara rättsligt bindande respektive inte. Ett problem i det hänseendet med den typ av principer som har antagits av olika organisationer eller grupperingar är att de utgår från en viss teknik, nämligen artificiell intelligens. Rättssystemet är ordnat efter en annan logik. Utgångspunkten för rättsregler är normalt att reglera en viss verksamhet eller ett visst förfarande, och strävan i vart fall från den svenska riksdagen och regeringen har som tidigare beskrivits länge varit att åstadkomma en teknikneutral reglering. De nämnda principerna om just artificiell intelligens tar inte i beaktande vilka rättsregler som redan finns, dvs. vad som redan krävs enligt gällande rätt.

Som exempel med anknytning till den ovan nämnda principen kan framhållas kraven i bl.a. förvaltningslagen på att skäl för beslut, med vissa möjligheter till undantag, ska framgå. Möjligheter till omprövning eller överprövning av beslut är också fundamentala

[143] Se t.ex. Asilomar AI Princiles, antagna vid 2017 Asilomar Conference, på https://futureoflife.org/ai-principles/ och principer antagna av Association for Computing Machinery US Public Policy Council (USACM) på http://www.acm.org/binaries/content/assets/publicpolicy/2017_usacm_statement_algorithms.pdf

komponenter i en rättssäker förvaltning och framgår redan i gällande rätt. Det som i stället kan behöva övervägas är om våra förfaranden, och de kunskaper som finns hos tjänstemän vid de instanser vi har, kommer att vara tillräckliga om beslut ska fattas av algoritmer som har möjlighet att beakta långt fler faktorer än en människa någonsin kan hantera och ta hänsyn till enorma mängder indata. Bland annat av den anledningen ser vi, såväl som andra vi talat med under utredningen, att förvaltningen i ett första läge inte i någon större utsträckning kommer att utnyttja den nya tekniken för att på egen hand fatta beslut med konsekvenser för enskilda. Snarare kan vi se framför oss en utveckling där sådan teknik i förstone kommer att användas vid analys, som beslutsstöd åt mänskliga befattningshavare eller för service. På det sättet kan, åtminstone till en början, nyttorna med den nya tekniken komma förvaltningen till del utan att beslutsfattandet helt övertas av datorprogram.

För att åstadkomma goda rättsliga förutsättningar för användande av AI inom förvaltningen ser vi inte heller anledning att gå ifrån den gängse metoden för rättsutveckling. Den innebär i likhet med våra överväganden i kapitel 7.6 att fortsatt undersöka om rättsregler behöver upphävas eller ändras eller om det saknas rättsregler för att åstadkomma rättsliga förutsättningar för den utveckling som är önskvärd. Generella överväganden om fördelning av ansvar och risker och i vilken utsträckning en samhällsförändring är så stor att riksdag eller regering bör leda vägen bör i det sammanhanget också göras. Vi återkommer också i kapitel 7.9.1 till överväganden om behovet av att i olika avseenden och oberoende av vilken teknik som används automationsanpassa lagstiftningen.

Eftersom möjligheterna och utmaningarna med AI, och särskilt maskininlärda algoritmer, är så påtagliga ser vi emellertid behov av att först uppehålla oss särskilt vid åtgärder som syftar till att förbättra de rättsliga förutsättningarna för att använda just denna teknik inom förvaltningen.

I det föregående kapitel 7.7 har vi lämnat de förslag som vi i ett första steg ser behövs för en i högre grad automatiserad förvaltning som också tar stöd av ny teknik med artificiell intelligens. Det måste ses som en grundläggande faktor för tilliten till en förvaltning som använder AI att myndigheter säkerställer att de, oavsett om myndigheten utvecklar egna lösningar eller om utvecklingen på ett eller annat sätt äger rum i samverkan med det privata näringslivet, kan

lämna information om hur de använder algoritmer eller datorprogram som helt eller delvis påverkar utfallet eller beslutet vid automatiserade urval eller beslut.

Det behövs emellertid ytterligare överväganden om hur rättsutvecklingen kan eller bör möta behovet av att använda AI inom den offentliga förvaltningen.

7.8.2 Rättssäkra förfaranden i en samverkande förvaltning

Utredningens bedömning: Det är för tidigt att i detta skede av teknikutvecklingen inom förvaltningen föreslå ytterligare reglering som särskilt föranleds av eller avser att träffa förvaltningens användning av artificiell intelligens (AI) med maskininlärda algoritmer.

Utredningens förslag: Regeringen uppdrar åt myndigheter som tillämpar eller överväger att tillämpa AI-system med maskininlärda algoritmer i sin verksamhet att – i samverkan med Sveriges Kommuner och Landsting, Myndigheten för digital förvaltning och tillsynsmyndigheter inom digital förvaltning – utarbeta förslag på förfaranden som innebär att tredje part kan utöva revision, tillsyn, certifiering eller annan typ av kontroll avseende de algoritmer som kommer att användas. Särskild vikt bör läggas vid de algoritmer som, helt eller delvis, påverkar utfallet vid urval eller beslut.

Det ska ingå i uppdraget att söka samverkan med det privata näringslivet och forskningssamhället liksom att bevaka den internationella utvecklingen.

I uppdraget ska också ingå att redovisa för regeringen om myndigheternas tillämpning, eller planerad eller tänkbar tillämpning av AI med maskininlärda algoritmer bör föranleda anpassning eller komplettering av gällande rätt.

Skälen för utredningens bedömning och förslag

Bättre förutsättningar för hantering av rättsliga utmaningar

Det kommer att krävas ett samspel mellan reglering och andra åtgärder för att åstadkomma goda möjligheter till AI-baserade förfaranden i förvaltningen som både är rättssäkra och kan visas vara detta. Det kommer visserligen inte att vara möjligt för hela förvaltningen och alla de olika men specifika användningsområden som finns för AI att omhänderta risker för bl.a. rättsosäkerhet på ett och samma sätt. Flera frågor som förvaltningen kommer att ställas inför, och i viss utsträckning redan gör, i samband med teknikutvecklingen kommer emellertid att vara gemensamma. Här avses bl.a. det som anförts i kapitel 7.5.2 om ansvar för tekniken och dess användning, om eller när beslutsstöd blir så tekniskt avancerade att det snarare är ansvaret för funktionen i de algoritmer eller datorprogram som används som behöver diskuteras, än de enskilda besluten där de automatiskt genererade beslutsunderlagen används. Här avses också omhändertagande av risk för att maskininlärda algoritmer medvetet eller omedvetet ”smittas” med felkällor eller felaktiga utgångspunkter med rättsosäkra eller diskriminerande förfaranden som följd. Även risker för att algoritmerna medvetet manipuleras för att orsaka ekonomisk eller personlig skada behöver beaktas.

Enligt vår bedömning är utvecklingen av användande av AI-system med maskininlärning inom förvaltningen ett område som lämpar sig väl för samverkan, såväl inom förvaltningen som i förhållande till privata näringslivet och forskarsamhället. Enligt vår uppfattning finns i och för sig inte något hinder mot att ett sådant uppdrag i stället lämnas till en särskild utredare. Oavsett uppdragstagare bör emellertid ett brett samråd såväl inom förvaltningen som i förhållande till privata aktörer eftersträvas.

Träning av algoritmer

Som framgått i kapitel 7.3.2 innebär maskininlärning att logiken inte längre är statisk, dvs. exakt programmerad på förhand, utan (förenklat beskrivet) tränas på stora datamängder med syfte att själv förstå samband mellan datapunkter.

En tillämpning av artificiell intelligens som är utformad med system för maskininlärning kan inte genast tas i bruk för att t.ex. ge service, göra ett urval eller stödja beslutsfattande genom att lämna underlag. Det krävs en period av träning för att systemet sedan ska kunna användas för att utföra dessa arbetsuppgifter. Ju mer träning, desto ”duktigare” blir de maskininlärda algoritmerna. För att det ska vara möjligt för en algoritm att förbättra sig själv krävs vidare att den har tillgång till stora mängder data. Mängden data som används vid denna träning kan i sig vara en nödvändig faktor för att kunna garantera rättssäkra förfaranden. Av rättssäkerhetsskäl krävs dessutom att träningen ägt rum med just den typ av data som sedan ska användas i skarpa fall. Om dessa förutsättningar inte ges kan inte tillräckligt kvalitativa svar, beslutsunderlag eller beslut lämnas när system med maskininlärda algoritmer tas i skarp drift. Med andra ord ökar risken för fel och rättsosäkerhet om dataunderlaget varit bristfälligt under AI-systemets ”upplärningsprocess”.

Processen med maskininlärning innebär vidare att algoritmen är föränderlig. Som vi har fått det förklarat för oss är den också, i varierad utsträckning beroende på efter vilken modell den har utformats, dunkel att tränga in i. Vissa använder begreppet ”svart låda”i den bemärkelsen att det inte går att fullt ut förstå vilka steg som har tagits när algoritmen kommit fram till sitt utfall, i vart fall inte för gemene man och såvitt vi förstår inte för någon människa om det rör sig om komplicerade neurala nätverk. I viss utsträckning skulle det kanske gå att jämföra processen med den bearbetning som görs i våra mänskliga hjärnor. AI-området är också föremål för snabb teknikutveckling, bl.a. när det gäller just systemens förmåga att kunna förklara sina utfall för oss människor.[144]

Vikten av att det finns goda förutsättningar för att träna AI-system med maskininlärda algoritmer innan de tas i bruk för att ge service eller komma med beslutsstöd etc. gör att det uppkommer rättsliga frågor redan på detta stadie. Här har vi inte möjlighet att ge generella svar på samtliga, men vill särskilt uppmärksamma att det av rättssäkerhetsskäl behöver finnas förutsättningar för att dessa algoritmer redan när de tränas har tillgång till stora datamängder av samma typ som kommer att användas i skarpa lägen. Om de datamängder som är nödvändiga för träningen kommer att innehålla

[144] Se t.ex. artikel på https://futureoflife.org/2017/09/27/explainable-ai-a-discussion-with-dan-weld/

personuppgifter behöver det därför finnas förutsättningar för datainsamlingen och behandlingen enligt dataskyddsregleringen redan på stadiet då algoritmen tränas. I de fall insamlingen eller behandlingen av uppgifter hindras av gällande rätt, t.ex. snävt formulerade ändamålsbestämmelser i de registerförfattningar som ska tillämpas eller bestämmelser om sekretess som hindrar att uppgifter samlas in, behöver författningsändringar göras redan på stadiet när algoritmerna ska tränas.

Som framgått av den korta beskrivningen ovan kommer den träning eller ”utbildning” som ett AI-system med maskininlärda algoritmer får att vara av stor betydelse för förmågan att i skarpa lägen ge t.ex. kvalitativa beslutsunderlag. Myndigheter bör därför enligt vår bedömning se till att upprätthålla en förmåga att ge information om hur träningen av dess maskininlärda algoritmer har gått till. Detta förfarande skulle i viss mån kunna jämföras med att myndigheter när det efterfrågas i dag har förmåga att redogöra för t.ex. vilken utbildning en handläggare vid myndigheten har.

Vi har övervägt att, i linje med vårt förslag i kapitel 7.7.2, mer detaljerat föreslå en reglering med explicit innebörd att en myndighet ska ha förmåga att kunna ge information om hur framtagandet av maskininlärda algoritmer som, helt eller delvis, påverkar utfallet eller beslutet vid automatiserade urval eller beslut har gått till. Vi har emellertid stannat vid att det är för tidigt att i detta skede av teknikutveckling inom förvaltningen uttryckligen reglera det sagda i författning, men det är vår uppfattning att myndigheter i linje med den generella reglering som föreslås i kapitel 7.7.2 behöver säkerställa att den förmågan finns när tekniken börjar användas.

Indata och beslutsunderlag

Att myndigheter ska ha kontroll över vilka typer av indata de använder i sina automatiserade förfaranden framgår i såväl dataskyddsregleringen som arkivregleringen (se kapitel 7.6.1 respektive 7.6.3). När en övergång görs till att nyttja maskininlärda algoritmer, som ovan beskrivits kunna vara i varierad grad ”dunkla” i den bemärkelsen att de är svåra att tränga in i, framstår det enligt vår uppfattning som än viktigare att välgenomtänkta beslut tas i fråga om vilka kategorier av uppgifter som algoritmen ska få behandla.

Vi har därför övervägt om det nu borde införas ytterligare reglering med uttryckliga och mer detaljerade krav på att kontrollera och dokumentera vilka indata som används när maskininlärda algoritmer tillämpas. Vi har emellertid, i linje med vad som framgått ovan, stannat vid att i vart fall i detta skede av teknikutveckling inte finns anledning att föreslå sådan specifik ytterligare reglering. Det är dock vår uppfattning att det, i enlighet med det generella krav som föreslås i kapitel 7.7.2, är av stor vikt att de regler som finns i fråga om dokumentation och öppenhet i fråga om vilka indata som används också tillämpas. Det kommer att vara av påtaglig vikt för tilliten till denna typ av automatiserade förfaranden att förvaltningen förmår förklara och redovisa vilket underlag algoritmen utgått ifrån, utöver hur den tränats för att komma fram till sina resultat.

Ytterligare en aspekt att hålla i åtanke inför att i framtiden låta AI-system med maskininlärda algoritmer stå för faktiskt beslutsfattande är att synliggöra vad som kommer att vara beslutsunderlaget. Är det enbart vissa uppgifter som rör ett individuellt ärende som kommer att utgöra beslutsunderlaget, eller blir all indata som algoritmen hanterat under sin träning och vid tillämpning i tidigare ärenden att fungera som beslutsunderlag? Om det sistnämnda blir fallet ser vi behov av att också särskilt uppmärksamma frågor som hur t.ex. omprövning eller överprövning ska gå till och vilken kompetens som kommer att krävas vid sådana förfaranden.

Uppdraget

Vårt förslag i kapitel 7.7.2 om förmåga att ge insyn i vissa automatiserade förfaranden bör fungera som en bas för att också ge goda rättsliga förutsättningar för rättssäkra AI-tillämpningar inom förvaltningen.

I stället för att i detta skede av teknikutveckling inom förvaltningen lämna ytterligare författningsförslag bedömer vi att det är lämpligt att regeringen ger ett särskilt uppdrag åt de myndigheter som tillämpar eller överväger att tillämpa AI-system med maskininlärda algoritmer i sin verksamhet att i samverkan utarbeta förslag som stärker tilliten och rättssäkerheten. Vi föreslår att regeringen specificerar att det ska ingå i uppdraget att lämna förslag på förfaranden som innebär att tredje part kan utöva revision, tillsyn,

certifiering eller annan typ av kontroll avseende de algoritmer som kommer att användas. Särskild vikt bör läggas vid de algoritmer som, helt eller delvis, påverkar utfallet vid urval eller beslut.

Uppdraget bör riktas mot de myndigheter under regeringen som tillämpar eller överväger att tillämpa AI-system med maskininlärda algoritmer i sin verksamhet. Samverkan bör äga rum även med Sveriges Kommuner och Landsting, Myndigheten för digital förvaltning, Datainspektionen[145] och Myndigheten för samhällsskydd och beredskap. Det bör också ingå i uppdraget att söka samverkan med det privata näringslivet och forskarsamhället liksom att bevaka den internationella utvecklingen.

Med beaktande av det som har anförts om behovet av att omhänderta risker för rättsosäkerhet bör det också ingå i uppdraget att myndigheterna ska redovisa för regeringen om myndigheternas tillämpning eller planerad eller tänkbar tillämpning av AI-system med maskininlärda algoritmer bör föranleda anpassning eller komplettering av gällande rätt. I detta ligger även att uppmärksamma regeringen på eventuella behov av författningsändringar för att t.ex. samla in och behandla de uppgifter som behövs för de förfaranden som planeras eller är önskvärda.

Konsekvenser av förslaget

Ett samverkansuppdrag från regeringen med inriktning på att utarbeta förslag som syftar till att åstadkomma trygga och rättssäkra AI-tillämpningar inom förvaltningen kan förväntas bidra till att kunskapen om tekniken sprids till flera och gagna innovation och effektivitet i svensk förvaltning. En sådan utveckling kan också gagna t.ex. sysselsättningen i Sverige.[146] Ett samverkansuppdrag av detta slag skulle också, och i huvudsak, syfta till att åstadkomma en sådan teknikanvändning inom förvaltningen på ett sätt som både är och kan visas vara rättssäkert. Uppdraget kan genomföras inom ramen för deltagande myndigheters anslag. Se även kapitel 14.2 om generella konsekvenser av våra förslag.

[145] Datainspektionen byter namn till Integritetsskyddsmyndigheten under år 2018.
[146] Jfr också norska Datatilsynets rapport *Kunstig inelligens og personvern*, januari 2018.

7.8.3 Ett kunskapsperspektiv

Artificiell intelligens med maskininlärda algoritmer har mycket stor potential att användas för olika former av analyser. När förvaltningen nu anordnar nya former för informationshantering, vare sig det rör sig om informationsförsörjning i form av öppna data eller mer specifika digitala informationsutbyten myndigheter emellan, är det enligt vår bedömning viktigt att även kunskapsperspektivet finns med när krav på t.ex. informationsstandarder diskuteras. Ibland kan också frågan om särskilda och nya informationsutbyten behöva diskuteras med anledning just av att åstadkomma förutsättningar för ny kunskap genom analys av digitala informationsflöden eller datamängder.

Det är med andra ord inte bara de rättsliga förutsättningarna för att utbyta information i en befintlig ärendeprocess som behöver hållas i åtanke vid digitalisering av processen ifråga. När utvecklingsarbetet pågår kan det också vara lämpligt att samtidigt överväga om det finns särskilda behov av att förbättra de rättsliga förutsättningarna för att anordna informationsflödena så att det ges bättre möjligheter för att med stöd av den nya tekniken göra olika former av analyser. Sådana analyser kan ge ökad kunskap om t.ex. hanteringen i en ärendeprocess, utfall, flaskhalsar eller andra former av underlag för bl.a. styrning (se kapitel 7.2.4).

7.9 Automationsanpassad lagstiftning

7.9.1 Gällande rätt med materiella bestämmelser

Utredningens bedömning: Om gällande materiell rätt lämnar ett visst utrymme för individuella bedömningar vid beslut, utgör det inte något generellt hinder mot automation av förfaranden som hittills har hanterats av människor.

Vid övergång från ett manuellt till ett automatiserat förfarande behöver det emellertid alltid övervägas om det är möjligt och lämpligt att en myndighet omsätter bedömningsutrymmen i gällande rätt till algoritmer med anknytande datorprogram, eller om förfarandet kan automatiseras endast under förutsättning att lagstiftningen anpassas.

Skälen för utredningens bedömning

Materiell rätt med bedömningsutrymmen och automatiserade beslut

Under kartläggningen har vi tagit del av exempel där lagstiftningen i gällande rätt i varierad utsträckning innehåller ett bedömningsutrymme i samband med beslutsfattande, men där hittillsvarande förfaranden vid manuell handläggning respektive utfallen vid beslut i praktiken ändå har blivit relativt likriktade. Bland myndigheter som hittills inte tillämpat automatiserade beslut har vi uppfattat tankar om att den typen av beslut borde kunna automatiseras.[147]

Vissa av de rättsregler som här avses har nog tillkommit i en tid då det inte alls varit aktuellt att åstadkomma rättssäkra beslutsförfaranden på annat sätt än genom manuell ärendehandläggning och beslutsfattande. Det har därför kanske inte gjorts några särskilda överväganden om hur lagtextens formuleringar om bedömningsutrymmet exakt borde utformas. Att materiell rätt lämnar olika grader av utrymme för bedömningar i enskilda fall vid förvaltningsbeslut kan därför enligt vår mening inte sägas utgöra något generellt och av lagstiftaren avsett hinder mot automation. Den slutsatsen stärks av uttalanden i propositionen med förslag till ny förvaltningslag, där det framgår att avsikten med att i förvaltningslagen slå fast att beslut kan fattas automatiserat har varit att det inte ska behövas en reglering i en specialförfattning för att en myndighet ska kunna använda denna beslutsform.

Under förutsättning att de risker som finns (se kapitel 7.5) uppmärksammas och hanteras i samband med en planerad automatiseringsåtgärd är det enligt vår bedömning många gånger möjligt för en myndighet att automatisera förfaranden utan att varje sådan åtgärd inom förvaltningen föregås av ändringar i den materiella lagstiftningen. Här kan paralleller dras till manuella förfaranden som i hög grad redan har likriktats hos myndigheter genom rutiner, handböcker, checklistor etc., utan att sådana detaljerade instruktioner har ansetts behöva framgå direkt i lagstiftningen. I kapitel 6.2 har också belysts att lagstiftning på områden som står under snabb utveckling som utgångspunkt inte bör belastas med detaljerade regler.

Även med beaktande av det ovan sagda kan det dock i några fall vara lämpligt, och i vissa fall krävas, att författningsändringar föregår

[147] Det skulle t.ex. kunna gälla beslut om utbetalning av särskilt bidrag för inköp av vinterkläder enligt 18 § lagen (1994:137) om mottagande av asylsökande m.fl.

en övergång till automatiserade förfaranden. Som framgått av beskrivningen i kapitel 7.5 är det inte möjligt att bedöma frågor om rättssäkerhet vid förvaltningens automationsåtgärder på ett sätt som är entydigt och enhetligt för all ärendehandläggning och beslutsfattande inom hela den offentliga förvaltningen. Risker för rättsosäkerhet kommer att behöva bedömas och hanteras beroende på vilket förfarande det är som avses vid överväganden om automation.

Ett exempel på hur risker skulle kunna hanteras i vissa fall är genom urval av individuella ärenden som behöver hanteras manuellt för att säkerställa ett utfall som är av tillräcklig kvalitet för att vara rättssäkert i det individuella fallet, även när ärendetypen generellt skulle kunna hanteras med automatiserade förfaranden. I andra fall kanske det är fråga om den typ av beslut där den part som är missnöjd med ett automatiskt fattat beslut kan återkomma med en särskild begäran om ny prövning, omprövning eller överprövning för korrigering av beslutet utan att riskera att drabbas av rättsförluster. Om den omprövningen eller överprövningen sköts på ett sätt som gör att hänsyn kan tas till t.ex. individuella omständigheter som det automatiserade förfarandet inte beaktat kan det enligt vår bedömning finnas fall där hela ärendeprocessen kan automatiseras fram till ett första beslut utan att någon betydande risk för rättsosäkerhet uppstår.

I åter andra fall kan det kanske vara lämpligt att lagstiftaren omhändertar vissa risker för felaktiga bedömningar när automatiserade förfaranden bedöms vara önskvärda, genom att t.ex. överväga särskilda regler om hur rättelse eller omprövning ska gå till.[148] Vi ser inte möjlighet att nu lämna förslag om vad som bör vara en lämplig ordning för alla typer av beslut som fattas och kommer att fattas automatiserat i förvaltningen. Vi ser dock inte heller att det bör göras några särskilda begränsningar med avseende på att vissa beslut inte får fattas automatiserat utan särskilt lagstöd för det. Även beslut som t.ex. har negativ innebörd för den enskilde bör alltså enligt vår bedömning kunna fattas automatiserat om det finns förutsättningar att ta hand om risker för rättsosäkerhet.

En anpassning av lagstiftningen på förhand kan också vara lämplig om automation övervägs på områden där bedömningsutrymmet i den gällande materiella rätt som ska tillämpas vid beslutsförfarandet

[148] Jfr t.ex. 18 kap. 5 och6 §§ förordningen) om vägtrafikregister, med särskilda regler om omprövning av beslut som fattas automatiserat.

är mycket stort eller oklart och det därtill finns risk för att en myndighet i arbetet med att automatisera ett beslutsförfarande bortser från viktiga bedömningsmoment.[149]

En anpassning av gällande rätt kan emellertid också krävas när det är fråga om beslut av särskild betydelse för den enskilde, för att också säkerställa ett konstitutionellt förankrat förfarande. Som angetts ovan menar vi inte här att t.ex. automatisering av varje beslutsförfarande som kan leda till negativa förvaltningsbeslut måste föregås av särskilda lagstiftningsåtgärder för att ge författningsstöd åt beslutsformen utöver förvaltningslagens reglering. Om automation däremot skulle övervägas på områden som rör ingrepp av särskilt stor betydelse för den enskilde, som exempelvis rör beslut om tvångsåtgärder eller åtgärder av liknande karaktär, bör det enligt vår bedömning finnas särskild anledning att riksdagen eller regeringen leder vägen genom översyn av regleringen på förhand. Det följer även av dataskyddsregleringen att det som huvudregel är förbjudet att basera automatiserade beslut enbart på känsliga personuppgifter.[150]

Utöver det som ovan anförts bör det hållas i åtanke att ny teknik med exempelvis maskininlärda algoritmer står för dörren. Synsättet att automatiserade förfaranden kräver helt styrande regler i form av rättsregler eller datorrelaterade regler kommer därmed sannolikt att behöva justeras med beaktande av den snabba teknikutvecklingen på området för artificiell intelligens. Tekniska förutsättningar får med andra ord också betydelse vid överväganden om den materiella rätt som tillämpas vid beslutsfattande bör eller behöver anpassas inför övergångar till helt eller delvis automatiserade förfaranden i förvaltningen.

Uppstår behov av att reglera nya ansvarsförhållanden?

Ett annat skäl till att en anpassning av den materiella rätten kan krävas på förhand är att automationen kan föra med sig nya rättsfrågor, t.ex. avseende vilken aktör som bör hållas ansvarig vid fel. En riskanalys inför ett förändringsarbete kan exempelvis leda till att det bedöms vara nödvändigt att sådana rättsfrågor besvaras på

[149] Jfr Inspektionen för socialförsäkringensarbetsrapport *Individuell eller standardiserad socialförsäkring – En diskussion för mer rättssäker handläggning*, 2015:3, s. 27.
[150] Se artikel 22.4 dataskyddsförordningen och 2 kap. 19 § förslag till brottsdatalag,SOU 2017:29.

förhand genom ansvarsfördelning i rättsregler, innan helt automatiska förfaranden börjar tillämpas. Det kan t.ex. röra sig om förfaranden på förvaltningens område för faktiskt handlande om mänskliga åtgärder ska ersättas med automatiserade eller robotiserade förfaranden. Vi har inom ramen för kartläggningen, i det stadie av utveckling förvaltningen nu befinner sig, inte stött på konkreta exempel på när automation inom förvaltningen medfört sådana nya behov av att fördela ansvar. Paralleller kan emellertid dras till exempelvis utvecklingen med självkörande fordon där det pågår debatt om bl.a. hur ansvarsfördelningen mellan förare och fordonsutvecklare ska se ut.[151]

När det gäller utvecklingen av just självkörande fordon har lagstiftare i flera länder valt att formulera rättsregler i försökslagstiftning, under tiden som utvecklingsarbete pågår. Det är en metod som vi ser sannolikt kommer att behövas på fler områden där det finns behov av att möta risker, t.ex. när det gäller att fördela ansvar, samtidigt som utveckling pågår.

7.9.2 Gällande rätt om automatiserat beslutsfattande

Utredningens bedömning: Befintlig särreglering av automatiserat beslutsfattande i lag och förordning, vid sidan av förvaltningslagen, bör upphävas i enlighet med E-delegationens förslag i betänkandet *Automatiserade beslut – färre regler ger tydligare reglering*.

Skälen för utredningens bedömning

Bakgrund

Hur förvaltningsmyndigheter under regeringen ska handlägga sina ärenden regleras bl.a. i myndighetsförordningen (2007:515). När det gäller formerna för ett ärendes avgörande och det materiella beslutet i fråga framgår av förordningen att ärenden som huvudregel avgörs

[151] Se t.ex. Utredningen om självkörande fordon på vägs delbetänkande *Vägen till självkörande fordon – försöksverksamhet* (SOU 2016:28) och slutbetänkande *Vägen till självkörande fordon – introduktion* (SOU 2018:16).

efter föredragning och att det för varje beslut i ett ärende ska upprättas en handling som bl.a. visar beslutets innehåll, vem som har fattat beslutet och vem som har varit föredragande. [152]

Bestämmelserna i myndighetsförordningen har tolkats som att det generellt sett behövs ett undantag för att myndigheter ska kunna fatta helt automatiserade beslut.[153] Sådana undantag har införts i vissa myndigheters instruktion, bl.a. för Bolagsverket, Försäkringskassan och Skatteverket.[154] I andra fall har särreglering införts i t.ex. registerförfattning. Här kan nämnas att Transportstyrelsen enligt förordningen om vägtrafikregister får fatta beslut genom automatiserad behandling av uppgifter i vägtrafikregistret.[155] Lagstiftaren har alltså valt olika författningstekniska lösningar för att möjliggöra för myndigheter att fatta automatiserade beslut. Regleringen har emellertid skapat osäkerhet eftersom den leder till motsatsvisa tolkningar, dvs. att myndigheter ser hinder mot att fatta automatiserade beslut när det saknas uttryckliga förskrifter som tillåter detta.

E-delegationens betänkande om automatiserade beslut

I ett betänkande från 2014 har E-delegationen pekat på att den pågående automatiseringen av myndigheternas beslutsfattande hämmas av onödiga och onödigt komplicerade regler.[156] E-delegationen framhöll att regleringen borde förenklas så att det inte råder någon osäkerhet om att beslut får fattas automatiserat. Mot denna bakgrund föreslog E-delegationen dels att författningsbestämmelser om att beslut får fattas automatiserat borde upphävas, dels att ett generellt undantag från 20 § och 21 § 3–5 i myndighetsförordningen borde införas. Majoriteten av remissinstanserna ställde sig generellt positiva till delegationens förslag men förslagen har ännu inte lett till författningsändringar.

---

[152] 20 och 21 §§ myndighetsförordningen.
[153] Se bl.a. JO:s protokoll, dnr 4728–2011.
[154] 14 § förordningen (2007:1110) med instruktion för Bolagsverket, 39 § förordning (2017:154) med instruktion för Skatteverket och 14 § förordning (2009:1174) med instruktion för Försäkringskassan.
[155] 18 kap. 5 § förordning om vägtrafikregister.
[156] Se E-delegationens betänkande, *Automatiserade beslut – färre regler ger tydligare reglering* (SOU 2014:75).

Förvaltningslagen

I förvaltningslagen framgår det numera uttryckligen att ett beslut kan fattas automatiserat.[157] Genom att det i lagen slås fast att beslut kan fattas automatiserat tydliggörs att det inte behövs en reglering i specialförfattning för att en myndighet ska kunna använda denna beslutsform.[158]

I förvaltningslagen har det därtill införts en bestämmelse som till sitt innehåll har sin förebild i 21 § myndighetsförordningen, dvs. den reglerar vilken dokumentation som ska tillföras ett beslut, bl.a. vad beslutet innehåller, vem eller vilka som har fattat beslutet och vem eller vilka som varit föredragande.[159] I förarbetena till bestämmelsen förklaras att i den utsträckning ett beslut fattas hos en myndighet helt på automatiserad väg saknas underlag för dokumentation av i vart fall delar av den information som anges som obligatorisk. Avsikten är att paragrafen för dessa fall ska tillämpas i enlighet med den praxis som har kommit till uttryck vid tillämpningen av motsvarande bestämmelse i 21 § myndighetsförordningen. Det finns i ett sådant fall t.ex. inte någon uppgift om föredragande eller uppgift om viss person som är beslutsfattare. Det räcker då att dokumentationen omfattar de uppgifter som är relevanta och aktuella för det enskilda ärendet, exempelvis uppgift om datum för beslutet och dess innehåll.[160] Enligt regeringens mening finns det inget behov av en särskild regel för dokumentation av automatiserade beslut.[161]

Förvaltningslagen är emellertid subsidiär och ska inte tillämpas om en annan lag eller förordning innehåller någon bestämmelse som avviker från lagen.[162] Det innebär att om det finns specialreglering i lag eller förordning som styr myndigheters möjlighet att fatta automatiserade beslut gäller denna i första hand.

[157] 28 § förvaltningslagen.
[158] Prop. 2016/17:180 s. 180.
[159] 31 § förvaltningslagen.
[160] A. prop. s. 319 f.
[161] A. prop. s. 185 f.
[162] 4 § förvaltningslagen.

Kartläggningsresultatet

I kartläggningsarbetet har framkommit att myndigheter generellt välkomnar regleringen om automatiserade beslut i den nya förvaltningslagen. Ett antal myndigheter har emellertid att tillämpa särreglering vad avser automatiserat beslutsfattande. För dessa myndigheter kvarstår viss rättslig osäkerhet om när, och i vilken utsträckning, det är tillåtet att fatta automatiserade beslut mot bakgrund av att särreglering har företräde framför förvaltningslagens bestämmelser. Exempelvis regleras, som tidigare nämnts, i förordningen om vägtrafikregister att beslut får fattas genom automatiserad behandling av uppgifter i vägtrafikregistret.[163] När bestämmelsen togs fram föranleddes den såvitt vi fått förklarat för oss av beslut som rörde fordonsregistreringen, vilket också är det område som i övrigt sakligt regleras i förordningen. Vid en läsning av bestämmelsen i sitt sammanhang i förordningens 18 kap. kan regleringen tolkas som att det bara är beslut om fordonsregistrering som får fattas genom automatiserad behandling av uppgifter i vägtrafikregistret. Transportstyrelsen har också lämnat in en framställan om författningsändringar, vilken ännu inte lett till någon förändring av regelverket.[164]

Upphävande av särreglering i annan lag eller förordning

Den nya bestämmelsen i 28 § första stycket förvaltningslagen klargör att den offentliga förvaltningen kan fatta helt automatiserade beslut utan stöd av annan särskild reglering. För flera statliga myndigheter kvarstår emellertid särreglering i myndighetsinstruktion eller annan speciallag eller förordning som har företräde framför förvaltningslagen. Det bör undvikas att sådan reglering kvarstår och tolkas som uttömmande i fråga om när en myndighet får fatta automatiserade beslut. En sådan tolkning innebär motsatsvis att myndigheten inte har rätt att fatta andra helt automatiserade beslut än de som omfattas av särregleringen. Enligt vår uppfattning synes denna potentiella inskränkning i myndigheternas möjlighet till automatiserat beslutsfattande inte ha varit lagstiftarens avsikt.

[163] 18 kap. 5 § förordning om vägtrafikregister.
[164] Se Transportstyrelsens framställan om författningsändringar i frågan om automatiserade beslut från den 8 mars 2012, dnr TSV 2012-1177.

Vi bedömer att det, i syfte att undanröja onödiga hinder i den digitala utvecklingen, finns vägande skäl för att utmönstra kvarstående särreglering om myndigheters automatiserade beslutsfattande i lag och förordning vid sidan av nya förvaltningslagen. Inte heller i förhållande till dataskyddsförordningens krav på särskilda åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen med avseende på just automatiserade beslut torde det finnas skäl för att behålla sådan särreglering. Befintlig särreglering av automatiserat beslutsfattande i lag och förordning, vid sidan av förvaltningslagen, bör därför enligt vår bedömning upphävas i enlighet med E-delegationens förslag i betänkandet *Automatiserade beslut – färre regler ger tydligare reglering*.[165]

7.10 Digitalt perspektiv vid framtagande av nya föreskrifter

Utredningens bedömning: Regeringen bör överväga att i förordningen om konsekvensutredning vid regelgivning föreskriva att en konsekvensutredning ska innehålla en bedömning av om särskilda hänsyn behöver tas när det gäller regleringens inverkan på digital tillgänglighet till förvaltningen eller dess inverkan på automatiserade förfaranden eller annan digital informationshantering i förvaltningen.

Skälen för utredningens bedömning

Kartläggningsresultatet om nya föreskrifter och en digital förvaltning

Under kartläggningen har myndighetsrepresentanter fört fram att uppdragsgivaren ibland tenderar att förbise att vid myndighetssamverkan i den digitala förvaltningen behöver frågor om reglering kring digital informationshantering i princip alltid omhändertas. Rättsliga frågor behöver ofta lösas ut för att t.ex. åstadkomma rättsligt stöd för digitalt informationsutbyte mellan myndigheter som berörs av en gemensam ärendeprocess. För att underlätta t.ex.

[165] SOU 2014:75.

ett myndighetsgemensamt utvecklingsarbete beskrivs det vara önskvärt att departementen och andra regelgivare redan från början tänker i digitala processer. Om så inte sker riskerar det att gå åt onödigt mycket tid för att i efterhand lösa rättsliga frågor om de förutsättningar för digitalt informationsutbyte som behövs för att t.ex. sköta en ny arbetsuppgift. Alternativt hindras effektiva och ändamålsenliga digitala processer eftersom processerna får brytas med manuella mellanled, med de nackdelar i form av bl.a. kostnader och ineffektiva förfaranden detta för med sig.

Flera av dem som deltagit i kartläggningsarbetet har också reagerat på att de nya författningar som tas fram sällan är anpassade till digitala processer. Det har uttryckts som att man i någon mån kan hävda att lagstiftningsprodukter, trots att utgångspunkten är teknikneutralitet, i de flesta fall fortfarande utgår ifrån analoga förfaranden i den offentliga förvaltningen i stället för digitala.

Digital tillgänglighet till den digitala förvaltningen

I det förevarande kapitel 7 har vi främst behandlat frågor som rör digitalisering inbegripet automation inom förvaltningen. Det är också det perspektivet som har lyfts från flera myndighetsrepresentanter under kartläggningen. Det finns dock anledning att här anknyta till vad som förts fram i kapitel 6.8 om de politiska målen, bl.a. att regeringens mål för digitaliseringen av den offentliga förvaltningen också är en enklare vardag för medborgare, en öppnare förvaltning som stödjer innovation och delaktighet samt högre kvalitet och effektivitet i verksamheten.[166]

I det följande kapitel 8 går vi närmare in på att privatpersoner och företag i ökad utsträckning ska ges digital tillgänglighet till förvaltningen. Utan att här föregripa de överväganden och bedömningar som där görs finns anledning att även i detta sammanhang reflektera kring vilka förfaranden som ska erbjudas vid kontakter mellan enskilda och förvaltningen. I likhet med vad myndighetsrepresentanter har framhållit under kartläggningen om vikten av att tänka på de praktiska förutsättningarna i myndigheters verksamheter när ny reglering tas fram, bl.a. att informationshanteringen inom förvaltningen förutsätts vara digital och att det behöver finnas

[166] Prop. 2017/18:1, utg. omr. 2, 6.2 Mål.

förutsättningar för automatiserade förfaranden, finns det enligt oss anledning att också på motsvarande sätt tänka på att enskilda har förväntningar på digital tillgänglighet till förvaltningen. Den kommunikationen förväntas nämligen också kunna skötas med digitala medel i första hand. Förutsättningarna för digital tillgänglighet till förvaltningen, bl.a. att det finns rättsliga förutsättningar för digital kommunikation mellan enskilda och förvaltningen, kan inte ses separat från den verksamhet som ska regleras i nya föreskrifter.

Konsekvensutredningar om inverkan på digital förvaltning

En stor del av våra analyser och överväganden rör hinder eller hämmande faktorer i befintlig lagstiftning, dvs. all den gällande rätt som ska tillämpas vid digitaliseringsåtgärder och löpande verksamhet i den digitala förvaltningen. Som framgått i utredningens kartläggning finns det en påtaglig mängd rättsfrågor att hantera. Det framstår emellertid som särskilt bekymmersamt att det inte endast är gällande rätt som riskerar att i onödan hindra eller hämma en önskad digital utveckling av den offentliga förvaltningen, utan att det dessutom kan tillkomma nya rättsliga problem när nya lagar och andra föreskrifter tas fram.

De rättsliga utmaningarna för den digitala och digitalt tillgängliga förvaltningen kan enligt vår uppfattning inte få fortsätta att öka. Det är därför angeläget att framtagandet av ny reglering föregås av analyser om reformen eller anpassningen har påverkan på digital tillgänglighet till förvaltningen eller dess inverkan på automatiserade förfaranden eller annan digital informationshantering i förvaltningen. Det är nämligen inte givet att det finns de rättsliga förutsättningar för digital informationshantering som behövs för att omsätta en reform eller regeländring i praktisk verksamhet. Det kan behövas särskilda åtgärder för att anpassa den reglering som styr informationshanteringen, även när informationshanteringen inte står i fokus för reformen eller förändringarna. Det bör, med beaktande av de politiska målen, därför analyseras om en tänkt reform eller förslag till författningsändring skulle kunna medföra än enklare och bättre service till privatpersoner eller företag om det tänkta förslaget t.ex. främjar digital kommunikation eller automatiserade förfaranden.

I vart fall bör det inte finnas oavsiktliga hinder mot en säker och effektiv digital informationshantering.

Bland annat behöver de rättsliga förutsättningarna för att behandla personuppgifter övervägas, eftersom behandling av personuppgifter är ett centralt inslag i stora delar av den informationshantering som äger rum inom förvaltningen. Om förfarandet innefattar beslutsfattande bör det också övervägas om besluten kan komma att fattas automatiserat och om regleringen ger goda förutsättningar för att omsättas i rättssäkra förfaranden i praktiken. De resonemang som förts i kapitel 7.9.1 kan i det avseendet vara en av utgångspunkterna för analysen. Även i de fall en informationshantering i nuläget främst kommer att skötas av människor som tar stöd av digitala förfaranden behöver inte sällan teknisk kompetens konsulteras för att få underlag för vad som kan vara en rimlig tid för ikraftträdande av förslaget med hänsyn till eventuellt behov av att utveckla it-stöd.

Med beaktande av det ovan beskrivna och med särskild utgångspunkt i vårt kartläggningsresultat bedömer vi sammanfattningsvis att det finns brister i den nuvarande ordningen. Det bör enligt vår bedömning finnas klarare direktiv om att det vid framtagande av nya författningar behöver analyseras vilka konsekvenser författningsförslagen medför för digital tillgänglighet till förvaltningen och för förvaltningens digitala eller automatiserade förfaranden.

Vilka konsekvensanalyser som ska göras inför en regeländring framgår i förordningen (2007:1244) om konsekvensutredning vid regelgivning. Förordningen om konsekvensutredning vid regelgivning är direkt tillämplig när förvaltningsmyndigheter under regeringen tar fram nya föreskrifter. Om en kommittés eller särskild utredares betänkande innehåller förslag till nya eller ändrade regler ska också konsekvenserna anges på ett sätt som motsvarar de krav på innehållet i konsekvensutredningar som finns i bl.a. 6 § förordningen om konsekvensutredning vid regelgivning.[167]

Ett alternativ är att uttryckligen utvidga förordningen om konsekvensutredning vid regelgivning med en bestämmelse om att konsekvensutredningar ska omfatta de analyser som vi ovan redogjort för, dvs. om ny reglering får inverkan på digital tillgänglighet till förvaltningen eller inverkan på automatiserade förfaranden eller annan digital informationshantering i förvaltningen.

[167] 15 a § kommittéförordningen (1998:1474).

Frågan är dock om det finns något annat alternativ för att vid regelgivning åstadkomma en belysning av de ovan beskrivna perspektiven om en digital förvaltning. Till exempel skulle Tillväxtverket, som har i uppdrag svara för metodutveckling, rådgivning och utbildning med anledning av förordningen om konsekvensutredning vid regelgivning,[168] kunna bistå i arbetet med att utveckla den handledning verket ger inom området eller genom utbildningar. En förordningsreglering skulle enligt vår bedömning med fördel kunna kompletteras med ytterligare handledning, utbildningar eller andra stödåtgärder från ansvarig myndighet, gärna i dialog med experter på det nu aktuella området.

Även med beaktande av att förordningen ska vara av generell karaktär anser vi emellertid att främjandet av förvaltningens digitalisering, till nytta för privatpersoner och företag, utgör ett sådant perspektiv som vid denna tidpunkt kan lyftas fram särskilt. Vi bedömer därför att regeringen bör överväga att regeringen i förordningen om konsekvensutredning vid regelgivning föreskriva att en konsekvensutredning ska innehålla en bedömning av om särskilda hänsyn behöver tas när det gäller regleringens inverkan på digital tillgänglighet till förvaltningen eller dess inverkan på automatiserade förfaranden eller annan digital informationshantering i förvaltningen. Också i Regeringskansliet bör det övervägas hur man i beredningsprocesserna kan omhänderta motsvarande behov av konsekvensanalyser.

Det finns vidare anledning att framhålla att frågor om hur informationshanteringen ska gå till och i vilken utsträckning förfaranden kan digitaliseras eller automatiseras är angelägna att tidigt ta i beaktande när nya rättsakter inom EU förhandlas fram. Även i de processerna kan det därför finnas anledning att i tid inhämta synpunkter från dem med teknisk kompetens hos de myndigheter som berörs av de förslag som förhandlas.

[168] 4 § förordning (2009:145) med instruktion för Tillväxtverket.

8 Digital kommunikation

8.1 Behovet av enkel, säker och effektiv kommunikation

Framväxten av den digitala förvaltningen har inneburit avsevärda förändringar i sätten att förmedla information till och från myndigheter. Under lång tid fanns inte andra medel för sådan kommunikation än skriftliga pappersförfaranden eller muntliga kontakter vid personliga möten eller per telefon. En omfattande utveckling av kommunikationsmedel har emellertid ägt rum från mitten av 1900-talet och framåt. Först gjorde faxen och sedan e-posten och webben sitt intåg i förvaltningen. Flertalet myndigheter erbjuder numera utöver e-post också andra former av digital kommunikation med privatpersoner och företag eller myndigheter emellan. Det rör sig bl.a. om kommunikation av meddelanden till enskilda via lösningen för säker myndighetspost betecknad Mina meddelanden och olika webbaserade digitala tjänster (hittills oftast benämnda e-tjänster). Det handlar också om andra tekniska lösningar för överföring av information från maskin till maskin via kanaler som uppfyller särskilda krav på säkerhet.

Att använda digitala tjänster för kommunikation innebär ofta fördelar i förhållande till användning av papperspost eller konventionell e-post. Digitala tjänster kan inledningsvis i flera avseenden möjliggöra nya former för service och information till enskilda. Med digitala medel kan exempelvis beslut beskrivas på andra sätt än vad som är möjligt att förmedla på ett papper eller i ett e-postmeddelande, bl.a. när det gäller att åskådliggöra beräkningar eller prognoser. Information från myndigheter kan också bättre anpassas till mottagarens individuella situation på ett annat sätt än vad som är möjligt när ett informationsinnehåll behövt fixeras i ett pappersdokument.

Under kartläggningen har vi sammantaget fått bilden av att myndigheternas utveckling av digitala tjänster, även vad avser de tjänster som redan finns i drift, ännu är i sin linda. Det står alltså klart för oss att den digitala formen för att förmedla information till privatpersoner och företag möjliggör långt mer informativa tjänster från förvaltningens sida än vad som alls varit möjligt på den tid papper varit formen för att bära den information som ska förmedlas.

Det finns uppenbara fördelar med digitala lösningar ur ett tillgänglighetsperspektiv. Digitala tjänster kan bl.a. anordnas så att enskilda med särskilda behov kan ta del av meddelanden direkt via tjänsten, i stället för att den enskilde behöver ha egen tillgång till särskilda tekniska hjälpmedel för att kunna tillgodogöra sig information som förmedlats på ett papper. Som exempel kan nämnas att digitala tjänster direkt kan förses med talsyntes eller skärmläsare som läser upp en text.

Jämfört med traditionell e-post har digitala tjänster också den fördelen att kommunikationen via sådana tjänster anordnas i förhållande till myndigheten som sådan, inte till enskilda tjänstemän som kan vara fallet när e-post används. Det finns, vilket också har uppmärksammats under kartläggningen, risker med att enskilda tar direkt kontakt med tjänstemän via e-post. Det gäller bl.a. försök att påverka utgången i förvaltningsärenden eller risk för hot mot tjänstemannen i fråga. Genom att anordna kommunikationskanalerna direkt till myndigheten via digitala tjänster finns det förutsättningar att minska denna typ av risker. Funktionsbrevlådor i stället för direkta e-postadresser till enskilda tjänstemän har också anordnats hos flera myndigheter i anledning av bl.a. dessa risker.

Till skillnad från när vanlig e-post används finns även möjlighet att inom ramen för digitala tjänster ordna förfaranden som säkerställer en god offentlighetsstruktur i fråga om bl.a. rutiner för rensning, arkivering, gallring och bevarande. Med effektiva medel kan myndigheten därigenom säkerställa att den följer regler som gagnar en öppen förvaltning. Omvänt leder användandet av konventionell e-post vid kommunikation med förvaltningen till hög arbetsbelastning hos myndigheterna. Personal vid myndigheterna behöver nämligen i hög grad manuellt hantera e-postmeddelandena enligt bestämmelserna om bl.a. handlingsoffentlighet och arkivering. Myndigheters möjligheter att använda spamspärrar och spamfilter i e-postlösningar kan också diskuteras ur ett rättsligt perspektiv, med beaktande av

den praktiska konsekvensen att stora mängder förmodad skräppost också behöver hanteras. När digitala tjänster i stället används vid kommunikation med förvaltningen uppnås fördelar även i nu nämnda hänseenden.

Det bör här också framhållas att digitala tjänster kan anordnas på ett sätt som möter bl.a. dataskyddsregleringens krav på säkerhet för behandling av känsliga personuppgifter, samtidigt som konventionell e-post inte har ansetts uppfylla sådana krav.[1] Här bör också framhållas den nytta som skapas både för enskilda och för förvaltningen genom att uppgifter som kommer in till myndigheten via digitala tjänster vanligen har ett mer strukturerat format som bl.a. underlättar fortsatta automatiserade förfaranden (se kapitel 7).

8.2 Enskildas självbestämmande och förvaltningens uppdrag

Under utredningens kartläggningsarbete har vi i flera sammanhang uppmärksammats på frågor som hör samman med det engelska begreppet ”My Data”. Begreppet relaterar till en strävan mot att förändra synsättet på förfogande över företrädesvis personuppgifter. Informationshantering och -flöden bör enligt denna strävan i lägre utsträckning styras av myndigheter och andra organisationer. Informationen bör i stället i högre utsträckning förfogas av den enskilda person som informationen rör. Med förfogande avses både tillgång till informationen och kontroll över informationen. Finland är ett av de länder som, genom regeringsprogram,[2] har antagit principer om att i förhållande till digitaliseringen av offentliga tjänster stärka medborgarnas rätt att övervaka och besluta om användningen av information som gäller dem själva.

Under kartläggningsarbetet har det förekommit att liknande koncept som ovan beskrivits har benämnts som en form av ”ägarskap” av information. Begreppet ”ägarskap” av information är juridiskt sett problematiskt, eftersom olika former av reglering ur olika perspektiv

[1] Se bl.a. information på Datainspektionens webbplats, www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/sakerhet-enligt-personuppgiftslagen/sakerhet-for-personuppgifter-i-e-post/

[2] Se http://vm.fi/sv/offentliga-tjanster-digitaliseras och http://vnk.fi/documents/10616/1930541/Bilaga+5+Digitalisering+f%C3%B6rs%C3%B6ksverksamhet+och+avveckling+av+normer.pdf/b97419d2-ad95-40df-b63a-99984ad1b868

definierar ansvar för information.[3] Vi väljer därför att inte använda termen ägarskap i detta sammanhang.

Frågor om den enskildes rätt att själv förfoga över information som rör den egna personen bör också sättas i samband med vilken medverkan från enskilda som exempelvis ska krävas när individer och företag ställs inför en livshändelse i privatlivet respektive verksamheten[4] som kräver en mängd kontakter med det offentliga. I nuläget måste den enskilde eller en person som företräder företaget eller organisationen ofta vara sin egen projektledare i en sådan situation. Utan myndighetsövergripande guidning behöver den enskilde eller företrädaren själv skapa sig en uppfattning om hur han eller hon ska gå till väga, vilka aktörer som behöver kontaktas, vilken information som måste skickas in till en eller flera myndigheter och i vilken form. Många gånger behöver samma uppgift lämnas in till flera olika aktörer, samtidigt som det saknas en övergripande bild över ärendegången.

I linje med vad som anförts ovan kan det finnas skäl för att informationshanteringen bör utgå från organisatoriska lösningar och förbättrade rättsliga förutsättningar för informationsutbyten mellan myndigheter, snarare än utökad arbetsinsats från den enskilde. I kapitel 7 har vi också pekat på den framtida utveckling vi ser mot att förvaltningens automationsåtgärder kommer att medföra att uppgifter i högre grad hämtas från databaser inom förvaltningen, dvs. digitala källor, och i lägre grad inhämtas direkt från den enskilde genom att denne på fri hand lämnar uppgifter själv i t.ex. ansökningsformulär när ärenden inleds.[5] Trots detta kommer det förstås

[3] Rättsregler som avser myndigheters ansvar för information finns i olika typer av författningar. Vissa typer av reglering som avser ansvar för information utgår från att skydda eller tillvarata särskilda intressen, såsom informationssäkerhet (se t.ex. förslag till 2 kap. 2 § ny säkerhetsskyddslag i *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag*, prop. 2017/18:89, 19 § förordningen [2015:1052] om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet [MSBFS 2016:1]), integritetsskydd (se t.ex. dataskyddsförordningen), god offentlighetsstruktur (se t.ex. 4 kap. offentlighets- och sekretesslagen [2009:400]) eller arkiv (se t.ex. arkivlagen [1990:782]).

[4] Med livshändelse menas enligt eSamverkansprogrammet (eSam) när en privatperson eller företagare ställs inför en händelse som påverkar och förändrar hans eller hennes livssituation och som kräver en mängd kontakter med det offentliga, se http://esamverka.se/vart-arbete/livshandelsedriven-utveckling.html

[5] Jfr vad som beskrivits i kapitel 6.6 om ”The Once-Only Principle” (TOOP) i EU:s handlingsplan för e-förvaltning. Principen innebär att offentliga förvaltningar bör säkerställa att medborgare och företag endast behöver lämna samma uppgifter en gång på ett ställe i den digitala förvaltningen.

ändå att kvarstå ett behov av kommunikation mellan enskilda och förvaltningen.

8.3 Behövs ny eller anpassad reglering om digital kommunikation med enskilda?

8.3.1 Våra inledande överväganden

Utredningens bedömning: Lagstiftningen bör anpassas för att ge rättslig styrning och stöd med regler om digital kommunikation vid kontakter mellan enskilda och förvaltningen. En sådan reglering skapar bättre förutsättningar för en sammanhållen och tillgänglig digital förvaltning.

Skälen för utredningens bedömning

Kartläggningsresultatet

I våra kommittédirektiv anges att utredningen särskilt ska analysera och föreslå vilket författningsstöd som krävs för att tillvarata den fulla potentialen i regeringens satsning Digitalt först, för att därigenom möjliggöra en övergång från traditionella ärendeflöden till digitala interaktioner.

Inom ramen för vår kartläggning har relativt få aktörer specifikt lyft frågor som rör reglering avseende formen för hur förvaltningen ska vara tillgänglig för kontakter från enskilda. Möjligen följer det sagda av att vi under kartläggningen främst har träffat myndigheter och inte enskilda. Flera myndighetsrepresentanter har i stället närmat sig frågan från motsatt håll genom att undra vilka krav förvaltningen kan ställa på enskilda att använda de kanaler som tas fram för digital kommunikation. Frågorna hör givetvis samman med varandra i den bemärkelsen att digitala tjänster som utvecklas inom förvaltningen också behöver användas av enskilda för att de ska vara till någon nytta. Att den digitala kommunikationen mellan förvaltningen och enskilda även i praktiken behöver fungera i båda riktningarna är också något som vi har uppmärksammats särskilt på, inte minst i samband med den hearing som utredningen anordnat.

Flera av de representanter vi mött under kartläggningen har emellertid på ett övergripande plan framfört att det behövs mer styrning genom rättsregler för att nå de politiska målen med en digital förvaltning. Några har framfört att det digitaliseringsarbete som bedrivs i dag många gånger bygger på att det finns eldsjälar som driver arbetet framåt, men att det ibland inte räcker med myndigheters eller enskilda medarbetares goda vilja för att nå de politiska målen utan att det krävs styrning och stöd genom rättsregler. Det har även framförts som önskvärt att förvaltningslagen skulle fokusera på en digital förvaltning. Med ett tydligare rättsligt stöd beskrivs det vara lättare för myndigheterna att ta ytterligare steg framåt vad gäller den digitala servicen.

Gällande och föreslagen reglering

Tidigare rättsutveckling avseende frågor som rör formen för förvaltningens kontakter med enskilda kan i viss mån sägas ha följt den teknik- och samhällsutveckling som ägt rum. Exempelvis infördes det i förvaltningslagen år 2003 en uttrycklig skyldighet för myndigheterna att se till att medborgarna kan kommunicera med dem med hjälp av telefax och elektronisk post.[6] I de motiv som angavs som skäl för att införa bestämmelsen anfördes bl.a. att e-post var ett effektivt och användarvänligt kommunikationsmedel och att det fanns ett påtagligt behov hos enskilda människor att kunna använda detta moderna sätt att kommunicera i sina kontakter med myndigheterna. Vidare anförde regeringen följande.

> Det är enligt regeringens mening ett grundläggande villkor att förvaltningen anpassar sig till de förändringar som sker i samhället. Myndigheterna skall uppfylla högt ställda krav på tillgänglighet och tillmötesgående. Informationstekniken är ett centralt redskap när det gäller att utveckla servicen i förvaltningen. Mot den nu angivna bakgrunden framstår det som angeläget att det införs en otvetydig skyldighet för myndigheterna att erbjuda medborgarna möjlighet att komma i kontakt med dem med hjälp av moderna kommunikationsmedel. Detta bör ske genom ett uttryckligt åliggande för förvaltningsmyndigheterna och domstolarna att vara tillgängliga per fax och, framför allt, e-post. Detta krav måste i princip anses gälla som god förvaltningspraxis redan i dag. Utgångspunkten är alltså att det alltid skall vara möjligt för en enskild

[6] 5 § andra stycket förvaltningslagen (1986:223).

att kontakta en myndighet med hjälp av e-post i stället för att t.ex. använda telefon eller brev.[7]

Genom den nya förvaltningslag som träder i kraft den 1 juli 2018 ändras den aktuella bestämmelsens lydelse så att den i stället anger att en myndighet ska vara tillgänglig för kontakter med enskilda och informera allmänheten om hur och när sådana kan tas. Ändringen motiverades av att regleringen i högre grad nu borde anpassas så att den är neutral i förhållande till den omfattande och kontinuerligt ökande digitala förvaltningen och att den även i övrigt borde göras mer ändamålsenlig. För att förvaltningen inte ska låsa sig vid de varianter som nu förekommer, utan vara öppen för nya lösningar när det gäller digitala kommunikationsformer, formulerades kravet mera allmänt.[8] Regleringen knyter alltså inte till sin lydelse an till den pågående utvecklingen där förvaltningen i ökad grad erbjuder, och enligt de politiska målen förväntas erbjuda, digitala tjänster för kommunikation med privatpersoner och företag.

Förvaltningslagen innehåller även en bestämmelse om kommunikation med den som är part i ett ärende innan en myndighet fattar beslut. Bestämmelsen innebär att det är myndigheten som avgör hur sådan underrättelse ska ske. Det följer dock av myndigheternas serviceskyldighet att valet av underrättelseform måste göras med beaktande av tillgänglighetsaspekter, exempelvis i kontakter med barn eller unga, eller om någon enskild till följd av en funktionsnedsättning har svårigheter att tillgodogöra sig muntlig eller skriftlig information.[9] En liknande bestämmelse i förvaltningslagen anger skyldighet att underrätta den som är part om innehållet i beslut och om överklagandemöjligheter.[10]

Förvaltningslagen anger därmed inte några handlingsdirektiv avseende formen för förvaltningens kommunikation med privatpersoner och företag. Den enskilda myndigheten har i stället själv att ta ställning till dels frågan om digitala tjänster alls ska erbjudas, dels hur dessa digitala tjänster i sådant fall ska utformas (med beaktande av annan reglering, se bl.a. översikten i kapitel 4) och användas.[11]

[7] *Några förvaltningsrättsliga frågor*, prop. 2002/03:62, s. 10 f.
[8] 7 § första stycket förvaltningslagen (2017:900) och *En modern och rättssäker förvaltning – ny förvaltningslag*, prop. 2016/17:180, s. 68 f.
[9] 25 § andra stycket förvaltningslagen och a. prop. s. 169 f.
[10] 33 § förvaltningslagen.
[11] Jfr t.ex. med kraven i 15 a § i den norska loven om behandlingsmåten i forvaltningssektor LOV-1967-02-10 (forvaltningsloven) och föreskriften om elektronisk kommunikation med och i förvaltningen FOR-2004-06-25-988 (e-förvaltningsföreskriften).

Utredningen om effektiv styrning av nationella digitala tjänster har å sin sida föreslagit att det ska införas en ny bestämmelse om att statliga myndigheter ska erbjuda elektronisk kommunikation i kontakten med enskilda. Den bestämmelse som föreslås avser inte myndigheters användning av digital post utan annan elektronisk kommunikation där privatpersoner och företag lämnar uppgifter till myndigheten i ett elektroniskt formulär eller får information presenterad för sig. Vidare beskrivs att för denna kommunikation behövs en identitets- och behörighetskontroll, dvs. inloggning.[12]

Den nämnda utredningen har också föreslagit att det ska införas en ny rätt för enskilda och företag att få myndighetspost elektroniskt och att alla statliga myndigheter ska skicka myndighetspost elektroniskt om inte regeringen beslutar annat.[13]

Några utgångspunkter

Finns det då mot den beskrivna bakgrunden behov av att införa reglering som ställer uttalade krav på att privatpersoner och företag enkelt ska kunna komma i digital kontakt med det offentliga Sverige? Eller kommer kommunikationsvägarna ändå att bli digitala med tiden, utan att några rättsregler alls behöver ange detta? Frågeställningen bör enligt oss belysas från huvudsakligen två perspektiv.

För det första bör det i linje med vad som anförts ovan övervägas om det behövs ytterligare handlingsdirektiv genom reglering för att det ska vara möjligt att nå de politiska målen om att det ska vara enkelt för privatpersoner och företag att kontakta förvaltningen digitalt. I denna del instämmer vi i de slutsatser som Utredningen om effektiv styrning av nationella digitala tjänster har dragit om att de befintliga politiska målen snarare utgör mål för regeringens arbete och politiken som helhet, än sådana mål som pekar ut vad myndigheterna ska göra eller förväntas uppnå.[14]

För det andra ger kartläggningen stöd för att våra överväganden om behov av regeländringar behöver göras med beaktande av att det

[12] Utredningen om effektiv styrning av nationella digitala tjänsters delbetänkande *digitalforvaltning.nu* (SOU 2017:23), s. 117 f. och förslag till 6 § första stycket förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte.
[13] A.a. s. 192 f. och samma utrednings slutbetänkande *reboot – omstart för den digitala förvaltningen* (SOU 2017:114) med förslag till lag om infrastruktur för digital post.
[14] SOU 2017:114 s. 101 f.

råder en rättslig osäkerhet i vissa särskilda frågor som rör förvaltningens kommunikation med enskilda. Den osäkerheten förstärks när tillämpliga rättsregler inte ger uttryck för ett rättsligt stöd för de kommunikationsformer som myndigheterna faktiskt tillhandahåller eller överväger att införa. Nuvarande reglering ger inte heller enskilda en rättvisande bild av hur förvaltningen faktiskt sköts och i allt högre utsträckning kommer att skötas.

Det finns ytterligare aspekter på frågan om det behövs rättsregler som anger att privatpersoner och företag enkelt ska kunna komma i digital kontakt med förvaltningen. En sådan aspekt, som utgör ett tredje skäl att överväga rättsregler, är vilken tidsram som bör accepteras för att förvaltningens digitalisering ska pågå parallellt med en traditionell pappershantering. Så länge papper behöver hanteras parallellt med att nya digitala tjänster tas fram kommer förvaltningen att behöva hantera ärendeprocesser på dubbla sätt.

Vi går här inte närmare in på beräkningar av vilka kostnader detta för med sig, utan stannar vid att konstatera att detta uppenbart kommer att vara fortsatt kostsamt vad avser såväl tid som ekonomiska resurser som behöver avsättas för post- och pappershantering, parallellt med utvecklingen och förvaltningen av de digitala tjänsterna.

Det förhållandet att samma ärendeprocesser nu under en övergångsperiod innefattar både digital hantering och pappershantering gör det också svårare att få överblick över och insyn i den samlade ärendehanteringen. Det finns med andra ord inte bara ett kostnads- eller effektivitetsperspektiv på frågan om förvaltningens upprätthållande av två sätt att förfara med samma ärendeprocesser. Det finns också ett insyns- och rättssäkerhetsperspektiv som enligt oss förtjänar att framhållas.

Enligt vår bedömning bör reglering mot den beskrivna bakgrunden särskilt övervägas i syfte att hålla tidsperioden för parallella sätt att hantera information så kort som möjlig, samtidigt som rättssäkra förfaranden garanteras.

Teknikneutral reglering

Vi ser positivt på att regleringen i den nya förvaltningslagen innehåller ett allmänt formulerat krav på att myndigheterna ska vara tillgängliga för kontakter med enskilda, utan att ange några detaljerade

krav på att myndigheterna måste skapa vissa utpekade tekniska förutsättningar som knyter an till sådana kommunikationsformer som är kända i dag.[15] Under kartläggningen har vi också fått en god bild över alla de former för digital tillgänglighet som nu och i närtid finns och planeras hos myndigheterna. Det rör sig om en varierad palett av digital kommunikation. Kommunikationskanalerna kan avse avancerade tekniska lösningar med maskin-till-maskin-inläsning av information genom öppna applikationer, eller digitala tjänster hos myndigheter med Mina sidor, kommunikation till enskilda via Mina meddelanden eller andra kanaler för digitala kontakter. Ibland kan de också kompletteras av nya sätt att ge service t.ex. via telefonsamtal eller andra former för röststyrning i stället för att förutsätta det skrivna ordet. Med beaktande av detta och att den tekniska utvecklingen kan förutspås gå fort framåt även framöver vad gäller formerna för digital kommunikation bör en reglering om förvaltningens tillgänglighet enligt vår bedömning förhålla sig neutral i förhållande till vilken teknik som används i nutid.

Det har också visat sig finnas nackdelar med att reglera att myndigheter ska vara skyldiga att tillhandahålla kommunikationskanaler via en särskilt utpekad teknik. Här bör särskilt hänvisas till vad som i kapitel 8.1 beskrivs vara problem med att kräva att myndigheter ska ta emot traditionell e-post. Enligt vår bedömning är det därför också positivt att det inte längre anges i den nya förvaltningslagen att myndigheter behöver vara tillgängliga via t.ex. fax eller e-post utan kan välja att helt avstå från att tillhandahålla sådana former för kommunikation.

Att en reglering bör förhålla sig teknikneutral och inte peka ut detaljer i frågan om vilka kommunikationskanaler som myndigheter ska vara skyldiga att tillhandahålla innebär emellertid inte att det bör råda en fullständig avsaknad av regler om hur enskilda kan förvänta sig nå den allt mer digitala (och också automatiserade, se kapitel 7) förvaltningen, eller hur förvaltningen bör kommunicera med enskilda.

Frågan om förvaltningens digitala tillgänglighet för enskilda och hur kommunikationen mellan förvaltningen och enskilda förväntas fungera är av central betydelse för många privatpersoner och företag och ytterst en fråga om hur rättssäkra förfaranden kan garanteras. För oss framstår det också som naturligt att inför våra bedömningar och

[15] Se kapitel 6.2 och prop. 2016/17:180 s. 68.

förslag ta en utgångspunkt i hur den allmänna förvaltningsrätten under lång tid har utvecklats. I såväl den hittills gällande som i 1971 års förvaltningslag har explicita författningskrav ställts på förvaltningen i fråga om tillgänglighet vid kommunikation i samband med ärendehandläggning och sammanhängande beslutsfattande och service.

Våra överväganden om behov av att anpassa lagstiftningen

Mot den beskrivna bakgrunden framstår det som en rimlig utgångspunkt att formerna för hur enskilda med fog kan förvänta sig att få kontakt med förvaltningen bör framgå i generell reglering som dels styr mot de politiska målen om en digital förvaltning, dels träffar den offentliga förvaltningen som helhet (dvs. förutom förvaltningsmyndigheter och domstolar även kommuner och landsting). Med detta i beaktande skulle den förordningsreglering som Utredningen om effektiv styrning av nationella digitala tjänster har föreslagit om skyldighet för statliga myndigheter att erbjuda elektronisk kommunikation i kontakten med enskilda[16] inte vara tillräcklig, eftersom den inte når hela förvaltningen på det sätt som enskilda enligt vår bedömning har anledning att förvänta sig. För den enskilde är det nämligen sällan av någon större betydelse om denne i samband med olika händelser i livet som kräver myndighetskontakt ska vända sig till en statlig eller kommunal myndighet, t.ex. när någon anländer som ny i Sverige eller vill starta ett företag.

Enligt vår bedömning är det inte heller tillräckligt att styra enskilda utvecklingsarbeten som rör enstaka digitala tjänster i förvaltningen genom uppdrag i regleringsbrev eller andra regeringsuppdrag. En sådan styrning avser normalt kortare perioder under utvecklingsfasen av nya tjänster och inte den digitala förvaltning som faktiskt byggs upp och därefter under längre tid ska vara i drift i förhållande till enskilda. Det blir inte heller transparent eller förutsebart för privatpersoner och företag på vilket sätt de kan förvänta sig att kommunikationen med förvaltningen kan, bör eller ska gå till. Behovet av reglering, och inte enbart styrning genom regeringsuppdrag, stärks också av den ovan nämnda utgångspunkten att reglering

[16] Förslag till 6 § första stycket förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte i SOU 2017:23 s. 117 f.

om en digitalt tillgänglig förvaltning bör omfatta förvaltningen som helhet, dvs. inte enbart statliga myndigheter.

Det skulle kunna invändas att en rättslig reglering med t.ex. huvudregler om digital kommunikation vid kontakter mellan förvaltningen och enskilda inte borde införas förrän teknisk infrastruktur för att stödja sådan kommunikation finns på plats. Det skulle också kunna hävdas att det, innan en sådan reglering övervägs, inte bör finnas några som helst övriga rättsliga hinder mot digital kommunikation mellan enskilda och förvaltningen t.ex. avseende regler i registerförfattningar om elektroniskt utlämnande av uppgifter. Mot detta kan enligt vår bedömning framhållas att generella krav behöver ställas just för att skapa incitament att åstadkomma dessa ytterligare förutsättningar. Faktorer som tekniska möjligheter och rättsliga förutsättningar i övrigt blir emellertid fortsatt nödvändiga att förhålla sig till.

Vi bedömer sammanfattningsvis att tiden är mogen för generella men övergripande och teknikneutrala regler om digital kommunikation vid kontakter mellan förvaltningen och enskilda. Genom en sådan reglering skapas bättre förutsättningar för en sammanhållen digital förvaltning som finns tillgänglig för privatpersoner och företag utifrån deras behov. Denna typ av reglering skapar också goda grundläggande rättsliga förutsättningar för att åstadkomma infrastrukturlösningar med t.ex. en gemensam plattform för olika myndigheters digitala tjänster. Det ska vara enkelt för den enskilde att komma i kontakt med den digitala förvaltningen, oavsett om det är en eller flera statliga eller kommunala myndigheter som ska hantera den enskildes ärende eller ärenden.[17]

8.3.2 Enskildas användande av digitala tjänster

Utredningens bedömning: Det bör inte nu införas en förvaltningsgemensam reglering som ålägger privatpersoner och företag en generell skyldighet att använda de digitala tjänster som förvaltningen tillhandahåller.

[17] Jfr vad som framgått i kapitel 6.6 om att offentliga förvaltningar bör leverera sina tjänster digitalt som förstahandsalternativ och att offentliga tjänster bör tillhandahållas via en enda kontaktpunkt (eller one-stop-shop) och via olika kanaler enligt den EU-gemensamma handlingsplanen för e-förvaltning.

Skälen för utredningens bedömning

Allas tillgänglighet till en digital förvaltning

Det pågår flera arbeten som ytterst syftar till att öka den digitala tillgängligheten till offentlig sektor för alla människor. Här kan inte en heltäckande bild av allt det aktuella arbetet ges, men några inledande och övergripande reflektioner bör göras om hur digitaliseringen förhåller sig till tillgänglighetsaspekter.

Vår utgångspunkt är att digitala kontaktvägar mellan förvaltningen och enskilda innebär förbättrade möjligheter för privatpersoner och företag att på sina villkor få tillgång till förvaltningens tjänster. Myndigheter som erbjuder digitala tjänster för att t.ex. inleda ärenden finns tillgängliga den tid på dygnet som den enskilde önskar. Digitala förfaranden ger också överlag förbättrade möjligheter för enskilda att snabbt och enkelt få tillgång till information och beslut från förvaltningens sida. För den breda allmänheten medför därmed digitaliseringen en bättre tillgänglighet till förvaltningen.

Det räcker dock inte att digitaliseringen generellt sett ger allmänheten en bättre tillgänglighet till förvaltningen. Frågan om förvaltningens tillgänglighet behöver belysas i förhållande till alla enskilda. I regeringens digitaliseringsstrategi anges bl.a. att digital kompetens innebär att alla ska vara förtrogna med digitala verktyg och tjänster samt ha förmåga att följa med och delta i den digitala utvecklingen utifrån sina förutsättningar. Alla människor, kvinnor och män, flickor och pojkar, oavsett social bakgrund, funktionsförmåga och ålder, ska också erbjudas förutsättningar att ta del av digital information och tjänster från det offentliga och delta på ett likvärdigt sätt i samhället. Genom digital trygghet ska människor, företag och organisationer känna tillit till användningen av digitala tjänster och att de är enkla att använda.[18]

[18] *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi*, Näringsdepartementet, dnr N2017/03643/D.

De som använder internet i dag är inte bara de som tidigt tog sig an tekniken, de är många fler än så. Det ställer krav på att bl.a. tillgänglighetsanpassa webbsidor och mobila applikationer så att dessa fungerar även för personer med funktionsnedsättning.[19] Digitala lösningar kan också utvecklas i syfte att öka tillgängligheten. Digitaliseringen kan alltså ge specifika lösningar som avhjälper någon typ av begränsning i den befintliga tillgängligheten. Bland annat kan digitala tjänster anordnas så att enskilda med särskilda behov kan ta del av meddelanden direkt via tjänsten, i stället för att den enskilde behöver ha egen tillgång till särskilda tekniska hjälpmedel för att kunna tillgodogöra sig information som har förmedlats på ett papper.

Frågor om digital tillgänglighet behöver också belysas i förhållande till dem som inte kan eller vill använda digital teknik. Även om den ”digitala klyftan” mellan dem som använder respektive inte använder digital teknik stadigt krymper i Sverige finns det fortfarande omkring en halv miljon svenskar som inte använder internet över huvud taget. I absoluta tal är det 500 000 svenskar som inte är uppkopplade, varav nära 430 000 är äldre än 66 år.[20] Att befolkningen kommer att innefatta bl.a. äldre personer med nedsatta kognitiva förmågor är inte heller en faktor som kommer att försvinna med tiden. Också ekonomiska faktorer, som förmåga till inköp av nödvändig utrustning, behöver beaktas i detta sammanhang.

Även med beaktande av att antalet personer som inte använder internet minskar i Sverige behöver det sammanfattningsvis hållas i åtanke att det, i vart fall under den tid vi nu kan överskåda, kommer att finnas personer som inte kan eller vill använda digital teknik vid kontakter med myndigheter. Samtidigt ska de fördelar som digitalisering av förvaltningen medför tas till vara så att såväl den breda allmänheten som enskilda med särskilda behov kan få ökad tillgång till förvaltningens tjänster liksom enklare och snabbare service.

[19] Se bl.a. artikel 9 i FN-konventionen om rättigheter för personer med funktionsnedsättning (SÖ 2008:26), 1 kap. 2 § regeringsformen, 1 § första stycket förordningen (2001:526) om de statliga myndigheternas ansvar för genomförande av funktionshinderspolitiken, diskrimineringslagen (2008:567), 4 kap. 23 § kommunallagen (2017:725), 9 kap. 2 § lagen (2016:1145) om offentlig upphandling och 9 kap. 2 § lagen (2016:1146) om upphandling inom försörjningssektorerna. Se vidare *Genomförande av webbtillgänglighetsdirektivet*, Ds 2017:60.
[20] Se *Svenskarna och internet 2017 – En årlig studie av svenska folkets internetvanor*, Internetstiftelsen i Sverige, på www.soi2017.se/vuxnas-digitala-kompetens/delaktighet-i-informationssamhallet/

Likabehandlingsprincipen

Av 1 kap. 9 § regeringsformen följer att domstolar, förvaltningsmyndigheter och andra som fullgör offentliga förvaltningsuppgifter i sin verksamhet ska beakta allas likhet inför lagen samt iaktta saklighet och opartiskhet. Kravet på allas likhet inför lagen innebär ett skydd mot godtycke och diskriminering. Genom stadgandet markeras att Sverige är en rättsstat, och bl.a. Riksdagens ombudsmän (JO) hänför sig ibland till grundlagsbestämmelsen i sina uttalanden.

Frågan om bestämmelsens betydelse i samband med förvaltningens digitalisering har tagits upp i JO:s beslut rörande Migrationsverkets handläggningstider i ärenden om uppehållstillstånd.[21] Inom flera av de ärendeslag som granskades fanns det en avsevärd skillnad i handläggningstid mellan webbansökningar och ansökningar på papper. Migrationsverket hade uppgett att man för att förmå människor att göra sina ansökningar via webben hade valt att prioritera handläggningen av elektroniska ansökningar före pappersansökningar bland ansökningar som i övrigt var likvärdiga. Förfarandet bedömdes av JO vara oförenligt med likhets- och objektivitetsprinciperna i regeringsformen, och Migrationsverket kritiserades för detta.

Några utgångspunkter

I våra kommittédirektiv anges att det, för att målsättningen om Digitalt först ska kunna uppnås, krävs bl.a. att den offentliga förvaltningen har rättsliga förutsättningar att styra relevanta ärendeflöden och interaktioner med individer och företag till digitala lösningar. Vidare är det tydligt för oss att en parallell pappershantering förr eller senare behöver utmönstras. Så länge papper behöver hanteras parallellt med att nya digitala tjänster tas fram kommer förvaltningen nämligen att behöva hantera ärendeprocesser på dubbla sätt. Att hantera en och samma ärendeprocess både digitalt och på papper medför som redan konstaterats kostnader för dubbla förfaranden. Att information lagras och hanteras på två olika sätt inom ramen för samma ärendeprocess försvårar också möjligheten att enkelt kunna få insyn i och överblick över den verksamhet som bedrivs. Det är med andra ord önskvärt att så snart det är möjligt

[21] JO:s beslut 2015/2016:JO1, s. 326 f. (Dnr 5497-2013).

avsluta en parallell pappershantering när t.ex. en viss ärendeprocess har digitaliserats.

Frågan är hur rättsliga förutsättningar kan åstadkommas för att inom rimlig tid avsluta parallella pappersförfaranden i en digital förvaltning. Redovisningen av gällande och föreslagen rätt i kapitel 8.3.1 visar att reglering som ställer krav på formen för kommunikation mellan enskilda och förvaltningen har funnits respektive föreslås, men enbart när det gäller krav riktade mot förvaltningen. Det finns med andra ord inte några generella regler som ålägger enskilda skyldigheter att å sin sida använda digital form när de kommunicerar med det offentliga. Vi inleder därför med att överväga om det vore möjligt och i sådant fall lämpligt att införa en sådan skyldighet, vilket skulle medföra att förvaltningen helt kunde styra sina ärendeflöden till digitala lösningar.

Gällande rätt i förvaltningslagen

Bestämmelsen om tillgänglighet i 7 § förvaltningslagen[22] anger ett allmänt krav på att en myndighet ska vara tillgänglig för kontakter med enskilda och att myndigheten ska informera allmänheten om hur och när sådana kontakter kan tas. Det innebär att myndigheterna ska vara tillgängliga för allmänheten i så stor utsträckning som möjligt. Av det allmänna kravet på myndigheters serviceskyldighet i 6 § framgår att en myndighet ska se till att kontakterna med enskilda blir smidiga och enkla, att myndigheten ska lämna den enskilde sådan hjälp att han eller hon kan ta tillvara sina intressen och att hjälpen ska ges i den utsträckning som är lämplig med hänsyn till frågans art, den enskildes behov av hjälp och myndighetens verksamhet. Rätten att få hjälp är inte begränsad till viss form. Förvaltningslagen och dess förarbeten[23] anger dock inte några närmare beskrivningar av var gränserna går för om eller när en myndighet kan välja att enbart tillhandahålla t.ex. digitala formulär för vissa typer av ansökningar.

[22] Här och i det följande avses förvaltningslagen (2017:900) med ikraftträdande den 1 juli 2018, om det inte särskilt anges att annan lydelse avses.
[23] Prop. 2016/17:180.

Våra överväganden om enskildas användande av digitala tjänster

Förutom det JO-beslut som refererats ovan saknas det, såvitt vi har kunnat se, närmare vägledning om hur just grundlagens krav på likhet och objektivitet ska förstås när det gäller digitalisering av kanaler för kommunikation från enskilda till förvaltningen.[24] Det saknas med andra ord en rättslig belysning av vilka förutsättningar myndigheter har att, i samtliga eller i vissa fall, enbart tillhandahålla digitala kommunikationskanaler, dvs. inte längre erbjuda exempelvis pappersblanketter för ansökningar eller till och med kräva att ansökningar ges in enbart via en viss digital tjänst för att ärendet ska behandlas av myndigheten.

Myndigheter inom förvaltningen hanterar en stor bredd av förvaltningsärenden som rör helt olika sakfrågor och innebär kontakter med en varierad krets av parter och andra berörda. Det finns därför anledning att i flera avseenden nyansera frågeställningen om myndigheter kan välja att endast erbjuda digitala kanaler för kommunikation, eller till och med kräva att ansökningar ges in via t.ex. en viss digital tjänst. Vid överväganden av vilka kommunikationskanaler som myndigheterna ska erbjuda för enskilda som t.ex. vill inleda ärenden bör det enligt oss läggas stor vikt vid frågan om ärendets typ och vilken krets av parter och andra berörda som förutses kommunicera med myndigheten i den specifika ärendetypen. Vilka enskilda som berörs, på vilket sätt de berörs, och vad de själva önskar är omständigheter som bör vara en naturlig utgångspunkt vid bedömningar om på vilket sätt digitala tjänster kan anordnas samtidigt som rättssäkra förfaranden kan garanteras.

Vi bedömer att det för närvarande inte finns förutsättningar för att föreslå en förvaltningsgemensam reglering som ålägger privatpersoner och företag en generell skyldighet att använda de digitala tjänster som förvaltningen tillhandahåller. Bland annat genomförandet av regeringens bredbandsstrategi[25] bör här nämnas som en nödvändig förutsättning på infrastrukturnivå för att kunna övergå till helt digitala förfaranden. Här kan också nämnas det arbete av infrastrukturkaraktär som bedrivs med avseende på tjänster, som

[24] Det finns emellertid ett antal avgöranden och beslut som rör frågor om bl.a. vad som i digitala miljöer ansetts utgöra beslut i förvaltningsrättslig mening. Se t.ex. RÅ 2004 ref. 8 (Olivoljemålet) och JO:s beslut av den 26 oktober 2017, dnr 7314-2016.
[25] Se regeringens bredbandsstrategi på www.regeringen.se/4b00e7/contentassets/a1a50c6a306544e28ebaf4f4aa29a74e/sverige-helt-uppkopplat-2025-slutlig.pdf

t.ex. arbetet med att åstadkomma förutsättningar för säker e-legitimering av fysiska personer. Sett till helheten av förvaltningens verksamhet kommer det också att finnas ärendetyper där parterna, åtminstone inte för närvarande, kan eller vill använda digital teknik.

Mot bakgrund av vår ovan beskrivna utgångspunkt att det inte är lämpligt att myndigheter nu och under lång tid hanterar ärendeprocesser på parallella sätt uppstår emellertid frågan hur förvaltningen i avsaknad av en generell skyldighet för enskilda att inleda ärenden digitalt ska kunna åstadkomma en digital ärendehantering. Trots att vi inte lämnar förslag till förvaltningsgemensam reglering med åläggande för privatpersoner och företag att använda förvaltningens digitala tjänster ser vi anledning att uppehålla oss särskilt vid frågan om hur en ökad grad av digital ärendehantering vid myndigheterna ändå skulle kunna åstadkommas.

Även med beaktande av grundlagsregleringen och det ovan nämnda uttalandet från JO är det enligt vår bedömning inte alls uteslutet att vissa myndigheter i princip enbart erbjuder digitala tjänster för t.ex. vissa typer av ansökningar eller viss kommunikation. Det förekommer också redan i dag att myndigheter enbart anvisar digitala tjänster och t.ex. inte längre tillhandahåller pappersblanketter för privatpersoners ansökningar i vissa ärendeslag. Särskilt när det är fråga om ärendetyper där enskilda inte efterfrågar andra kanaler, utan tvärtom utgår från att kontakten med myndigheten ska skötas genom enkla och smidiga digitala tjänster, finns enligt vår bedömning inte anledning att myndigheten inom ramen för gällande rätt aktivt behöver erbjuda någon annan kanal.

När det gäller ärenden som avser ansökan om förmåner ser vi dock anledning att framhålla att det inte förekommer eller får förekomma att någon fråntas rättigheter genom att de saknar faktiska möjligheter att ansöka om att ta del av rättigheten i fråga.[26] Om det visar sig att en person behöver komma i kontakt med en myndighet för att t.ex. ansöka om att få ta del av en förmån faktiskt inte har förutsättningar att använda den digitala tjänst som särskilt har tagits fram för det ändamålet, behöver myndigheten kunna hantera även den situationen. Här finns också anledning att påminna om förvaltningslagens bestämmelse om att en enskild part som vill lämna uppgifter muntligt i ett redan inlett ärende ska ges tillfälle till

[26] Se bl.a. JO 1968 s. 225 angående att en felaktigt eller ofullständigt ifylld blankett inte fick leda till att ansökan inte togs upp till sakprövning.

det, om det inte framstår som obehövligt, och att det är myndigheten som bestämmer hur det ska gå till (t.ex. via telefontjänster eller ett personligt möte).[27] En myndighet behöver alltid beakta tillgänglighetsaspekter, t.ex. om någon enskild till följd av en funktionsnedsättning har svårigheter att tillgodogöra sig muntlig eller skriftlig information. Partens intressen i det enskilda fallet behöver alltså alltid vägas in.[28]

Frågor om hur länge myndigheter, vid sidan av digitala tjänster, också behöver tillhandahålla särskilda pappersblanketter eller formulär får avvägas i förhållande till när förutsättningar finns att på annat sätt ge nödvändig service till enskilda som inte kan eller vill använda den digitala tekniken. Exempelvis kan det vägas in om det fortsatt kommer att vara vanligt att de parter som myndigheten har kontakt med inte har möjlighet att använda de digitala tjänster som tas fram. Myndigheter bör dock enligt vår bedömning sträva efter att sköta informationshanteringen digitalt även när den enskilde inte själv kan eller vill inleda ärendet genom en digital tjänst. Det kan t.ex. åstadkommas genom service i form av kompletterande telefontjänster eller personligt besök på sätt som gör att myndigheten kan registrera nödvändiga uppgifter digitalt så att pappershantering inte längre behövs. En stärkt organisation för lokal statlig service är därmed även positivt ur digitaliseringsperspektiv, eftersom tillgång till personlig service vid myndighetsbesök ökar förutsättningarna att komma i från en pappershantering i förhållande till dem som inte kan eller vill nyttja digitala tjänster.[29]

Här kan också nämnas att biblioteken, som är öppna och tillgängliga för alla, erbjuder ett flertal aktiviteter som syftar till att öka kunskaperna om digitala tjänster. Flera bibliotek erbjuder även digital hjälp utifrån användarnas behov.[30] Det förhållandet att biblioteken också bidrar till att öka den digitala delaktigheten fråntar dock inte myndigheter deras skyldighet enligt förvaltningslagen att själva lämna service och finnas tillgängliga för enskilda.

[27] 24 § förvaltningslagen.
[28] 25 § andra stycket första meningen förvaltningslagen och prop. 2016/17:180 s. 312.
[29] *En organisation för lokal statlig service* (dir. 2017:95).
[30] Se rapporten av Ida Norberg, *Insatser för digital kompetens på folkbiblioteken – En studie om folkbibliotekens arbete med digital delaktighet* (på uppdrag av SKL, Digidelnätverket och Kungliga biblioteket), som finns tillgänglig via https://skl.se/skolakulturfritid/kulturfritid/bibliotek/digitaldelaktighet.13039.html

I detta sammanhang uppkommer vidare frågor om att pappershantering kan behövas för att tillgodose författningskrav på underskrifter från enskilda och frågor om behovet av att bevara en originalhandling eller på annat sätt säkerställa att den enskilde står bakom en viljeyttring. De frågorna återkommer vi till i kapitel 12.2.1.

Även med en strävan att frångå pappershantering förmodar vi, när hela förvaltningens vidd hålls i åtanke, att i vart fall vissa myndigheter under en tid framöver fortsatt behöver hantera handlingar som ges in i fysisk form. Under kartläggningen har det exempelvis beskrivits för oss att det fortfarande är vanligt att kartor ges in och behöver hanteras i pappersform. Möjligen är detta också en fråga om att det behövs nya tekniska lösningar för att kunna hantera digitala kartor med samma funktionalitet som papperskartor.

Vi vill vidare särskilt framhålla att det enligt vår bedömning borde finnas anledning att utgå från att aktörer som i sin yrkesroll kommer i kontakt med förvaltningen, i än högre grad än privatpersoner, bör kunna förväntas använda de digitala kanaler för kommunikation som tas fram. Det finns också exempel på att förvaltningen kräver att en viss typ av digitala kanaler används för ansökan från aktörer som agerar i sin yrkesroll, nämligen förfarandet vid utbetalning i samband med skattereduktion för hushållsarbete. I det fallet har det särskilt reglerats att utförarens begäran om utbetalning ska lämnas elektroniskt.[31]

Ofta torde frågan om vilka kommunikationskanaler som ska användas kunna lösas i samförstånd mellan den myndighet som tar fram digitala tjänster och de aktörer som i sin yrkesroll förväntas använda dem. Enligt vår bedömning vore det ur ett förvaltningsgemensamt perspektiv mindre lämpligt att behöva ta fram särreglering vid varje tillfälle som den digitala förvaltningen kommer att kräva att sådana aktörer använder de digitala tjänster som tillhandahålls för kommunikation, dvs. när ingen parallell pappersprocess kommer att finnas tillgänglig. Vi ser emellertid inte heller förutsättningar för att inom ramen för denna utredning nu föreslå generella skyldigheter för yrkesverksamma aktörer att använda alla typer av digitala tjänster som tillhandahålls och kommer att tillhandahållas inom förvaltningen.

[31] 8 § lagen (2009:194) om förfarandet vid skattereduktion för hushållsarbete och *Ett enklare system för skattereduktion för hushållsarbete*, prop. 2008/09:77.

8.3.3 Ny huvudregel om digital tillgänglighet

Utredningens förslag: 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 säkerhetsskäl eller av andra skäl.

Skälen för utredningens förslag

Våra inledande överväganden

Vi har ovan gjort bedömningen att styrningen av relevanta ärendeflöden och interaktioner med individer och företag till digitala lösningar inte bör utformas som en skyldighet för privatpersoner och företag att använda de digitala tjänster som förvaltningen tillhandahåller. I stället bör det enligt vår bedömning fortsatt vara myndigheter som ska svara för att uppfylla kraven på tillgänglighet, även när det gäller digital tillgänglighet. Med andra ord bör det vara förvaltningen som har en skyldighet att motsvara enskildas förväntningar på att kunna kommunicera digitalt. Den bedömningen ligger också i linje med bl.a. Tallindeklarationen om e-förvaltning, enligt vilken privatpersoner och företag ska ges möjlighet till digitala kanaler för interaktion med förvaltningen om de väljer det.[32]

Huvudregel om digitala mottagningsfunktioner

Som framgått av våra överväganden i kapitel 8.3.1 har vi funnit att det behövs generella, men övergripande och teknikneutrala, regler om digital kommunikation vid kontakter mellan förvaltningen och enskilda. Vi har där också gjort bedömningen att regleringen bör träffa förvaltningen som helhet, dvs. inte enbart statliga myndigheter. Det övergripande syftet med en reglering är att skapa bättre förutsättningar för en sammanhållen digital förvaltning som finns tillgänglig för privatpersoner och företag utifrån deras behov.

Inledningsvis noterar vi att det inte synes finnas några tecken på en teknik- eller samhällsutveckling som innebär att det inom överskådlig tid kan väntas komma fram helt nya sätt för kommunikation

[32] Se Tallindeklarationen på www.newsd.admin.ch/newsd/message/attachments/49838.pdf

till och från förvaltningen. Med andra ord ser vi inte en utveckling som i tekniskt avseende väsentligt skiljer sig från digitala tjänster för att lämna meddelanden till förvaltningen via webben eller kommunikation via lösningar som t.ex. Mina meddelanden. Vad som däremot kan förutspås ligga i den framtida utvecklingen är digitala lösningar där tjänsten inte enbart fokuserar på det skrivna ordet, utan t.ex. inkluderar funktioner för att förmedla information via bild eller ljud. I det följande använder vi begreppen handlingar och meddelanden synonymt i den bemärkelsen att meddelanden är en typ av handlingar som i detta sammanhang är föremål för kommunikation mellan myndighet och enskild.

En reglering med skyldigheter för förvaltningen att motsvara enskildas förväntningar på digital tillgänglighet skulle kunna utformas på olika sätt. I våra överväganden har vi, vid sidan av enskildas intressen av att enkelt komma i kontakt med den digitala förvaltningen, också att beakta bl.a. säkerhets- och kostnadsaspekter för förvaltningen. Särskilt med de sistnämnda aspekterna i åtanke har vi inledningsvis övervägt om det vore möjligt och lämpligt att formulera en reglering om digitala tjänster i första hand som ett målsättningsstadgande, snarare än en uttrycklig skyldighet för förvaltningen. Vid närmare analys har vi emellertid funnit att den typen av icke tvingande bestämmelse vore mindre lämplig, särskilt med beaktande av att regleringen enligt vår uppfattning bör bidra till att det ska vara förutsebart för privatpersoner och företag på vilket sätt de kan förvänta sig att kommunikationen med förvaltningen fungerar.

Mot bakgrund av de nackdelar vi sett med användande av traditionell e-post har vi också övervägt om målsättningen med Digitalt först borde komma till uttryck som en bestämmelse om att myndigheter ska vara skyldiga att tillhandahålla just digitala tjänster, dvs. särskilt framtagna tjänster för att t.ex. inleda ett ärende och kommunicera under ärendehandläggningen. Att i dagsläget uppställa ett sådant generellt och uttryckligt krav skulle emellertid riskera att bli betungande för förvaltningen i kostnadshänseende, särskilt med beaktande av att vi funnit att regleringen bör omfatta hela förvaltningen och inte enbart statliga myndigheter.

Vi har slutligen stannat vid bedömningen att en generell reglering med krav på förvaltningen i fråga om dess digitala tillgänglighet bör utformas helt neutralt i förhållande till vilken form av digital kommunikation som avses. Det krav som enligt oss bör ställas är att en

myndighet ska tillhandahålla en eller flera digitala mottagningsfunktioner dit handlingar kan förmedlas. Vi väljer termen ”digital mottagningsfunktion” för att poängtera att det är ett funktionskrav snarare än en fysisk plats som avses. På senare tid har beskrivningen av hur informationsteknik används också skiftat från begreppet elektronisk till begreppet digital.[33] Vi väljer därför det senare begreppet.

Ett krav på förvaltningen att finnas tillgänglig via digitala mottagningsfunktioner innebär enligt oss en förstärkt möjlighet för enskilda att få tillgång till förvaltningen digitalt. Även lokutionen ”digital mottagningsfunktion” kan emellertid väcka frågan om vilken typ av kommunikation som omfattas. Enligt vår bedömning bör det inte göras någon begränsning av innebörd att enbart skriftliga handlingar kan tas emot i en sådan digital mottagningsfunktion. Termen digital mottagningsfunktion är neutral och kan omfatta även tjänster där handlingar tas emot som innefattar information i form av ljud eller bild.

I lokutionen att det ska vara fråga om en särskild funktion för att ta emot digitala handlingar ligger emellertid en avgränsning i förhållande till t.ex. myndigheters service via muntlig och omedelbar tvåvägskommunikation såsom telefonsamtal, videosamtal eller webbaserade samtal. Trots att även teknik för sådana samtal kan vara digital kan den servicen inte anses innefattas i det särskilda kravet på digital tillgänglighet via mottagningsfunktioner som nu diskuteras. Det sagda utesluter dock inte att användandet av sådana digitala tjänster som har utformats med en mottagningsfunktion kompletteras med möjligheter till service via t.ex. telefonilösningar. Som framgått av våra inledande överväganden bör förvaltningen sträva mot att tillhandahålla de former för service till enskilda, som inte själva kan eller vill använda digitala tjänster, som medför att förvaltningen kan hämta in de uppgifter som behövs för att t.ex. påbörja handläggningen av ett ärende utan att någon pappershantering behöver involveras.

Vi ser inte heller anledning att framhålla tillgänglighet via traditionella e-postadresser, i linje med vad som ovan anförts om de problem som kan förknippas med den formen för kommunikation. Det neutrala begreppet digital mottagningsfunktion kan dock i och för sig sägas omfatta även funktion för mottagande av meddelanden

[33] Jfr Ds 2017:60 s. 50.

genom tekniken för e-post.[34] Här bör emellertid särskilt lyftas fram problemen med att traditionell e-post inte utgör en tillräckligt säker form för kommunikation när det exempelvis gäller förmedling av personuppgifter som är känsliga.

Det krav på myndigheter att vara tillgängliga digitalt som nu diskuteras innebär sammanfattningsvis inte någon skyldighet att kunna ta emot handlingar i någon specifik form eller via någon specifik teknisk lösning. Det bör fortsatt vara upp till respektive myndighet att avgöra de närmare formerna och lösningarna för den digitala tillgängligheten.

De grundläggande krav på myndigheters tillgänglighet som uppställs i 7 § förvaltningslagen bör också fortsatt gälla. En myndighet ska vara tillgänglig för allmänheten i så stor utsträckning som möjligt och vidta de åtgärder i fråga om tillgänglighet som behövs för att den ska kunna uppfylla sina skyldigheter gentemot allmänheten enligt 2 kap. tryckfrihetsförordningen om rätten att ta del av allmänna handlingar. I förhållande till detta grundläggande krav på myndigheter att vara tillgängliga för allmänheten utgör vårt förslag en specificering avseende vad som förväntas av myndigheterna i fråga om just digital tillgänglighet.

En offentlig aktör som omfattas av det nya s.k. webbtillgänglighetsdirektivets[35] tillämpningsområde ska också uppfylla de tillgänglighetskrav som kommer att följa av den lagstiftning som genomför det direktivet i svensk rätt.[36] Bland annat ska sådan digital service som tillhandahålls via tekniska lösningar vilka omfattas av den regleringen, dvs. webbplatser och mobila applikationer,[37] följa även dessa tillgänglighetskrav.

Av de grundläggande kraven på tillgänglighet som följer av 7 § förvaltningslagen framgår att det är myndigheten som informerar allmänheten om hur och när kontakter kan tas. Detsamma bör enligt

[34] I detta sammanhang kan det finnas anledning att erinra om att det kan vara olämpligt även ur arbetsrättslig synpunkt att anordna kommunikationen med traditionella e-postadresser för enskilda befattningshavare, eftersom det finns gränser för på vilket sätt arbetsgivaren får övervaka den typen av kommunikation. Se Europadomstolens dom i målet Bărbulescu v Romania ([2017] ECHR 754). Europadomstolen fann att en arbetsgivares övervakning av en arbetstagares personliga kommunikation på Yahoo Messenger innebar ett brott mot artikel 8 i Europakonventionen.

[35] Europaparlamentets och rådets direktiv (EU) 2016/2012 av den 26 oktober 2016 om tillgänglighet avseende offentliga myndigheters webbplatser och mobila applikationer (webbtillgänglighetsdirektivet).

[36] Se Ds 2017:60.

[37] Artikel 4 webbtillgänglighetsdirektivet och a.a. s. 47 f.

vår uppfattning gälla i fråga om kontakter via de särskilda digitala mottagningsfunktioner som nu diskuteras. Enligt vår uppfattning bör det emellertid krävas att det är enkelt för enskilda att förstå vilka digitala kontaktvägar som de förväntas använda för att uppnå sitt syfte med att kontakta myndigheten. Det kanske inte är möjligt eller lämpligt att t.ex. inleda ärenden via sociala medier trots att en myndighet finns tillgänglig där. Enligt vår bedömning bör detta markeras genom att det i den nu föreslagna regleringen ställs upp krav på att myndigheten ska anvisa en eller flera digitala mottagningsfunktioner dit enskilda kan förmedla handlingar.

Krav på att myndigheterna ska anvisa digitala mottagningsfunktioner förväntas enligt vår bedömning bidra till förenklingar för den enskilde samtidigt som myndigheten genom sådana anvisningar har förutsättningar att styra ärendeflöden mot de kommunikationslösningar som myndigheten bedömt vara lämpliga. Det skapar också goda förutsättningar för att åstadkomma infrastrukturlösningar med t.ex. en gemensam plattform för olika myndigheters digitala tjänster. I detta sammanhang bör också erinras om att det i vissa fall kan finnas lagstiftning, t.ex. inom EU-rätten, som kräver att en viss digital kanal används för att komma i kontakt med förvaltningen i ett visst syfte. I de fallen bör denna digitala mottagningsfunktion anvisas.

När huvudregeln inte tillämpas

I föregående avsnitt har vi konstaterat att en bestämmelse om att myndigheter ska anvisa, vad som kan vara en eller flera, digitala mottagningsfunktioner dit handlingar kan förmedlas förhåller sig neutral till vilken form av digital kommunikation som avses. Med beaktande av att den valda ordalydelsen inte utesluter tekniska lösningar som t.ex. e-post skulle det kunna hävdas att motsvarande krav har uppställts i 1986 års förvaltningslag och att det därför kan förväntas att förvaltningen som helhet redan uppfyller ett sådant krav. Någon möjlighet att frångå kravet skulle därmed inte behövas.

Vi ser emellertid framför oss att enskilda framöver i allt större utsträckning kommer att förvänta sig ökad digital service i förhållande till vad som kan ges genom e-post, och ser som beskrivits flera nackdelar med den kommunikationsformen. Även en neutralt formulerad reglering om att förvaltningen ska vara digitalt tillgänglig

kommer därför vid varje tid att behöva möta de tillgänglighetskrav som allmänheten uppställer.[38] I kapitel 8.1 och i det ovan sagda har vidare flera nackdelar med traditionell e-post för kommunikation med förvaltningen uppmärksammats, bl.a. det förhållandet att den kanalen inte är tillräckligt säker för viss kommunikation. Det är därför inte den typen av kommunikationskanal som vi ser kommer att förväntas av den framtida digitala förvaltningen. Mot bakgrund av detta, och för att undvika att den föreslagna huvudregeln vid någon tidpunkt eller i något hänseende blir alltför betungande för förvaltningen, eller leder till orimliga eller oförutsedda konsekvenser för det allmänna, bör den därför inte utformas som ett ovillkorligt krav på förvaltningen.

Det ska här framhållas att den reglering vi nu diskuterar, som framgått i kapitel 8.3.1, inte kommer att ha företräde framför t.ex. bestämmelser i registerförfattningar eller bestämmelser om sekretess. Det kan alltså fortfarande finnas annan reglering som uppställer hinder mot digital kommunikation. Vidare ska bestämmelser med krav på säkerhet följas (se bl.a. kapitel 4.5 om regler till skydd för enskildas personliga integritet, kapitel 4.6 om sekretess, kapitel 9 om informationssäkerhet och kapitel 12 om behov av fortsatt rättsutveckling). Det betyder bl.a. att en myndighet behöver uppnå tillräcklig säkerhet för att digital kommunikation ska kunna krävas. Mot den bakgrunden bedömer vi att det bör framgå av regleringen att en myndighet inte ska tillhandahålla en digital mottagningsfunktion i de fall det är olämpligt av säkerhetsskäl. Viss verksamhet i den statliga förvaltningen torde vidare med beaktande av säkerhetsaspekter vara av sådan karaktär att det inte alls är lämpligt med digital kommunikation i förhållande till enskilda, i vart fall inte med nu kända medel. Samtidigt torde frågan om säkerhetsnivå inte sällan höra samman med kostnadsaspekter. Även med hänsyn tagen till överväganden om kostnadseffektivitet skulle det i vissa fall kunna bedömas vara olämpligt att en myndighet alltid måste tillhandahålla en digital mottagningsfunktion. Intresset av att låta bli att tillhandahålla en digital mottagningsfunktion, t.ex. med anledning av kostnadsaspekter, behöver emellertid sättas i relation till enskildas intressen av digital tillgänglighet till myndigheten. Vid den bedömning som en myndighet

[38] Jfr regeringens uttalande i *Några förvaltningsrättsliga frågor*, prop. 2002/03:62 s. 10 f.

gör av om det är olämpligt att tillhandahålla en digital mottagningsfunktion bör därför, enligt oss, enskildas intressen av digital tillgänglighet till myndigheten särskilt beaktas.

8.3.4 Anpassad regel om ankomstdag

Utredningens förslag: En handling som har förmedlats till en anvisad digital mottagningsfunktion ska anses ha kommit in till myndigheten när den tagits emot där.

Skälen för utredningens förslag

Tidigare överväganden om reglering av ankomstdag

En handling anses som huvudregel komma in till en myndighet den dag då handlingen anländer till myndigheten eller kommer en behörig tjänsteman till handa.[39] Vid handläggning av mål och ärenden är det av flera skäl viktigt att kunna fastställa vid vilken tidpunkt handlingar har kommit in till myndigheten. Frågan om vilken dag en handling kommit in är bl.a. av betydelse för att bedöma tidsfrister, till exempel vid beräkning av retroaktiv tid eller när någon begär omprövning av ett beslut. Ankomstdagen för en handling kan också utlösa en frist inom vilken myndigheten ska göra en prövning och meddela ett beslut eller ligga till grund för exempelvis en registreringsåtgärd som får rättsverkningar för den enskilde.

I den nya förvaltningslagen har, med viss anpassning, särskilda hjälpregler behållits om när traditionella postförsändelser eller avier anses ha kommit in till myndigheten via postkontor eller postlåda.[40] Hjälpreglerna behölls trots att risken för att någon enskild ska drabbas av rättsförluster på grund av förseningar i postgången bedömdes vara förhållandevis liten. Utrymmet för osäkerhet bedömdes dock vara något större i dessa situationer än när det t.ex. gäller handlingar som skickas in via en elektronisk kontaktväg.[41] Det har

[39] 10 § förvaltningslagen (1986:223). Bestämmelserna om inkommande handlingar i 44 § förvaltningsprocesslagen (1971:291), 33 kap. 3 § rättegångsbalken och 44 § lagen (1996:242) om domstolsärenden är i sak samordnade.
[40] 22 § andra och tredje stycket förvaltningslagen.
[41] Prop. 2016/17:180 s. 143.

inte antagits någon uttrycklig hjälpregel om när digitala handlingar anses ha kommit in till en myndighet.

Våra överväganden om en hjälpregel om ankomstdag

Den inledningsvis beskrivna huvudregeln i förvaltningslagen om tidpunkt för när en handling anses ha kommit in till en myndighet är enkel. Bestämmelsen innefattar enligt vår bedömning vad som krävs för att man i normalsituationer med en rimlig grad av precision ska kunna fastställa när en handling har kommit in till myndigheten. I flera fall borde den därför vara tillräcklig även i de situationer där den enskilde kommunicerar med myndigheten via digitala kanaler. Det kan därför hävdas att risken för att enskilda lider några rättsförluster på grund av tveksamheter i fråga om dagen för en handlings inkommande är så låga att det inte behövs någon hjälpregel för att avgöra när en handling som förmedlas i digital form har kommit in till en myndighet.

Det finns emellertid skäl som talar för att fortsatt överväga hjälpreglering som anger när handlingar som översänds digitalt ska anses ha kommit in till en myndighet. Ett inledande skäl är att en sådan reglering skulle klargöra rättsläget för de myndigheter i förvaltningen som ska tillämpa reglerna, vid såväl utvecklingsarbeten när nya digitala tjänster tas fram som vid bedömningar av ankomstdag i samband med att handlingar ges in i enskilda ärenden.

Ytterligare ett skäl för att fortsatt överväga reglering av handlingars ankomst till en myndighet via digitala kanaler är att skapa rättslig klarhet för privatpersoner och företag som ska använda de digitala tjänster som förvaltningen tar fram. Det skälet väger enligt vår bedömning tungt.

Regeringens bedömning av utrymmet för osäkerhet i fråga om tidpunkten för när handlingar som lämnas via digitala kommunikationskanaler kommer in till en myndighet synes i viss utsträckning utgå från att det inte, eller sällan, uppstår några fel eller brister i den digitala kommunikationen.[42] Det förekommer emellertid då och då avbrott i driften, och avbrott kan framöver förväntas även med ett gott informationssäkerhetsarbete i grunden. Också andra typer av risker för fel i den digitala kommunikationen, oavsett om de beror

[42] A. prop. s. 143.

på misstag vid handhavandet från den enskildes sida eller på myndighetens utformning av tjänster eller annat, kan leda till att handlingar inte kommer fram på avsett sätt i den digitala miljön. Det finns därför enligt oss anledning att vara uppmärksam på att enskilda kan uppleva en osäkerhet över vad som gäller i fråga om tidsfrister om det uppstår avbrott eller brister i den digitala kommunikationen med en myndighet. Här bör särskilt beaktas att avsändaren enligt förarbetena till den nya förvaltningslagen bär risken om överföringen inte fungerar eller försenas, och att det är av betydelse att myndigheterna på ett någorlunda enkelt sätt kan fastställa när en handling är att anse som inkommen utan att rättssäkerheten åsidosätts.[43] Hur ansvar och risker fördelas kan enligt vår bedömning påverka incitamenten för privatpersoner och företag att använda digitala kanaler för kommunikation med förvaltningen.

Vi har också föreslagit att det ska införas en ny huvudregel om att en myndighet ska tillhandahålla, och på lämpligt sätt anvisa, en eller flera digitala mottagningsfunktioner dit handlingar kan förmedlas. Det finns anledning att lyfta fram just den anvisade mottagningsfunktionen särskilt, till skillnad från andra kanaler för kommunikation som också kan vara digitala, t.ex. konton på sociala medier. I sådana särskilda mottagningsfunktioner finns det förutsättningar för myndigheten att bl.a. anordna säkerheten på ett betryggande sätt, exempelvis genom att handlingar i form av meddelanden som innehåller skadlig kod stoppas i myndighetens säkerhetssystem innan de når den digitala mottagningsfunktionen. Sådana handlingar ska enligt vår bedömning inte anses ha kommit in till myndigheten, trots att de kanske tekniskt finns tillgängliga på myndighetens server för någon befattningshavare vid myndigheten.

I kapitel 8.3.1 har vi övervägt möjligheten att ålägga enskilda en skyldighet att använda digitala kanaler, men inte funnit att det nu är möjligt eller lämpligt att generellt införa en sådan skyldighet. Det leder till att förvaltningen har att hantera såväl digitala kommunikationskanaler samtidigt som ansökningar och andra handlingar parallellt, i vart fall i vissa situationer, fortsatt måste kunna hanteras på papper. Vi har också belyst nackdelarna med sådan parallell hantering, såväl ur kostnadssynpunkt som med beaktande av brister i möjligheten att enkelt få insyn i och överblick över myndighetens verksamhet. Enligt vår bedömning bör det därför prioriteras att

[43] A. prop. s. 138 och 140 f.

överväga sådan reglering som kan fungera som incitament för att öka graden av användning av de digitala tjänster som tas fram, så att tidsperioden för parallell pappershantering i den digitala förvaltningen kan hållas så kort som möjligt.

En reglering som klargör vad som gäller i fråga om ankomsttidpunkt för de handlingar som ges in digitalt skulle, i likhet med vad som redan gäller för papperspost, syfta till att begränsa den enskildes risk. En sådan reglering skulle enligt oss bidra till att skapa ökad trygghet och incitament för enskilda att använda de digitala tjänster som tillhandahålls. En reglering får också förutsättas skapa större klarhet än helt avtalsbaserad fördelning av ansvar och risk mellan den enskilde och en myndighet. Det sistnämnda kan t.ex. innebära att den enskilde, för att kunna använda en specifik tjänst, måste godkänna den riskfördelning som anges i myndighetens användarvillkor.

Redan med beaktande av de skäl som här inledningsvis har anförts ser utredningen att det finns behov av att föreslå reglering om dels hjälpbestämmelser för att fastslå tid för ankomst av handlingar som kommer in till en myndighet via digitala kanaler, dels underrättelser till avsändaren om att handlingar har tagits emot. I det följande presenteras de närmare förslagen och ytterligare några skäl varför vi anser att regleringen behövs.

En hjälpregel för bestämmande av ankomstdag

Vi har övervägt om det, i stället för att föreslå en generell och för förvaltningen gemensam reglering, vore bättre att föreslå en reglering i olika specialförfattningar för att åstadkomma en mer situationsanpassad reglering om hur ankomsttidpunkt bestäms vid kommunikation med förvaltningen. Sådan särreglering om ankomstdag i olika specialförfattningar bör emellertid undvikas eftersom det riskerar att ge upphov till oklarheter hos både allmänheten och myndigheter.[44]

Det framstår också som särskilt angeläget att åstadkomma en hjälpregel om bestämmande av ankomsttid för handlingar som förmedlas digitalt för att skapa goda rättsliga grundförutsättningar för en nationell plattform för olika myndigheters digitala tjänster dit den enskilde enkelt kan vända sig. Här kan särskilt framhållas att det

[44] A. prop. s. 145.

ska vara enkelt för den enskilde oavsett vilken myndighet som ska hantera den enskildes ärende eller ärenden (se kapitel 6.6 om att offentliga tjänster enligt EU:s handlingsplan för e-förvaltning bör tillhandahållas via en enda kontaktpunkt,”one-stop-shop”, och via olika kanaler).[45] Det framstår därför som lämpligt att den hjälpreglering som här diskuteras bör vara gemensam för förvaltningen som helhet.

I linje med vad som anförts i kapitel 6.2 ser vi inte skäl att belasta lagtext med detaljer eller tekniska termer. Den reglering som föreslås behöver också kunna appliceras på en mängd olika tekniska lösningar. Regleringen bör med andra ord kunna gälla för hela den palett av digital kommunikation som redan förekommer. Det gäller allt från mer avancerade tekniska lösningar med maskin-till-maskin-inläsning av information genom öppna applikationer, digitala tjänster hos myndigheter med Mina sidor till andra former av digitala tjänster. Ibland kompletteras sådana lösningar också av nya sätt att t.ex. ge service via telefoni. Regleringen behöver därtill vara möjlig att tillämpa på kommunikation genom tekniska lösningar som ännu inte är kända.

En modell för utformning av hjälpregel som knyter an till den ovan föreslagna och neutrala huvudregeln om att myndigheter ska tillhandahålla och anvisa digitala mottagningsfunktioner, framstår som den lämpligaste lösningen.[46] Vi föreslår därför en bestämmelse om att en handling som har förmedlats till en anvisad digital mottagningsfunktion bör anses ha kommit in till myndigheten när den tagits emot i mottagningsfunktionen. En sådan reglering bör såvitt vi ser det inte kräva någon omarbetning av de digitala tjänster som redan har tagits fram, men däremot åstadkomma nyttor i form av bl.a. ökat incitament för användande av tjänsterna. En sådan reglering bör också ge goda rättsliga förutsättningar för en gemensam plattform för olika myndigheters digitala tjänster som diskuterats ovan.

[45] Jfr t.ex. den norska portalen Altinn på https://www.altinn.no/
[46] Jfr också *Vägledning för hantering av inkommande elektroniska handlingar*, E-nämnden, 11 maj 2005 och *Promemoria om inkommandetidpunkt – när har en handling kommit in till myndighet*?, eSam, 31 oktober 2017.

8.3.5 Ny huvudregel om underrättelse när handlingar tas emot digitalt

Utredningens bedömning: För att skapa tillit till digitala förfaranden bör huvudregeln vara att myndigheter ska underrätta avsändare om att en handling har anlänt till en anvisad digital mottagningsfunktion.

En bestämmelse om att myndigheter ska lämna underrättelse om mottagande av handlingar bör dock begränsas till att omfatta sådana handlingar som medför ärendehandläggning. Det bör också finnas möjlighet till undantag från huvudregeln.

Utredningens förslag: En myndighet ska digitalt förmedla underrättelse till avsändaren när en handling har anlänt till en anvisad digital mottagningsfunktion.

Myndigheten behöver inte förmedla underrättelse till avsändaren om

1. det på annat sätt framgår för avsändaren att handlingen har tagits emot,
2. handlingen utan onödigt dröjsmål besvaras med ett helt eller delvis automatiserat beslut, eller
3. det är olämpligt.

Skälen för utredningens bedömning och förslag: I propositionen med förslag till ny förvaltningslag har regeringen anfört att det på ett övergripande plan bör uppmuntras att myndigheterna säkerställer tillförlitliga och säkra system för bekräftelse av handlingar som tas emot i mottagningsställen för elektroniska meddelanden. Med beaktande av remissutfallet har regeringen dock inte funnit skäl att genomföra förslaget om en generell skyldighet för myndigheterna att bekräfta elektroniska meddelanden, utan menat att det kan vara lämpligare att i stället vid behov knyta ett eventuellt åliggande till de fall där enskilda har ett mer konkret och praktiskt behov av att få en sådan bekräftelse.[47] Frågan kommer i nytt ljus i anledning av våra förslag om huvudregler om digital kommunikation och hjälpreglering för att bestämma ankomstdag för digitala handlingar.

[47] Prop. 2016/17:180 s. 70.

Vad som ovan anförts om behovet av ökade incitament för att enskilda ska känna sig trygga med att använda de digitala tjänster som tas fram, i syfte att parallell pappershantering så snart som möjligt kan utmönstras, är emellertid enligt vår bedömning ett tungt vägande skäl till varför reglering om underrättelser när handlingar tas emot digitalt fortfarande behöver övervägas. Det handlar som sagt om att skapa så goda förutsättningar som möjligt för att enskilda ska välja att använda de digitala kanaler för kommunikation som tas fram inom förvaltningen, utan att det samtidigt sätts upp detaljerade krav som hindrar förvaltningen från att utforma tjänsterna i enlighet med vad som är lämpligast i de enskilda fallen.

I likhet med vad som ovan anförts om att huvudregeln bör vara digital kommunikation bör det enligt vår bedömning även vara en huvudregel att myndigheter ska underrätta avsändare om att ett meddelande har anlänt till en anvisad digital mottagningsfunktion. Samtidigt ska de förslag vi lämnar inte medföra orimligt betungande krav på förvaltningen. Vår strävan är i stället närmast att i rättsregler befästa och beskriva vad enskilda i dag och framöver kan förvänta sig av den digitala förvaltningen, för att minska den enskildes risk för rättsförluster och i stället åstadkomma tillit som ger grund för hög grad av användning av de digitala tjänster som tillhandahålls.

Vi föreslår, i linje med det nyss sagda, en huvudregel om att myndigheter bör underrätta enskilda om att meddelanden tagits emot. En underrättelse förutsätter, vilket närmare belyses i kapitel 8.3.6, av rättssäkerhetsskäl normalt en aktiv kommunikation från myndighetens sida. För att bestämmelsen inte ska bli för betungande bör den därför endast träffa det område där det finns ett behov av sådana underrättelser. Det huvudsakliga praktiska behovet som enskilda kan ha av att få en sådan bekräftelse ligger enligt vår bedömning inom ramen för myndigheternas ärendehandläggning. En första avgränsning bör därför göras till ärendehandläggningen.

Från huvudregeln bör det vidare ges flera möjligheter till undantag. Det bör inte krävas särskilda underrättelser om mottagande av handlingar i alla situationer när enskildas meddelanden medför ärendehandläggning. Aktivt förmedlade underrättelser bör inledningsvis inte krävas om det på annat sätt framgår för avsändaren att handlingen har tagits emot, t.ex. genom att en enskild som är inloggad i en digital tjänst hos myndigheten för att där fylla i och

förmedla en ansökan direkt kan se att handlingen tagits emot. I sådant fall behöver myndigheten inte dessutom aktivt kommunicera ut en underrättelse om att handlingen har tagits emot.

En särskild underrättelse framstår vidare som obehövlig om myndigheten tagit emot en handling som utan onödigt dröjsmål kommer att besvaras digitalt med ett helt eller delvis automatiserat beslut. Det kan även, beroende på situationen, finnas andra skäl som gör att det är olämpligt att lämna underrättelse till den enskilde om att dennes meddelande har tagits emot av myndigheten. Det skulle t.ex. kunna vara fråga om att enskilda i något sammanhang behöver kunna agera anonymt när de via en digital tjänst kommunicerar med en myndighet. Det skulle i sådant fall kunna bedömas vara olämpligt att anordna tekniska förutsättningar för återkoppling till den enskilde om att meddelandet har tagits emot.

Den föreslagna regleringen torde såvitt vi kan bedöma inte kräva omarbetning av de digitala tjänster som redan har tagits fram. Att enskilda kan konstatera att förvaltningens digitala tjänster är rättssäkra i fråga om mottagande av handlingar, genom att underrättelser i de beskrivna fallen lämnas, bidrar enligt vår uppfattning till att öka incitamenten för att tjänsterna ska användas. Ytterligare ett syfte med den föreslagna regleringen är att ge stabila förutsättningar för de myndighetsgemensamma digitala tjänster som framöver kommer att tas fram, liksom för en gemensam plattform för olika myndigheters digitala tjänster som diskuterats ovan.

8.3.6 Ny huvudregel om digital kommunikation till enskilda

Utredningens bedömning: För att det ska vara tydligt och förutsebart för enskilda hur förvaltningen kommunicerar underrättelser eller andra handlingar bör huvudsakliga principer framgå i reglering.

Utredningens förslag: En myndighets skriftliga underrättelser eller andra handlingar till enskilda ska förmedlas digitalt, om det inte är olämpligt av säkerhetsskäl eller av andra skäl.

Enskilda kan meddela att de inte önskar ta emot skriftliga underrättelser eller andra handlingar från myndigheten i digital form.

Följdändringar ska göras i förvaltningslagens bestämmelser om dels kommunikation, dels underrättelse om innehållet i beslut och hur ett överklagande går till.

Skälen för utredningens bedömning och förslag

Våra inledande överväganden

I tidigare avsnitt (se kapitel 8.3.2) har vi bedömt att det inte nu bör införas en förvaltningsgemensam reglering som ålägger privatpersoner och företag en generell skyldighet att använda de digitala tjänster som förvaltningen tillhandahåller.

De fördelar som digitalisering av förvaltningen medför behöver emellertid tas till vara så att såväl den breda allmänheten som enskilda med särskilda behov kan få enklare, snabbare och förbättrad tillgång till beslut och annan information från förvaltningens sida.

Därtill kommer vår inledningsvis gjorda bedömning avseende behovet av regler om digital kommunikation vid kontakter mellan förvaltningen och enskilda för att såväl styra som stödja förvaltningens utvecklingsarbeten (se kapitel 8.3.1). Det förtjänar att särskilt framhållas att ett syfte med att överväga ny eller anpassad reglering om kommunikation från förvaltningen till enskilda är att pågående, planerad och kommande digitalisering ska leda till mer rättssäkra förfaranden, inte till rättsosäkerhet. Regleringen bör också enligt vår bedömning ge enskilda en rättvisande bild av hur förvaltningens kommunikation faktiskt sköts och i allt högre utsträckning kommer att skötas. För att det ska vara tydligt och förutsebart för enskilda hur förvaltningen kommunicerar underrättelser eller andra handlingar bör huvudsakliga principer enligt vår bedömning framgå i reglering.

Enkla och snabba förfaranden för underrättelser om beslut och annan kommunikation medför därtill effektivitetsvinster för förvaltningen. Genom att öka graden av digital förmedling av underrättelser och andra handlingar till enskilda kan förvaltningen minska såväl kostnader som resursåtgång för att hantera utskick av papperspost. En minskning av mängden papperspost från förvaltningen leder också till minskad miljöpåverkan.

Gällande rätt i förvaltningslagen m.m.

Kommunikation av beslutsunderlag

Inom bl.a. förvaltningsrätten kommer den grundläggande rättsprincipen att ingen ska dömas ohörd till uttryck som en kommunikationsprincip. En regelrätt kommunikation förutsätter, till skillnad från den allmänna rätt till insyn i det egna ärendet som gäller för parter, att en myndighet aktivt både informerar en part om sådana uppgifter som har tillförts ärendet och ger parten tillfälle att lämna synpunkter på innehållet i uppgifterna. Tillämpningen av kommunikationsprincipen fyller också en viktig funktion som utredningsmedel, eftersom den säkerställer ett fortlöpande utbyte av information och argument mellan dem som medverkar i ärendet. På så sätt bidrar kommunikationsskyldigheten till att uppfylla de övergripande ändamålen att värna enskildas rättssäkerhet och underlätta snabba avgöranden. I detta sammanhang görs ingen skillnad mellan fysiska eller juridiska personer, inte heller mellan enskilda och offentliga parter.[48]

Enligt 25 § första stycket första meningen förvaltningslagen ska en myndighet, innan den fattar beslut i ett ärende och om det inte är uppenbart obehövligt, underrätta den som är part om allt material av betydelse för beslutet och ge parten tillfälle att inom en bestämd tid yttra sig över materialet. Kommunikation ska alltså föregå allt beslutsfattande, inte bara ärendets slutliga avgörande. Skyldigheten att kommunicera innefattar dock enbart sådant material som utgör underlag för beslutet, inte varje uppgift som tillförts utifrån. Regeln innebär också att kommunikation inte behöver ske om det är uppenbart obehövligt. Detta rekvisit ska emellertid tolkas snävt och är tillämpligt enbart i sådana fall där behovet av kommunikation – sett ur den enskildes perspektiv – är mindre framträdande eller helt saknas. Det är t.ex. i många fall uppenbart obehövligt att kommunicera uppgifter som har lämnats av parten själv.

Det finns också i 25 § första stycket 1–3 förvaltningslagen undantag från huvudregeln om obligatorisk kommunikation. Enligt första stycket 1 får myndigheten avstå från kommunikation om ärendet gäller anställning av någon och det inte är fråga om prövning i högre instans efter överklagande. Av första stycket 2 följer att myndigheten får avstå från kommunikation om det kan befaras att det

[48] Prop. 2016/17:180 s. 154.

annars skulle bli avsevärt svårare att genomföra beslutet. Enligt första stycket 3 får myndigheten avstå från kommunikation om ett väsentligt allmänt eller enskilt intresse kräver att beslutet meddelas omedelbart.

Av 25 § andra stycket första meningen förvaltningslagen följer att myndigheten bestämmer hur underrättelse ska ske. Kommunikation kan genomföras såväl muntligt som skriftligt. Ett typiskt exempel är enligt förarbetsuttalanden att myndigheten kommunicerar handlingar genom att skicka kopior av handlingarna till parten. Bestämmelsen hindrar dock inte att parten får del av materialet genom t.ex. ett telefonsamtal eller i samband med besök hos myndigheten. Myndighetens val av underrättelseform kan dock inte göras helt skönsmässigt utan måste ske med beaktande av det allmänna kravet på service och de allmänna utgångspunkterna för handläggningen i 6 och 9 §§ förvaltningslagen. Det innebär bl.a. att myndigheten måste beakta tillgänglighetsaspekter, exempelvis om någon enskild till följd av en funktionsnedsättning har svårigheter att tillgodogöra sig muntlig eller skriftlig information. Myndigheten måste också välja den underrättelseform som med beaktande av partens intressen i det enskilda fallet är enklast och ger det snabbaste resultatet.[49]

I 25 § andra stycket andra meningen förvaltningslagen anges att underrättelse får ske genom delgivning. Det innebär att myndigheten kan använda sig av delgivning i enlighet med delgivningslagen (2010:1932) för att säkerställa att parten fått del av materialet.

Enligt 25 § tredje stycket förvaltningslagen gäller begränsningar i kravet på obligatorisk kommunikation till följd av sekretess.

Bestämmelser om kommunikation av besluts- eller processunderlag finns också i annan lagstiftning. Här kan bl.a. nämnas den reglering som finns i rättegångsbalken och i förvaltningsprocesslagen (1971:291). Där finns även bestämmelser om delgivning.

Underrättelse om beslut och överklagande

En myndighet som meddelar ett beslut i ett ärende ska enligt 33 § första stycket förvaltningslagen så snart som möjligt underrätta den som är part om det fullständiga innehållet i beslutet, om det inte är obehövligt. Det är av betydelse i flera avseenden att en myndighet tillkännager sina beslut för parter och andra intressenter. För den enskilde är det naturligtvis av vikt att få reda på utgången i ett ärende

[49] A. prop. s. 312.

som rör honom eller henne och i de allra flesta fall också vilka beslut som fattats under handläggningen. Genom att beslutet ges till känna för den det riktar sig till börjar i allmänhet också överklagandetiden att löpa. Dessutom kan åtskilliga beslut, i synnerhet förpliktande sådana, ofta inte verkställas förrän den som direkt berörs av beslutet fått del av detta.

Att det fullständiga innehållet ska redovisas för parten innebär att det inte är tillräckligt att underrätta parten i sammandrag om innebörden av beslutet. Parten ska alltså underrättas om beslutet i sin helhet. Underrättelseskyldigheten omfattar formellt alla slags beslut som myndigheten fattar under handläggningen av ett ärende. Undantagsmöjligheten ska enligt förarbetsuttalanden tolkas snävt. Det måste i princip framstå som klart för myndigheten att åtgärden inte har någon funktion att fylla i det aktuella fallet.[50]

Om en part får överklaga ett beslut är myndigheten enligt 33 § andra stycket förvaltningslagen också skyldig att lämna underrättelse om hur ett eventuellt överklagande ska gå till. En sådan underrättelse ska innehålla information om vilka krav som ställs på överklagandets form och innehåll, vad som gäller i fråga om överklagandetid och information om till vilken myndighet överklagandet ska vara ställt och var det ska skickas. Bestämmelsen syftar till att säkerställa att parten får nödvändig vägledning för att kunna ta till vara sin rätt. Det följer också av bestämmelsen att myndigheten samtidigt som den lämnar underrättelse om hur man överklagar i förekommande fall ska upplysa parten om avvikande meningar som har antecknats.

Enligt 33 § tredje stycket förvaltningslagen bestämmer myndigheten själv hur en underrättelse om ett beslut ska gå till. Underrättelsen kan vara skriftlig eller muntlig. En part har dock alltid rätt att få en skriftlig underrättelse om han eller hon begär det. I förarbetsuttalanden anges att även om myndigheten i andra fall har en valfrihet i fråga om formen torde det typiskt sett vara lämpligt att myndigheten även då lämnar en skriftlig underrättelse. En muntlig underrättelse bör lämnas endast i undantagsfall, främst då handläggningen i sin helhet har skett muntligt och beslutet är enkelt att motivera och förstå.[51]

[50] A. prop. s. 324.
[51] A. prop. s. 324.

Det anges vidare i förarbetsuttalande att en skriftlig underrättelse kan ges genom översändande av en handling i en vanlig postförsändelse. En annan tänkbar överföringsmetod kan vara användning av e-post. Regeringen har ansett att lagen inte bör innehålla någon exemplifierande uppräkning av olika varianter av försändelser eftersom det finns en risk att en sådan uppräkning låser tillämpningen till de varianter som för närvarande är kända och således överblickbara. Lagtexten borde i stället utformas så att den gör det möjligt att använda också sådana kommunikationsmetoder, främst av elektroniskt slag, som för närvarande är mindre utvecklade eller ännu inte förekommande.[52]

Myndighetens val av underrättelseform måste, bl.a. när det gäller underrättelse om beslut och överklagande, ske även med beaktande av det allmänna kravet på service och de allmänna utgångspunkterna för handläggningen i 6 och 9 §§ förvaltningslagen (jfr vad som angetts i avsnittet ovan om kommunikation). Myndigheten måste sammanfattningsvis välja den underrättelseform som med beaktande av partens intressen i det enskilda fallet är enklast.[53]

Av 33 § fjärde stycket förvaltningslagen framgår att underrättelse får ske genom delgivning. Det innebär att myndigheten kan använda sig av de metoder för delgivning som regleras i delgivningslagen för att säkerställa att parten får del av underrättelsen. I valet om sättet för underrättelse bör särskilt beaktas om behov finns att få bevis om utgångspunkten för den tid inom vilken den enskilde kan överklaga beslutet. I vilka fall det behövs bevis om mottagandet får avgöras med hänsyn till ärendets utgång och karaktär.

Reglerna om underrättelse om innehållet i beslut och hur ett överklagande går till ska tillämpas också när någon som inte är part begär att få ta del av ett beslut som han eller hon får överklaga (34 § förvaltningslagen).

Bestämmelser om underrättelser om beslut och överklaganden finns också i annan lagstiftning. Här kan bl.a. nämnas den reglering som, beträffande allmän domstols dom eller beslut, finns i förordningen (1996:271) om mål och ärenden i allmän domstol och den reglering som, beträffande förvaltningsdomstols beslut, finns i förvaltningsprocesslagen.

[52] A. prop. s. 208.
[53] A. prop. s. 207 och 324 f.

Andra meddelanden

Även utanför den ärendehandläggning som myndigheter utför finns behov av att förvaltningen kommunicerar med enskilda. Det gäller i första hand förvaltningens förmedling av information av service-karaktär till enskilda. Exempelvis kan det gälla information som kan ha en påverkan på hur privatpersoner väljer att agera i förhållande till förvaltningen, t.ex. information avseende föräldraförsäkringen som kan inverka på hur föräldrar väljer att planera och ansöka om föräldrapenning.

Även begäran om utlämnande av allmän handling föranleder att myndigheter förmedlar de begärda handlingarna till den som begärt dem utlämnade. Denna sistnämnda aspekt behandlas inte vidare inom ramen för detta kapitel. Vi berör dock frågan i kapitel 12.2.5 och 12.2.7.

Tidigare överväganden om digital kommunikation till enskilda

Digitaliseringskommissionen har föreslagit att regeringen under en treårsperiod borde fasa ut traditionell posthantering från de statliga myndigheterna och ge samtliga individer och företag tillgång till en digital postlåda. Den traditionella posthanteringen skulle dock kunna behållas genom ett aktivt val från individen eller företaget.[54]

Utredningen om effektiv styrning av nationella digitala tjänster har också gjort bedömningen att i princip all myndighetspost måste vara digital inom ett par år. För att åstadkomma detta har utredningen föreslagit en rättighet för privatpersoner och företag att som mottagare få försändelser från statliga myndigheter elektroniskt, om de uttryckligen har begärt det och det inte finns särskilda skäl för undantag. Utredningen har också föreslagit en förordningsreglering som bl.a. innebär att statliga myndigheter som avsändare ska skicka säkra elektroniska försändelser, om inte regeringen beslutar annat. Kommunala myndigheter bör enligt utredningen inte åläggas en sådan skyldighet utan får som avsändare använda den infrastruktur som tas fram (här avses Mina meddelanden). Utredningen bedömde vidare bl.a. att det inte var ett alternativ att göra det obligatoriskt för

[54] Digitaliseringskommissionens betänkande *Digitaliseringens transformerande kraft – vägval för framtiden* (SOU 2015:91), s. 154 f.

enskilda att ha en digital brevlåda så länge som flertalet relevanta myndigheter inte var anslutna.[55]

Digitalt först vid kommunikation till enskilda

Rättssäkerhetsaspekter utgör ett grundläggande fundament såväl när det gäller frågan om *att* kommunicera beslutsunderlag och beslut med enskilda parter som frågan om *hur* detta ska gå till. Vi diskuterar nu endast frågan om formen för sådan kommunikation, dvs. hur det ska gå till. Även när denna fråga belyses vill vi framhålla att rätten för en enskild part att bli informerad om hur ärendet handläggs och få möjlighet att påverka detta inte får inskränkas. De allmänna utgångspunkterna i 6 och 9 §§ förvaltningslagen står också fast. Det innebär bl.a. att myndigheten måste beakta tillgänglighetsaspekter, exempelvis om någon enskild till följd av en funktionsnedsättning har svårigheter att tillgodogöra sig muntlig eller skriftlig information.

Vi delar emellertid också den bedömning som såväl Digitaliseringskommissionen som Utredningen om effektiv styrning av nationella digitala tjänster har gjort om att pappersposten behöver fasas ut. Den problematik som beskrivits i bl.a. kapitel 8.3.1, dvs. att förvaltningen behåller sin pappershantering parallellt med att digitala kommunikationskanaler införs, gör sig gällande även i det nu aktuella avseendet. Enskilda kan i nuläget få del av meddelanden från förvaltningen på olika sätt, dels via post, dels digitalt. De dubbla förfarandena kan även gälla kommunikation från en och samma myndighet beroende på vilka ärendeprocesser som har digitaliserats respektive inte. Dubbla förfaranden i fråga om hur förvaltningen kommunicerar skriftliga underrättelser eller andra handlingar kan leda till rättsosäkerhet, särskilt om det saknas reglering som anger vilka principer som gäller. Parallella förfaranden är också kostsamma och förvaltningen kan göra besparingar om digital form i högre grad används vid förmedling av skriftliga underrättelser och andra handlingar.[56]

Vår bedömning är, i likhet med vad som anförts i kapitel 8.3.1, att digitala förfaranden överlag ger förbättrade möjligheter för enskilda att snabbt och enkelt få tillgång till information och beslut från

[55] Se SOU 2017:23 s. 183 f.. Se även SOU 2017:114 med förslag till lag om infrastruktur för digital post.
[56] Se även SOU 2017:23 s. 155 f. och 181 f.

förvaltningens sida. Generellt leder digitala förfaranden till kortare handläggningstider. Det skulle därför kunna invändas att digital kommunikation med beaktande av 6 och 9 §§ förvaltningslagen redan är utgångsläget, eftersom den digitala kommunikationsformen allmänt sett är enklast och ger det snabbaste förfarandet.

Fortfarande utgör emellertid flöden av papperspost från förvaltningen till enskilda ett normalt förfarande. En förklaring till att det förhåller sig på det sättet kan vara att de sätt för att förmedla information digitalt som ofta används har varit vanlig e-post, vilket inte utgör en tillräckligt säker kommunikationskanal för att t.ex. förmedla känsliga personuppgifter.[57] En annan förklaring kan vara att förvaltningen har bristande tillgång till information om hur enskilda kan nås digitalt. Trots att en myndighetsgemensam infrastruktur för säkra digitala försändelser,[58] Mina meddelanden, har tagits fram går det emellertid långsamt att öka graden av digitala försändelser från förvaltningen. Vi instämmer i tidigare gjorda bedömningar om att frivilligheten från myndigheters sida att avgöra formerna för meddelanden till enskilda är en bidragande orsak till detta.[59] Vår bedömning och vårt förslag innebär därför att det bör införas en reglering som anger att en myndighets skriftliga underrättelser eller andra meddelanden till enskilda som huvudregel ska förmedlas digitalt.

I förvaltningslagens bestämmelser om kommunikation av beslutsunderlag respektive underrättelse om innehållet i beslut anges att det är myndigheten som bestämmer hur underrättelse ska ske. Det är med andra ord enligt gällande rätt upp till myndigheten att bestämma vilket tillvägagångssätt som ska användas för att underrätta parten. Myndigheter bör enligt vår uppfattning fortfarande vara fria att, med beaktande av såväl förvaltningslagens reglering i 6 och 9 §§ som situationen i det enskilda fallet, avgöra om underrättelsen bör lämnas muntligen direkt till parten, t.ex. via telefonsamtal eller ett personligt besök, eller om underrättelsen bör lämnas skriftligen. Det är när myndigheten har valt skriftlig form för att lämna underrättelsen, eller när parten har begärt skriftlig form, som den

[57] Se t.ex. artikel 32 i dataskyddsförordningen om säkerhet i samband med behandling av personuppgifter.
[58] Med säker avses här att meddelandet sänds krypterat, med angiven avsändare och tas emot i en brevlåda som skyddas av kryptering, och att meddelandet enbart kan läsas av en mottagare som legitimerar sig. Se även SOU 2017:23 s. 153.
[59] Se bl.a. *Budgetpropositionen för 2017*, prop. 2016/17:1, utg. omr. 22, s. 110.

nya huvudregeln om digital kommunikation enligt vår bedömning bör aktualiseras. Som en följd av den reglering som vi föreslår bör därför ändringar göras i 25 § andra stycket första meningen och 33 tredje stycket första meningen i förvaltningslagen. Av den nya lydelsen bör det framgå att myndighetens möjlighet att bestämma formen för underrättelse innebär att myndigheten enligt dessa bestämmelser avgör om underrättelse ska lämnas muntligt eller skriftligt.

Närmare om innebörden av den föreslagna regleringen

Flera myndigheter har tagit fram digitala tjänster för enskilda, antingen inom ramen för en myndighets eget verksamhetsområde eller i myndighetssamverkan. En del tjänster medför att enskilda kan följa sitt ärendes handläggning genom t.ex. webbaserad inloggning till vad som ofta kallas Mina sidor hos myndigheten i fråga. Enligt vår bedömning är det inte möjligt att ge ett entydigt svar i frågan om vilka digitala förfaranden som krävs för att kommunikation av bl.a. skriftliga underrättelser till enskilda ska anses rättssäkra. Ärendetypen och partens intressen i det enskilda fallet behöver, som ovan framgått, beaktas. För att åstadkomma rättssäkra förfaranden i samband med t.ex. skriftlig underrättelse om beslut torde det emellertid enligt vår bedömning normalt krävas att myndigheten aktivt kommunicerar ut antingen underrättelsen eller information om var underrättelsen finns tillgänglig så att den enskilde enkelt och smidigt kan ta del av den. Det kan exempelvis göras genom ett meddelande med en länk eller någon annan form av notisfunktion som aktivt uppmärksammar den enskilde på förekomsten av och tillgängligheten till den handling som en underrättelse avser.[60] Den kommunikationen kan enligt vår bedömning vara digital samtidigt som rättssäkerheten garanteras, särskilt som vi nu föreslår en generell reglering som tydliggör att förvaltningen i första hand kommunicerar digitalt med enskilda.

När myndigheten saknar tillgång till information om digitala kontaktvägar som gör det möjligt att förmedla underrättelser eller andra meddelanden digitalt till den enskilde kan givetvis den formen för kommunikation inte användas. I linje med vad vi tidigare anfört

[60] Jfr JO:s beslut 2010/11:JO1 s. 501 (Dnr 6697-2009).

om behovet av styrning och stöd genom rättsregler ser vi inte att detta hindrar införandet av en ny huvudregel om digital kommunikation när handlingar översänds till enskilda. Den föreslagna utformningen av bestämmelsen hindrar inte heller en sådan tillämpning som innebär att huvudregeln frångås när det på grund av avsaknad av kontaktuppgifter inte finns förutsättningar att följa den. Vår uppfattning är dock, även om det inte legat inom ramen för vår utredning att närmare gå in i dessa infrastrukturella frågor, att digitala kontaktuppgifter till privatpersoner och företag i närtid som huvudregel bör bli obligatoriska. Det skulle exempelvis kunna vara fråga om att enskilda ska inneha en brevlåda för att kunna ta emot digital post från myndigheter om han eller hon inte uttryckligen har meddelat önskemål om att slippa ta emot skriftliga underrättelser eller andra handlingar från myndigheter i digital form.[61] Vårt förslag till ny huvudregel om digital kommunikation förhåller sig emellertid neutralt i förhållande till vilken teknik som används för den digitala kommunikationen.

När huvudregeln inte tillämpas

En huvudregel om digital kommunikation kan inte gälla undantagslöst. En generell regel av nu aktuellt slag bör vara subsidiär i förhållande till särskild reglering om formen för kommunikation. Det följer av 4 § förvaltningslagen att om en annan lag eller en förordning innehåller någon bestämmelse som avviker från denna lag, tillämpas den bestämmelsen. Den reglering som vi nu diskuterar kommer alltså inte att ha företräde framför t.ex. bestämmelser i registerförfattningar om elektroniskt utlämnande av uppgifter eller bestämmelser om sekretess. Det kan därmed fortfarande finnas annan reglering som uppställer hinder mot digital kommunikation.

En myndighet behöver vidare uppnå tillräcklig säkerhet för att digital kommunikation ska kunna krävas. Det bör mot den bakgrunden, i likhet med vad som anförts i kapitel 8.3.3 om en ny huvudregel om digital tillgänglighet, enligt vår bedömning framgå av regleringen att det av säkerhetsskäl eller av annat skäl kan vara olämpligt att förvaltningen kommunicerar digitalt med den enskilde.

[61] Jfr Utredningen om effektiv styrning av nationella digitala tjänsters bedömning i SOU 2017:23 s. 186 f.

I fråga om när det är olämpligt med digital kommunikation av andra skäl än säkerhetsskäl bör särskilt framhållas att den enskilde som utgångspunkt själv bör kunna meddela på vilket sätt han eller hon tar emot skriftliga underrättelser eller andra handlingar från förvaltningen, t.ex. att han eller hon inte önskar ta emot skriftliga underrättelser eller andra handlingar från myndigheter i digital form.[62] Det kan så småningom utvecklas nya system för att enskilda mer generellt ska kunna ge besked till förvaltningen om önskad form för kommunikation, i linje med vad som ovan anförts om brevlådor för att kunna ta emot digital post från myndigheter. Innan sådana lösningar finns på plats bör den enskildes önskemål i vart fall beaktas i det enskilda ärendet. En sådan önskan bör förvaltningen som regel följa i linje med den allmänna serviceskyldigheten. Myndigheten får då överväga att översända underrättelser eller andra handlingar per papperspost i stället om inte någon form av muntlig kommunikation bedöms lämpligare (se bl.a. 25 och 33 §§ förvaltningslagen).

Det bör överlåtas åt tillämpande myndigheter att avgöra när det annars kan vara olämpligt med digital kommunikation, t.ex. om det är något i det enskilda ärendet, något som framkommit i tidigare kontakter med den enskilde, eller för en viss typ av handlingar som gör att myndigheten bedömer det vara olämpligt med digital kommunikation.

Vi föreslår alltså sammanfattningsvis att en myndighets skriftliga underrättelser eller andra handlingar till enskilda ska förmedlas digitalt, om det inte är olämpligt av säkerhetsskäl eller av andra skäl, och att enskilda ska kunna meddela att de inte önskar ta emot skriftliga underrättelser eller andra handlingar från myndigheten i digital form.

Annan reglering

I ett nästa steg bör enligt vår uppfattning också särskilda överväganden göras om hur nya sätt för digital delgivning ska kunna utformas. Vi har emellertid inte haft möjlighet att inom ramen för denna utredning närmare analysera frågan. Den av oss föreslagna

[62] Jfr, i fråga om att beakta enskildas önskemål om form för kommunikation, t.ex. departementspromemorian *En snabbare lagföring Försöksprojekt med ett snabbförfarande i brottmål*, Ds 2017:36, s. 61 f.

regleringen kring enskildas självbestämmande i fråga om digital kommunikation vid underrättelser bör emellertid inte hindra fortsatta överväganden om hur nya sätt för delgivning kan utformas.

I förordningen (2003:234) om tiden för tillhandahållande av domar och beslut, m.m. finns bestämmelser om hur handlingar ska tillhandahållas. Förordningen innehåller bestämmelser för domstolar och statliga förvaltningsmyndigheter. Där anges bl.a. i 9 § att en handling som ska tillhandahållas bör skickas med post, om inte något annat har begärts. I 10 § anges att om det är lämpligt får en handling skickas med telefax eller elektronisk post eller på annat sätt tillhandahållas i elektronisk form.[63] Regeringen bör enligt vår bedömning överväga att anpassa regleringen i den förordningen efter det förslag som här lämnas, även om det anges att förordningen är subsidiär till annan författning.

8.3.7 En angränsande fråga om kommunikation

I kapitel 12 återkommer vi till några av de analyser vi gjort med anledning av kartläggningsresultatet, bl.a. i frågan om reglering avseende informationsförsörjning. Där görs bedömningen att det sannolikt kommer att finnas ett behov av att se över vissa registerförfattningar som t.ex. förutsätter att vissa myndigheter håller centrala register för att försörja förvaltningen och samhället i stort med viss information (se kapitel 12.2.4).

Om det i fortsatt lagstiftningsarbete blir aktuellt med reglering som anger att andra myndigheter ska hämta vissa uppgifter från en utpekad digital källa bör det också övervägas om det finns eller ska ges förutsättningar som innebär att dessa uppgifter inte alltid behöver kommuniceras med enskilda i varje enskilt ärende enligt 25 § förvaltningslagen. Det bör enligt vår bedömning kunna vara tillräckligt att enskilda har möjlighet att kontrollera uppgifterna och t.ex. begära rättelse av dem vid källan, med beaktande av att också dataskyddsregleringen uppställer krav på information till den enskilde.[64] Ett sådant förfarande kan underlätta förvaltningens effektivitet samtidigt som det besparar enskilda onödigt arbete med att ta

[63] Se även i fråga om denna förordning *Följdändringar till ny förvaltningslag,* Ds 2017:42, s. 235.
[64] Se t.ex. artikel 13.1.e och 13.2.e dataskyddsförordningen.

emot underrättelser och granska beslutsunderlag som är gemensamt för förvaltningen.

8.3.8 Placering och tillämpningsområde

Utredningens förslag: De föreslagna bestämmelserna som rör digital kommunikation ska placeras i förvaltningslagen och följa den lagens struktur och tillämpningsområde.

Skälen för utredningens förslag: Den för förvaltningen gemensamma regleringen om tillgänglighet och kommunikation med enskilda finns i förvaltningslagen. Vi har övervägt om det borde skapas en särskild lag som bl.a. reglerar den digitala tillgänglighet och de digitala förfaranden som diskuterats i detta kapitel. Vi har dock stannat vid att regler om förvaltningens tillgänglighet och förfaranden bör hållas samlade. Det gäller särskilt med beaktande av att förvaltningens verksamhet i hög grad redan är digital och i ökad utsträckning förväntas bli det, bl.a. till följd av de av oss lämnade förslagen. Vi föreslår därför att bestämmelserna införs i förvaltningslagen.

Bestämmelser om förvaltningens tillgänglighet hör till grunderna för en god förvaltning. Vi finner inte anledning att se annorlunda på den nu föreslagna regleringen med en ny huvudregel om digital tillgänglighet. Även bestämmelsen med huvudregel om digital kommunikation till enskilda bör enligt vår bedömning ges ett så omfattande tillämpningsområde som möjligt. Vi föreslår därför att dessa bestämmelser införs i förvaltningslagens inledande avsnitt.

Den föreslagna anpassningen i regleringen om ankomstdag liksom huvudregeln om underrättelser när handlingar tas emot digitalt bör enligt vår bedömning endast gälla vid ärendehandläggning. Vi föreslår därför att de bestämmelserna ska tillföras förvaltningslagens allmänna krav på handläggningen av ärenden.

Av den föreslagna placeringen i förvaltningslagen följer att samma avgränsningar i förhållande till bl.a. tillämpningsområdet för kommunala ärenden där besluten kan laglighetsprövas, brottsbekämpande verksamhet, hälso- och sjukvårdsverksamhet och privat utförande av offentligt finansierad verksamhet kommer att gälla som för förvaltningslagens tillämpningsområde i övrigt.

8.3.9 Konsekvenser av förslagen

På en övergripande nivå bedömer vi att förslagen som rör digital kommunikation med enskilda ger en stabil rättslig bas för att förvaltningen ska kunna ta ytterligare steg i utvecklingen att lämna god digital service till privatpersoner och företag, samtidigt som grundlagsfästa krav på likabehandling upprätthålls. Såväl privatpersoners som företagskontakter med förvaltningen blir smidigare och enklare. Ett grundläggande syfte med förslagen är att stärka rättssäkerheten avseende de digitala förfaranden som tas fram i förvaltningen. Förslagen bidrar också till att öka incitamenten för att enskilda ska använda de digitala tjänster som förvaltningen tar fram.

Förvaltningen förväntas även i intern bemärkelse bli mer effektiv genom att i högre grad kunna övergå till enklare och mer effektiv digital kommunikation där myndighetspersonal inte behöver lägga ned tid på att hantera manuella pappers- och postförfaranden. Förutom denna resursbesparing minskar de direkta kostnaderna för att hantera utskick av papperspost. Någon beräkning i fråga om graden av kostnadseffektivitet som just de nu lämnade förslagen kommer att medföra för förvaltningen kan emellertid svårligen göras med anledning av dels redan pågående digitaliseringsarbeten, dels att även andra förslag som rör förvaltningens digitala kommunikation med enskilda och infrastrukturlösningar för detta nu bereds (se SOU 2017:23 och 2017:114). En minskning av mängden papperspost från förvaltningen leder dessutom till minskad miljöpåverkan.

Såväl förvaltningsmyndigheter och domstolar som kommuner och landsting åläggs enligt förslagen en skyldighet att som huvudregel tillhandahålla digitala mottagningsfunktioner för att ta emot handlingar och att i första hand kommunicera digitalt med enskilda. Så som förslagen har utformats innebär de dock inte en ovillkorlig skyldighet att senast ett visst datum t.ex. tillhandahålla digitala tjänster för att inleda ärenden vid myndigheten. En avvägning har också gjorts så att intresset av säkra förfaranden ska beaktas.

Även med hänsyn tagen till överväganden om kostnadseffektivitet går det i praktiken inte att sätta ett visst datum för när varje myndighet ska tillhandahålla en sådan digital mottagningsfunktion. Förslagen förväntas därför inte nu leda till några direkta kostnader för myndigheternas utvecklingsarbeten. Intresset av att inte tillämpa huvudregeln av kostnadsskäl behöver dock sättas i relation till

enskildas intressen av digital tillgänglighet till myndigheten. Vi menar vidare att det föreslagna kravet kommer att leda till att framtagandet av digitala tjänster för service till privatpersoner och företag i högre utsträckning kommer att prioriteras. Någon omarbetning av de digitala tjänster som redan har tagits fram torde inte krävas, varför förslagen därmed inte heller medför några särskilda kostnader i det avseendet.

Förslagen har bäring även på kommuner och landsting. Vi menar att utvecklingen i fråga om vilken service som i förvaltningsrättslig mening kan krävas av myndigheter, även kommunala och landstingskommunala, följer nu gällande ordning. De förslag vi lämnar för därmed inte med sig någon ny konsekvens för den kommunala självstyrelsen. Med anledning av att förslagen i sig inte väntas leda till direkta kostnader, omfattas de inte heller av den kommunala finansieringsprincipen.

Förslagen skapar goda förutsättningar för att åstadkomma infrastrukturlösningar med t.ex. en gemensam plattform för olika myndigheters digitala tjänster.

Den föreslagna regleringen bör enligt vår bedömning föranleda informationsinsatser för att sprida kunskap om bestämmelserna till enskilda. En sådan informationsinsats bör kunna samordnas med t.ex. informationsinsatser som görs för att sprida kännedom om infrastrukturen för digital post. Erfarenheter kan också hämtas från t.ex. den danska övergången till obligatorisk digital post.[65] Vi bedömer att det även ur rättssäkerhetssynpunkt är en fördel att en sådan informationsinsats samordnas för förvaltningen som helhet, för att öka medvetenheten hos enskilda om att digital kommunikation från förvaltningen blir huvudregeln. De begränsade kostnader som en sådan informationsinsats medför, särskilt om de samordnas med informationsinsatser av infrastrukturansvarig myndighet[66] kan finansieras inom den myndighetens ordinarie anslag.

Förslagen kan härutöver inte förväntas leda till andra konsekvenser än de generella konsekvenser av våra förslag som redovisas i kapitel 14.2.

[65] SOU 2017:23 s. 169.
[66] A.a. s. 266.

8.4 Digitala tjänster med eget utrymme

8.4.1 Användarvänliga digitala tjänster

I syfte att erbjuda en god service och att uppnå politiska målsättningar om en enklare vardag för privatpersoner och företag har det kommit att bli allt vanligare att myndigheter som tillhandahåller digitala tjänster ger användaren möjlighet att, inom ramen för vad som brukar kallas ett eget utrymme, t.ex. skapa utkast för senare inlämning av uppgifter till myndigheten. Denna möjlighet kan vara en avgörande förutsättning för att tjänsterna alls ska kunna användas, särskilt i de fall där t.ex. ett stort antal uppgifter ska lämnas in och användaren har behov av att tillfälligt lagra uppgifter i tjänsten utan att uppgifterna anses ha kommit in till myndigheten enligt tryckfrihetsförordningen eller förvaltningslagen.

Utmärkande för den typ av digitala tjänster det här är fråga om är således att de innehåller ett så kallat eget utrymme där användaren exempelvis kan registrera och lagra uppgifter utan att myndigheten som tillhandahåller det egna utrymmet har insyn i eller tar del av uppgifterna i fråga. Ett ytterligare kännetecken för denna typ av tjänster är att den myndighet som tillhandahåller det egna utrymmet enbart tekniskt bearbetar eller tekniskt lagrar uppgifterna för annans räkning fram till dess användaren aktivt förmedlat uppgifterna i fråga till myndigheten.

Även om begreppet eget utrymme kan anses relativt etablerat i förvaltningsrättsliga sammanhang bör det framhållas att begreppet inte tillkommit enbart utifrån tekniska aspekter, utan snarare som en rättsfigur.[67] Förvaltningens digitala utveckling har nämligen förutsatt att myndigheterna svarat upp mot de förväntningar som privatpersoner och företag har på att handlingar inte blir att anse som inkomna till myndigheten i ett för tidigt skede, dvs. innan avsikten varit att ge in dem till myndigheten.

[67] Se t.ex. användningen av begreppet i *Utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring*, prop. 2016/17:198.

8.4.2 Kartläggningsresultatet

En myndighet som utvecklar en digital tjänst med eget utrymme konfronteras med en rad juridiska frågeställningar. Eftersom de juridiska bedömningarna många gånger är avhängiga av tjänstens tekniska utformning kan frågorna vara svårgripbara för jurister som saknar djupare kunskap om tekniska funktioner.

Vårt kartläggningsarbete har å ena sidan visat att vissa aktörer känner sig trygga med den myndighetspraxis som har utvecklats när det gäller utformning av tjänster med eget utrymme. Att en sådan myndighetspraxis har kunnat utvecklas, och digitala tjänster har kunnat införas, beror till stor del på de vägledningar som har tagits fram inom ramen för E-delegationen och eSamverkansprogrammet (eSam).[68] Å andra sidan har flera av dem vi mött under kartläggningen framhållit att de anser att det fortfarande råder en rättslig osäkerhet inom området. Det rör sig om osäkerhet beträffande tolkning och tillämpning av 2 kap. 10 § första stycket tryckfrihetsförordningen. Hur ska tjänster utformas rent faktiskt för att omfattas av lokutionen ”endast som led i teknisk bearbetning eller teknisk lagring för annans räkning”? Vilken service kan en myndighet ge inom ramen för ett eget utrymme utan att en handling ska anses inkommen? Under vilka förutsättningar behövs uttalat författningsstöd för behandlingen av uppgifter i ett eget utrymme? Dessa frågeställningar har också samband med funderingar kring hur dataskyddsregleringens krav på rättslig grund för personuppgiftsbehandling ska förstås beträffande egna utrymmen och hur personuppgiftsansvaret, för den behandling av personuppgifter som sker i det egna utrymmet, ska fördelas. Även frågor om vem som har ansvar för informationssäkerheten har relevans i sammanhanget.

Kartläggningsresultatet ger också anledning för oss att förutse ett växande användningsområde för digitala tjänster med eget utrymme. Det gäller inte enbart ökat tillhandahållande av sådana tjänster för enskilda. En myndighet kan också tillhandahålla ett eget utrymme åt en annan myndighet inom ramen för en gemensam digital process (se kapitel 5.2.4). Myndighetsgemensamma processer kan med andra ord förenklas och effektiviseras genom att en myndighet tillhandahåller ett eget utrymme åt en annan myndighet. Även här

[68] Se bl.a. *Juridisk vägledning för verksamhetsutveckling inom e-förvaltningen*, version 2.0, E-delegationen, 19 mars 2015 och *Eget utrymme hos myndighet - en vägledning*, eSam, april 2016.

framhåller myndigheter behov av att få stöd i sitt digitala utvecklingsarbete så att de tjänster som utformas är förenliga med gällande rätt.

Majoriteten av dem som uttalat sig i frågan under kartläggningen är förvisso överens om att de vägledningar som finns inom området är välgrundade och har stor praktisk betydelse för deras utvecklingsarbeten. Men ett antal myndighetsrepresentanter framhåller som en brist att de vägledningar som finns saknar en naturlig plats i normhierarkin. Det har bl.a. framförts att, om inte författningsändringar genomförs, skulle en ordning där lagstiftaren eller regeringen pekar ut den aktör som ska stå för stödmaterial och vägledning ge en ökad rättslig stabilitet.

I följande avsnitt redogör vi för den rättsliga regleringen och de anknytande frågeställningar som aktualiseras vid utveckling av digitala tjänster med eget utrymme. Därefter följer våra huvudsakliga överväganden och förslag.

8.4.3 Gällande rätt och några inledande överväganden

Legalitetsprincipen

Legalitetsprincipen brukar, som också angetts i kapitel 4, framhållas som ett skydd mot en nyckfull och godtycklig maktutövning från det allmännas sida. Den är en av de principer som anses kännetecknа en rättsstat och tillmäts en avgörande vikt i EU:s rättssystem liksom i Europakonventionen. Legalitetsprincipen är inte enhetligt definierad men brukar vanligtvis uppfattas som ett krav på att ingripanden mot enskilda ska ha ett klart författningsstöd. I denna betydelse är legalitetsprincipen också grundlagsfäst genom bestämmelsen i 1 kap. 1 § regeringsformen om att ”den offentliga makten utövas under lagarna”. Med uttrycket lagarna avses i detta sammanhang inte endast sådana föreskrifter som riksdagen har beslutat utan även andra författningar och sedvanerätt.[69] Legalitetsprincipen innebär alltså att myndigheternas maktutövning i vidsträckt mening måste ha stöd i någon av de källor som tillsammans bildar rättsordningen.

Inom förvaltningsrätten är legalitetsprincipen av central betydelse eftersom kravet på författningsstöd bildar utgångspunkt för myndigheternas verksamhet såväl när det gäller att handlägga ärenden

[69] Prop. 2016/17:180 s. 57.

och besluta i dessa, som i fråga om annan verksamhet som en myndighet bedriver. Regeringen har också anfört att pågående utveckling där myndigheters verksamhet går från en mer klassisk förvaltning mot en förvaltning med ökade inslag av informationsuppgifter och mera kundrelaterade aktiviteter, t.ex. i form av olika digitala självbetjäningstjänster, innebär ökade risker för att myndigheter inte alltid i tillräcklig utsträckning tar reda på om de har stöd i rättsordningen för sina åtgärder.[70]

I syfte att bl.a. markera myndigheternas skyldighet att fullgöra bestämda uppgifter i det allmännas tjänst och hindra myndigheterna från att agera vid sidan av sina i författning angivna åligganden, har i den nya förvaltningslagen förts in en bestämmelse om att en myndighet endast får vidta åtgärder som har stöd i rättsordningen.[71] Den nya bestämmelsen innebär ett krav på att myndighetens agerade ska ha stöd i någon av de källor som tillsammans bildar rättsordningen i vidsträckt mening. Vad som krävs är alltså att det ska finnas någon normmässig förankring för all typ av verksamhet som en myndighet bedriver.[72] Legalitetsprincipen gäller alltså såväl vid myndigheters handläggning och beslut i ärenden som vid s.k. faktiskt handlande.

I den nya förvaltningslagen införs också en bestämmelse om att en myndighet inom sitt verksamhetsområde ska samverka med andra myndigheter.[73] En myndighet ska därtill i rimlig utsträckning hjälpa den enskilde genom att själv inhämta upplysningar eller yttranden från andra myndigheter. Enligt regeringens uttalanden i propositionen till ny förvaltningslag har bestämmelsen två syften.[74] För det första är det fråga om en mer generell skyldighet för myndigheter att samverka med varandra. Myndigheternas verksamhet styrs enligt legalitetsprincipen av de föreskrifter om arbetsuppgifter som lagstiftaren eller någon annan normgivare har meddelat. Det innebär bl.a. att det inte får förekomma några nyskapelser i form av särskilda samarbetsorgan, som oberoende av tillämpliga föreskrifter fattar beslut som inte kan härledas till någon av de samverkande myndigheterna. För det andra avser bestämmelsen att ge en klar indikation om att samverkansskyldigheten inte enbart tar sikte på att

[70] A. prop. s. 58.
[71] 5 § första stycket förvaltningslagen.
[72] Prop. 2016/17:180 s. 59.
[73] 8 § förvaltningslagen.
[74] Prop. 2016/17:180 s. 71.

förvaltningen generellt ska bli så enhetlig eller effektiv som möjligt, utan också är avsedd att underlätta för den enskilde i kontakterna med myndigheterna. Bestämmelsen ger dock inte stöd för verksamhetsprojekt som faller utanför respektive myndighets verksamhetsområde.[75]

För de flesta myndighetsgemensamma utvecklingsarbeten som t.ex. innefattar utveckling av en digital tjänst med eget utrymme finns normalt sett någon form av rättsligt stöd för arbetet, antingen i de författningar som gäller myndigheternas verksamhet, i särskilda regeringsbeslut eller i berörda myndigheters regleringsbrev. I vårt kartläggningsarbete har emellertid framkommit att det inte alltid är helt tydligt vad som utgör ramen för den verksamhet en myndighet ska ägna sig åt. Det gäller i synnerhet var gränserna går mot andra aktörer.

Tryckfrihetsförordningen och offentlighetsprincipen

Enligt tryckfrihetsförordningen ska varje svensk medborgare ha rätt att ta del av allmänna handlingar.[76] En handling är allmän om den förvaras hos en myndighet och är att anse som inkommen till eller upprättad hos myndigheten.[77] En elektronisk handling i form av en upptagning anses inkommen till myndigheten när annan gjort upptagningen tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas.[78] En handling som förvaras hos en myndighet endast som led i teknisk bearbetning eller teknisk lagring för annans räkning anses emellertid inte vara någon allmän handling enligt 2 kap. 10 § första stycket tryckfrihetsförordningen. En sådan handling omfattas således inte av bestämmelserna om handlingsoffentlighet och kan inte bli föremål för utlämnande.

Stöd i förarbetsuttalanden för att 2 kap. 10 § första stycket tryckfrihetsförordningen kan tillämpas när myndigheter tillhandahåller digitala tjänster med ett eget utrymme finns numera i två separata

[75] A. prop. s. 293.
[76] 2 kap. 1 § tryckfrihetsförordningen. Observera att ändringar i bl.a. 2 kap. tryckfrihetsförordningen föreslås i *Ändrade mediegrundlagar*, prop. 2017/18:49. Ändringarna innebär bl.a. ändrade beteckningar på lagrum.
[77] 2 kap. 3 § tryckfrihetsförordningen.
[78] 2 kap. 6 § tryckfrihetsförordningen.

lagstiftningsärenden. I anslutning till en redogörelse om huruvida en handling som fylls i av en enskild i ett eget utrymme ska anses som inkommen i förvaltningsrättslig mening framför regeringen följande i propositionen med förslag till en ny förvaltningslag.[79]

> Under förutsättning att uppgifterna på servern inte görs tillgängliga för myndighetens handläggare före nämnda tidpunkt, torde det också vara möjligt att se en eventuell lagring som föregår ingivandet som en form av teknisk lagring för den enskildes räkning, som enligt 2 kap. 10 § första stycket TF innebär att handlingen inte är att anse som allmän innan den ”skickats in” (jfr HFD 2011 ref. 52). Detta bör myndigheterna ha i åtanke vid utformningen av de tekniska systemen och vid behörighetstilldelningen i dessa.

I propositionen *Utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring* har regeringen uttalat att det finns stöd i praxis för att myndigheterna tillhandahåller digitala tjänster som uppfyller kraven i 2 kap. 10 § första stycket tryckfrihetsförordningen.[80] Som exempel på egna utrymmen i befintliga digitala tjänster inom förvaltningen kan nämnas Skatteverkets blankettjänst för deklaration, Arbetsförmedlingens CV-databas och tjänster för lagring av affärsmodeller som tillhandahålls av bl.a. Tillväxtverket. Digitala tjänster för enskilda kan dock utformas på många olika sätt. Det innebär enligt regeringen i nämnda proposition att det ytterst är en fråga för rättstillämpningen att avgöra om information i egna utrymmen omfattas av regleringen i 2 kap. 10 § första stycket tryckfrihetsförordningen och därmed inte utgör allmänna handlingar.

Tillämpningen av undantagsbestämmelsen i 2 kap. 10 § första stycket tryckfrihetsförordningen har bl.a. prövats i ett mål om utlämnande av uppgifter ur Riksrevisionsverkets centrala ekonomisystem Cosmos.[81] Bakgrunden till rättsfallet var att flera andra myndigheter hade valt att lagra sina ekonomidata i detta system, som tekniskt förvaltades av en extern it-leverantör. Riksrevisionsverket disponerade inte över innehållet i de andra myndigheternas redovisning, utan tillhandahöll endast den tekniska lösningen och lagringsutrymmet. Regeringsrätten[82] bedömde i det aktuella fallet, med hänvisning till 2 kap. 10 § första stycket tryckfrihetsförordningen, att handlingarna hos Riksrevisionsverket som innehöll de begärda

[79] Prop. 2016/17:180 s. 141 f.
[80] Prop. 2016/17:198 s. 16.
[81] RÅ1994 ref. 64.
[82] Den 1 januari 2011 bytte Regeringsrätten namn till Högsta förvaltningsdomstolen.

uppgifterna inte var att anse som allmänna handlingar hos myndigheten.

I ett annat rättsfall prövade Högsta förvaltningsdomstolen om ett webbaserat arbetsskadesystem omfattades av den aktuella bestämmelsen.[83] Systemet var gemensamt för polismyndigheterna och administrerades av Rikspolisstyrelsen. Vissa befattningshavare vid Rikspolisstyrelsen kunde ta del av handlingarna i systemet för att bl.a. utarbeta statistik och lämna rapporter till Arbetsmiljöverket. Domstolen ansåg att i vart fall den användningen av uppgifterna inte kunde anses hänförlig till sådan teknisk bearbetning eller teknisk lagring som avses i 2 kap. 10 § första stycket tryckfrihetsförordningen.

I rättspraxis saknas det vägledande avgöranden som ger ett tydligt besked om vilka egna utrymmen i digitala tjänster som myndigheter tillhandahåller som kan falla in under 2 kap. 10 § första stycket tryckfrihetsförordningen, och som därmed inte leder till att allmänna handlingar anses inkomna. Kammarrätten har dock i ett mål bedömt att handlingar som förvaras i en CV-databas hos Arbetsförmedlingen fick anses vara förvarade hos myndigheten endast som led i teknisk bearbetning eller teknisk lagring för annans räkning.[84] CV-databasen bestod av konton för arbetssökande och arbetsgivare. De arbetssökande kunde lagra CV och annan information i ett eget utrymme och arbetsgivare kunde söka bland profilerna, läsa dem och skicka förfrågningar.

Service i eget utrymme

I takt med att enskilda i allt högre grad använder digitala tjänster i kontakterna med förvaltningen ställs högre krav på myndigheterna att i enlighet med den allmänna serviceskyldigheten också erbjuda stöd och hjälp till företag och privatpersoner för att de ska kunna använda tjänsterna på ett effektivt sätt. Sådant stöd kan lämnas på olika sätt. Exempelvis kan stödet vara helt automatiserat genom summering av belopp eller automatiserade svar på vissa frågor. Sådan automatiserad service kan ges helt utan mänsklig inblandning vilket enligt vår bedömning bör innebära att myndighetens hantering av

[83] HFD 2011 ref. 52.
[84] Kammarrätten i Stockholms dom den 26 oktober 2015, mål nr 7369-15.

uppgifterna utgör teknisk bearbetning eller teknisk lagring för användarens räkning.

I kartläggningen har emellertid framkommit att användaren av en digital tjänst också kan ha behov av ett mer anpassat stöd. Sådant stöd kan ges genom att myndigheten erbjuder hjälptjänster,[85] t.ex. i form av chatt eller telefonsamtal med myndighetens personal. En företeelse som blir allt vanligare är att den enskilde genom s.k. skärmdelning delar de uppgifter som finns på hans eller hennes bildskärm med personal anställd vid myndigheten. När myndigheten i en hjälptjänst lämnar stöd till en enskild genom skärmdelning eller chatt kan handlingar bli allmänna hos myndigheten. Sådana handlingar förvaras inte endast för enbart teknisk bearbetning eller teknisk lagring, (2 kap. 10 § första stycket tryckfrihetsförordningen) utan är i regel att anse som till myndigheten inkomna handlingar. Allmänna handlingar kan andra begära att få utlämnade. Men uppgifter som tillgängliggörs för myndighetens befattningshavare i samband med en hjälptjänst torde normalt endast vara av betydelse för myndighetens verksamhet under tiden som samtalet eller sessionen pågår och bör därefter oftast kunna gallras.[86]

En annan typ av service som kan tillhandahållas inom ramen för ett eget utrymme är sammanställning och presentation av uppgifter eller handlingar som har hämtats in från flera olika aktörer, en s.k. presentationstjänst.[87] Syftet med en sådan tjänst är att den enskilde på ett enkelt sätt ska kunna ta del av samlad information på ett ställe, i stället för att behöva vända sig till flera olika aktörer. Handlingar som uppstår i samband med tillhandahållandet av en presentationstjänst kan inte alltid anses förvarade endast som ett led i teknisk bearbetning eller teknisk lagring för annans räkning. Uppgifterna som samlas in och sammanställs i en presentationstjänst kan därför utgöra del av allmänna handlingar. Presentationstjänster bör dock ofta kunna utformas så att myndighetens hantering av uppgifterna sker i form teknisk bearbetning eller lagring för användarens räkning.

[85] Om begreppsanvändningen se prop. 2016/17:198 och E-delegationens betänkande *Så enkelt som möjligt för så många som möjligt, Bättre juridiska förutsättningar för samverkan och service* (SOU 2014:39).
[86] Prop. 2016/17:198 s. 24.
[87] Om begreppsanvändningen se a. prop. och SOU 2014:39.

Även när allmänna handlingar upprättas hos en myndighet i samband med tillhandahållandet av en presentationstjänst torde de kunna gallras efter att tjänsten tillhandahållits.[88]

Förvaltningslagen och inkommen handling

Uppgifter som den enskilde lämnar i en digital tjänst för ansökan eller anmälan via webben finns normalt sett tekniskt tillgängliga för myndigheten på dess server redan innan den tidpunkt då den enskilde har färdigställt sitt formulär. När det gäller frågan om när en handling i förvaltningsrättslig mening ska anses vara inkommen till en myndighet har regeringen i propositionen med förslag till en ny förvaltningslag framfört följande.[89]

> Uppgifter som den enskilde lämnar i ett webbformulär finns i vissa fall tekniskt tillgängliga för myndigheten på dess server för databehandling redan innan den tidpunkt då den enskilde har färdigställt en ansökan. Så kan fallet vara t.ex. under den tid som ett webbformulär håller på att fyllas i fram till dess att den enskilde vidtagit en särskild åtgärd som markerar att ansökan är färdig och inskickad. Enligt regeringens mening bör ett sådant förhållande som regel inte anses innebära att handlingen i förvaltningsrättslig mening ska anses ha kommit in till myndigheten. Ingivandet kan exempelvis manifesteras genom att den enskilde trycker på en skicka-knapp i webbformuläret.

I kapitel 8.3.3–8.3.5 lämnar vi förslag på en uttrycklig reglering avseende digitala mottagningsfunktioner. Genom förslagen tydliggörs ytterligare, även i förhållande till enskilda, vad som gäller i fråga om bl.a. ankomstdag och underrättelse om att en handling har kommit in till en myndighet i förvaltningsrättslig mening.

Sekretesskydd vid teknisk bearbetning och lagring

I offentlighets- och sekretesslagen har införts bestämmelser som syftar till att säkerställa skyddet för uppgifter om enskildas personliga eller ekonomiska förhållanden, liksom skyddet för allmänna intressen, vid t.ex. användning av digitala tjänster. Regleringen, som redogörs för närmare nedan, kan bli aktuell både för eget utrymme

[88] A. prop. s. 26.
[89] Prop. 2016/17:180 s. 141.

som tillhandahålls en enskild och för eget utrymme som tillhandahålls en annan myndighet.

Enligt 40 kap. 5 § offentlighets- och sekretesslagen gäller sekretess i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning för uppgift om en enskilds personliga eller ekonomiska förhållanden. Bestämmelsen innebär att tystnadsplikt ska gälla för uppgifter om enskilds personliga eller ekonomiska förhållanden i verksamhet av det aktuella slaget. Om myndigheternas personal får del av en uppgift i denna verksamhet, t.ex. i samband med att han eller hon rättat ett fel i det tekniska systemet, eller vidtagit en åtgärd som är nödvändig från informationssäkerhetssynpunkt, skyddas uppgiften av sekretess. Tillämpningsområdet är detsamma som för det undantag från bestämmelserna om allmänna handlingar som föreskrivs i 2 kap. 10 § första stycket tryckfrihetsförordningen. Sekretessbestämmelsen kommer därför enbart att tillämpas på de digitala tjänster som har utformats på ett sådant sätt att de avser förvaring av handlingar endast som led i teknisk bearbetning eller lagring för annans räkning.[90]

Offentlighets- och sekretesslagen innehåller dessutom en bestämmelse, 11 kap. 4 a §, som reglerar att när en myndighet i sin verksamhet för enbart teknisk bearbetning eller teknisk lagring för en annan myndighets räkning får en uppgift som hos den senare myndigheten är sekretessreglerad av hänsyn till ett allmänt intresse, ska sekretessbestämmelsen även tillämpas hos den mottagande myndigheten. Det skydd som kan aktualiseras är även här en tystnadsplikt som t.ex. gäller i samband med digitala tjänster som en myndighet tillhandahåller åt en annan myndighet. Bestämmelsen är också tillämplig på uppgifter som den mottagande myndigheten får från enskilda eller andra myndigheter än beställarmyndigheten för den senare myndighetens räkning. Tillämpningsområdet för denna bestämmelse är också detsamma som för det undantag från bestämmelserna om allmänna handlingar som föreskrivs i 2 kap. 10 § första stycket tryckfrihetsförordningen.[91]

[90] Prop. 2016/17:198 s. 28 f.
[91] A. prop. s. 28.

8.4.4 Personuppgiftsansvar m.m.

Dataskyddsregleringen

En utgångspunkt vid behandling av personuppgifter i digitala tjänster med eget utrymme är givetvis att den personuppgiftsansvarige har att efterleva samtliga tillämpliga bestämmelser i dataskyddsregleringen för att behandlingen i fråga ska vara tillåten. En övergripande beskrivning av dataskyddsregleringen har lämnats i kapitel 4.5. Där har bl.a. de grundläggande principerna om dataskydd presenterats. I kapitel 7.6.1 har också bl.a. de generella reglerna i dataskyddsförordningen presenterats. I det följande lägger vi främst fokus på de bestämmelser som reglerar personuppgiftsansvaret eftersom det har visat sig att detta kan vara en utmanande uppgift vid utvecklande av tjänster med ett eget utrymme. Avslutningsvis berör vi också kortfattat den rättsliga grunden för personuppgiftsbehandlingen.

Fördelning av personuppgiftsansvar

Inledning

I takt med att utvecklingen av nya digitala tjänster med eget utrymme ökar har frågan om fördelning av personuppgiftsansvar vid flera tillfällen ställts på sin spets. Så har t.ex. skett i samband med Skatteverkets förmedlingstjänst Mina meddelanden och eHälsomyndighetens personliga hälsokonto Hälsa för mig.[92] Svårigheterna med att göra en rättsligt korrekt bedömning av personuppgiftsansvaret i en myndighetsgemensam tjänst med eget utrymme ska inte underskattas. I vårt kartläggningsarbete har det framhållits att det saknas lämpliga verktyg som kan underlätta en bedömning av fördelning av personuppgiftsansvar. Detta leder inte sällan till att myndigheterna får lägga ned oproportionerligt mycket tid på att utreda fördelningen av personuppgiftsansvar men att en rättslig osäkerhet trots denna arbetsinsats ändå ofta kvarstår.

Vår ambition i detta avsnitt är inte att presentera en fullständig rättslig utredning av personuppgiftsansvar i digitala tjänster med eget utrymme. Vår ambition är snarare att beskriva och belysa den problematik som finns inom området och redogöra för främst den

[92] Se bl.a. SOU 2017:114 kap. 21.8 om fördelning av personuppgiftsansvaret i Mina meddelanden och Förvaltningsrätten i Stockholms mål 11458-17 om personuppgiftsansvaret i Hälsa för mig.

generella reglering som styr bedömningen av personuppgiftsansvar. Det bör dock framhållas att redogörelsen inte är begränsad till frågan om personuppgiftsansvar i rättsfiguren eget utrymme utan avser personuppgiftsansvaret i hela dess vidd i digitala tjänster som innehåller ett eget utrymme.

Problembeskrivning

En digital tjänst som innefattar ett eget utrymme kan utformas på många olika sätt och vända sig till olika målgrupper, t.ex. privatpersoner eller företag. Tjänsten kan tillhandahållas av en enskild myndighet eller av flera myndigheter gemensamt. Exempelvis kan en myndighet ansvara för att leverera den tekniska infrastrukturen dvs. gränssnittet för tjänsten och det egna utrymmet. En annan myndighet, eller en privat aktör, kan ha åtagit sig att skicka uppgifter till det egna utrymmet på den enskildes begäran när denne använder utrymmet.

Som tidigare beskrivits är syftet med det egna utrymmet att enskilda ska kunna upprätta utkast, lagra uppgifter m.m. utan att de uppgifter som den enskilde hanterar blir att anse som allmänna handlingar hos myndigheten enligt tryckfrihetsförordningen eller inkomna till myndigheten enligt förvaltningslagen. En förutsättning för att uppgifterna som hanteras i ett eget utrymme inte ska bli allmänna handlingar eller anses inkomna, är att myndigheten som tillhandahåller det egna utrymmet hanterar den enskildes uppgifter endast som ett led i teknisk bearbetning eller teknisk lagring innan denne aktivt har valt att skicka in en handling till myndigheten i fråga. Det innebär i praktiken att myndigheten inte ska ta del av de uppgifter som en enskild behandlar i ett eget utrymme.

När det gäller myndighetsgemensamma digitala tjänster med eget utrymme behöver det fastställas dels hur personuppgiftsansvaret är fördelat mellan de parter som på olika sätt svarar för att tillhandahålla den tekniska plattformen eller delfunktioner i tjänsten, dels vem eller vilka som är personuppgiftsansvariga för den behandling av personuppgifter som äger rum i det egna utrymmet.

Bedömningen av i vilken omfattning en myndighet är personuppgiftsansvarig för behandlingen av personuppgifter i en digital tjänst med eget utrymme kan vara komplicerad ur flera olika perspektiv.

För det första kan man fråga sig vilka faktiska och praktiska möjligheter en myndighet har att utöva sitt personsuppgiftsansvar

för den del av personuppgiftsbehandlingen som äger rum i ett eget utrymme på initiativ av en privatperson och där utgångspunkten är att myndigheten inte ska eller får ta del av de uppgifter som behandlas (se avsnittet nedan om privatundantaget). Hur kan myndigheten t.ex. säkerställa att privatpersonen, vid användning av det egna utrymmet, bara för in uppgifter som är adekvata och relevanta och inte för omfattande i förhållande till de ändamål för vilka uppgifterna ska behandlas?[93]

För det andra finns det anledning att reflektera över om en näringsidkare, som inte omfattas av privatundantaget,[94] kan åläggas personuppgiftsansvar för den personuppgiftsbehandling som näringsidkaren utför i ett eget utrymme (se avsnittet nedan om juridiska personer). Hur kan en näringsidkare som bedöms vara personuppgiftsansvarig i så fall säkerställa att nödvändiga säkerhetsåtgärder vidtas för att skydda personuppgifterna som behandlas?

När det gäller digitala tjänster som t.ex. tillhandahålls gemensamt av flera myndigheter och privata aktörer behöver man för det tredje, med en tillräckligt hög grad av exakthet, fastställa hur personuppgiftsansvaret fördelar sig mellan de inblandade parterna. Hur personuppgiftsansvaret är fördelat när personuppgifter behandlas i komplexa digitala miljöer kan emellertid vara svårt att avgöra.

Regleringen av personuppgiftsansvar

Personuppgiftsansvaret regleras generellt i dataskyddsförordningen och specifikt i olika registerförfattningar. Av dataskyddsförordningens definition framgår att personuppgiftsansvarig är den som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.[95]

Den som är personuppgiftsansvarig bär ansvaret för att den behandling av personuppgifter, som ansvaret omfattar, är tillåten enligt dataskyddsregleringen dvs. att personuppgifterna behandlas för ett berättigat ändamål, att det finns en laglig grund för behandlingen, att den registrerades intressen tillvaratas etc.[96] Den som är

[93] Artikel 5.1 c dataskyddsförordningen, principen om uppgiftsminimering.
[94] Med ”privatundantaget” avses att behandling av personuppgifter som en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll inte omfattas av dataskyddsförordningens reglering, se artikel 2.2.c dataskyddsförordningen.
[95] Artikel 4.7 dataskyddsförordningen.
[96] Se t.ex. artiklarna 5, 6 och 12–22 dataskyddsförordningen.

personuppgiftsansvarig är skyldig att ersätta varje person som har lidit materiell eller immateriell skada till följd av överträdelse av dataskyddsförordningen.[97] En personuppgiftsansvarig kan också vid en rättslig prövning påföras administrativa sanktionsavgifter.[98]

I en registerförfattning regleras normalt sett vilken aktör som är personuppgiftsansvarig för en personuppgiftsbehandling som äger rum i en viss verksamhet. I exempelvis 1 kap. 6 § lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet pekas Skatteverket ut som personuppgiftsansvarig för den behandling av personuppgifter som verket ska utföra. Det kan jämföras med 2 kap. 6 § patientdatalagen (2008:355) som i stället för att peka ut en specifik namngiven aktör reglerar personuppgiftsansvaret för en särskild verksamhet, nämligen vårdgivare. Enligt patientdatalagen är en vårdgivare personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför. Hur personuppgiftsansvaret utfaller enligt patientdatalagen kan alltså delvis vara en effekt av hur ett landsting eller en kommun har valt att organisera sig.

En konsekvens av att personuppgiftsansvar fastställs i registerförfattning kan bli att en aktör bedöms vara personuppgiftsansvarig för en personuppgiftsbehandling som denne inte helt kan råda över. Exempelvis kan en myndighet, av en annan myndighet, vara anvisad en digital tjänst för registrering och befordran av vissa uppgifter. Är den avsändande myndighetens personuppgiftsansvar utpekat i registerförfattning kan denne komma att betraktas som ansvarig för den tekniska och organisatoriska säkerheten i tjänsten trots att den avsändande myndigheten inte alls har, eller har mycket små, möjligheter att påverka eller kontrollera säkerheten i tjänsten.

Gemensamt personuppgiftsansvariga

I dataskyddsförordningen har införts en bestämmelse om gemensamt personuppgiftsansvariga.[99] Bestämmelsen saknar motsvarighet i dataskyddsdirektivet[100] som ligger till grund för regleringen i personuppgiftslagen (1998:204). Av bestämmelsen framgår i huvudsak att om två eller flera personuppgiftsansvariga gemensamt fastställer

[97] Artikel 82 dataskyddsförordningen.
[98] Artikel 83 dataskyddsförordningen.
[99] Artikel 26 dataskyddsförordningen.
[100] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

ändamålen och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. De gemensamt personuppgiftsansvariga ska under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna i dataskyddsförordningen. Ansvarsfördelningen ska på lämpligt sätt återspegla de personuppgiftsansvarigas respektive roller och förhållanden gentemot den registrerade. Det gäller bl.a. skyldigheterna att tillse att de registrerade får information om personuppgiftsbehandlingen och att dessa kan utöva sina rättigheter enligt förordningen. De personuppgiftsansvariga får inom ramen för det gemensamma personuppgiftsansvaret utse en gemensam kontaktpunkt. Men oavsett hur de gemensamt personuppgiftsansvariga har fördelat ansvaret att fullgöra sina skyldigheter får den registrerade utöva sina rättigheter enligt dataskyddsförordningen emot var och en av de personuppgiftsansvariga.

I skälen till dataskyddsförordningen ges ingen ytterligare ledning i hur bestämmelsen är tänkt att tillämpas. Enligt vår uppfattning kan det dock inte uteslutas att bestämmelsen ger en öppning för att på ett mer flexibelt sätt fastställa det gemensamma personuppgiftsansvaret utifrån det ansvar respektive part i realiteten kan utöva så länge det inte påverkar den registrerades möjlighet att utöva sina rättigheter och under förutsättning att det inte strider mot den personuppgiftsansvariges skyldigheter som fastställts i t.ex. i registerförfattning.

Privatundantaget

Behandling av personuppgifter som en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll omfattas inte av dataskyddsförordningens reglering (det s.k. privatundantaget).[101] Att dataskyddsförordningen inte är tillämplig vid sådan behandling som en privatperson utför som ett led i verksamhet av rent privat natur innebär t.ex. att denne inte kan åläggas ett personuppgiftsansvar för behandlingen i fråga eller vara skyldig att skydda uppgifterna på lämpligt sätt.

Vem som är personuppgiftsansvarig för den behandling av personuppgifter som en privatperson utför inom ramen för en digital tjänst med ett eget utrymme har varit föremål för diskussion under de senaste åren bl.a. i förhållande till Skatteverkets förmedlingstjänst Mina meddelanden. Datainspektionen har i ett svar på en förfrågan

[101] Artikel 2.2 c dataskyddsförordningen.

från Skatteverket angående personuppgiftsansvaret i tjänsten Mina meddelanden uttalat att privatundantaget i 6 § personuppgiftslagen[102] innebär att fysiska personer ofta inte kan åläggas ett ansvar för behandlingar av personuppgifter som de utför i brevlådan.[103]

Utredningen om effektiv styrning av nationella digitala tjänster har föreslagit en författningsreglering av personuppgiftsansvaret för de aktörer som behandlar personuppgifter inom ramen för Mina meddelanden.[104]

Frågan om vem som är personuppgiftsansvarig för den behandling av personuppgifter som utförs av en privatperson inom ramen för ett eget utrymme är för närvarande uppe för prövning i förvaltningsrätten.[105] Målet gäller eHälsomyndighetens hälsokonto Hälsa för mig.[106]

Juridiska personers personuppgiftsansvar

Juridiska personer som behandlar personuppgifter i ett eget utrymme omfattas inte av det ovan beskrivna privatundantaget. Det innebär att en juridisk person kan vara ensamt eller gemensamt personuppgiftsansvarig för den behandling av personuppgifter som utförs i ett eget utrymme. En juridisk person som är personuppgiftsansvarig för en personuppgiftsbehandling i ett av en myndighet tillhandahållet eget utrymme saknar emellertid förutsättningar att garantera fullständig efterlevnad av dataskyddsregleringen. Även om en juridisk person i regel självständigt kan avgöra om en digital tjänst med eget utrymme ska användas för att utföra vissa myndighetsärenden[107] och eventuellt kan påverka vilka uppgifter som ska behandlas i tjänsten kan denne i princip aldrig påverka vilka tekniska och organisatoriska säkerhetsåtgärder som ska vidtas för att skydda uppgifterna i fråga. Det kan därför enligt vår bedömning ifrågasättas om en juridisk person kan bära hela personuppgiftsansvaret för alla

[102] Privatundantaget i 6 § personuppgiftslagen överensstämmer i sak med privatundantaget som föreskrivs i artikel 2.2 c i dataskyddsförordningen.
[103] *Svar på Skatteverkets förfrågan om personuppgiftsansvar i Mina Meddelanden*, Datainspektionen, 27 april 2015, dnr 111-2014.
[104] Se förslag till lag om infrastruktur för digital post, SOU 2017:114.
[105] Förvaltningsrätten i Stockholm, mål nr 11458-17.
[106] Hälsa för mig är en tjänst där enskilda individer ska kunna skapa ett personligt konto och lagra uppgifter om sin hälsa. eHälsomyndigheten tillhandahåller den tekniska plattformen för tjänsten och kan ge tredje part möjlighet att utveckla hälsorelaterade tjänster t.ex. appar för användarna.
[107] Jfr dock Skatteverkets tjänst för rot- och rutavdrag där endast digitala kommunikationskanaler kan användas för att ge in en ansökan till Skatteverket.

delar av den behandling av personuppgifter som sker inom ramen för ett eget utrymme.

Rättspraxis och tidigare utredning

Rättspraxis är knapphändig vad gäller myndigheters personuppgiftsansvar i digitala tjänster som tillhandahålls enskilda. Viss ledning för bedömningen av personuppgiftsansvaret kan emellertid hämtas i Högsta förvaltningsdomstolens avgörande HFD 2012 ref. 21. I målet prövade domstolen Försäkringskassans personuppgiftsansvar vid tillhandhållande av en elektronisk självbetjäningstjänst för anmälan av tillfällig föräldrapenning. Bakgrunden var att Datainspektionen i ett tillsynsbeslut hade förelagt Försäkringskassan att, som personuppgiftsansvarig, genomföra en risk- och sårbarhetsanalys av sin sms-tjänst för anmälan av tillfällig föräldrapenning. Högsta förvaltningsdomstolen fastställde inledningsvis att Försäkringskassan bestämt ändamål och medel med behandlingen, dvs. att anmäla sjukfall genom en särskild anvisad kommunikationskanal. Därefter gjorde domstolen bedömningen att den serie av åtgärder i fråga om personuppgifter som vidtas i de aktuella fallen kan betraktas som ett led i Försäkringskassans behandling av uppgifter i enskilda ärenden. Det gäller trots att Försäkringskassan saknar möjlighet att påverka hur uppgifterna hanteras innan de blir tillgängliga för kassan.

Rättsfallet ger uttryck för att en personuppgiftsansvarig som tillhandahåller och anvisar enskilda en särskild kommunikationskanal också ansvarar för den behandling som sker innan uppgifterna inkommit till myndigheten. Även om den personuppgiftsansvarige inte kan uppfylla sitt ansvar fullt ut är denne skyldig att vidta nödvändiga säkerhetsåtgärder för att uppgifterna som behandlas i tjänsten ska ha ett tillräckligt skydd också innan de överförs till den personuppgiftsansvarige i fråga.

Utredningen om effektiv styrning av nationella digitala tjänster har tagit ett vidare grepp i fråga om bedömningen av personuppgiftsansvar när det gäller behandling av personuppgifter inom ramen för ett eget utrymme. I sitt delbetänkande föreslår utredningen att regeringen utreder och tar ställning till hur offentliga myndigheter ska behandla och förhålla sig till s.k. eget utrymme.[108] Ett par remissinstanser har avstyrkt förslaget bl.a. mot bakgrund av att frågan om

[108] SOU 2017:23 s. 225.

personuppgiftsansvar ytterst avgörs av bestämmelserna i dataskyddsförordningen eller av nationell reglering av personuppgiftsansvar.

Våra överväganden om fördelning av personuppgiftsansvar

Begreppet personuppgiftsansvarig tjänar dels till att avgöra vem eller vilka som ansvarar för efterlevnaden av dataskyddsregleringen, dels till att peka ut vem eller vilka myndigheter eller andra aktörer den registrerade kan vända sig till för att utöva sina rättigheter. Likväl som det kan vara tämligen självklart vem som är personuppgiftsansvarig för en viss behandling kan det också vara förenat med avsevärda svårigheter att med en hög grad av exakthet fastställa ramarna för respektive aktörs personuppgiftsansvar i myndighetsgemensamma digitala tjänster med eget utrymme. Betydelsen av att med en tillräckligt hög grad av precision fastställa personuppgiftsansvaret kan emellertid förväntas öka bl.a. med beaktande av dataskyddsförordningens nya sanktionsmöjligheter.

För varje personuppgiftsbehandling som utförs i den offentliga förvaltningen finns en eller flera myndigheter som bär personuppgiftsansvaret för behandlingen ifråga. Hur ansvaret fördelas ska utredas av de parter som har del i personuppgiftsbehandlingen innan behandlingen påbörjas.

Utgångspunkten är att personuppgiftsansvaret fördelas utifrån omständigheterna i det enskilda fallet. I en myndighetsgemensam tjänst med eget utrymme kan det t.ex. förekomma att vissa myndigheter bär ett gemensamt personuppgiftsansvar medan andra aktörers ansvar har en mer begränsad räckvidd. En myndighet vars personuppgiftsansvar är fastställt i registerförfattning har regelmässigt ett mer begränsat bedömningsutrymme avseende gränserna för sitt personuppgiftsansvar jämfört med en myndighet eller annan aktör vars personuppgiftsansvar följer direkt av dataskyddsförordningen.

Komplexiteten i dagens digitala miljöer där flera olika parter kan dela på eller ha tillgång till samma digitala infrastruktur och där informationsöverföring sker sekundsnabbt gör att det kan vara förenat med komplicerade avvägningar att vid alla tillfällen och med hög grad av precision fastställa och fördela personuppgiftsansvaret. Hur ska t.ex. personuppgiftsansvaret fördelas när en myndighet registrerar och skickar uppgifter till en annan myndighet inom ramen för den mottagande myndighetens digitala infrastruktur? Övergår

ansvaret när den avsändande myndigheten trycker på skicka-knappen eller är ansvaret gemensamt med den mottagande myndighetens under tiden registreringen pågår? Upphör den avsändande myndighetens personuppgiftsansvar när en tjänsteman vid myndigheten tryckt på skicka-knappen eller sträcker det sig längre än så? Är en myndighets personuppgiftsansvar reglerat i registerförfattning kan det leda till att myndighetens personuppgiftsansvar utsträcks till att omfatta sådana områden myndigheten i praktiken inte kan råda över, t.ex. ansvar för tekniska och organisatoriska säkerhetsåtgärder i en tjänst som rent faktiskt tillhandahålls och förvaltas av en annan part.

Om det, med beaktande av omständigheterna i det enskilda fallet, inte är möjligt att med hög grad av precision fastställa personuppgiftsansvaret behöver det finnas andra metoder för att fördela ansvaret. Vissa remissinstansers ställningstaganden vid beredningen av Utredningen om effektiv styrning av nationella digitala tjänsters delbetänkande[109] i kombination med vad som förmedlats under vårt kartläggningsarbete pekar mot att det finns en tydlig vilja hos myndigheter att själva bedöma personuppgiftsansvar även när det är både rättsligt och tekniskt komplicerat. Att i författning peka ut personuppgiftsansvar kan förvisso vara lämpligt i vissa fall men utgångspunkten bör enligt vår uppfattning vara att myndigheter har egen kapacitet och förmåga att fastställa och fördela personuppgiftsansvar. För att detta ska kunna realiseras behöver myndigheterna emellertid få nödvändigt stöd för att kunna göra korrekta bedömningar.

I vårt kartläggningsarbete har det framhållits att praktiskt utformade vägledningar eller typfallsmodeller skulle vara till god hjälp i myndigheters arbete med att fastställa och fördela personuppgiftsansvar. Vi uppfattar att det finns ett klart behov av sådant stödmaterial men kan också se att det kommer att kvarstå situationer där t.ex. komplexiteten i ett it-system kan medföra att det, trots hjälp av stödmaterial, är svårt att fastställa exakt i vilken omfattning respektive aktör är personuppgiftsansvarig. För sådana situationer behöver det finnas en acceptans för att personuppgiftsansvaret i vissa delar måste fastställas genom överenskommelse eller avtal som är specifika för situationen i fråga.

[109] SOU 2017:114.

Dataskyddsförordningens nya bestämmelse om gemensamt personuppgiftsansvariga[110] reglerar att gemensamt personuppgiftsansvariga i viss utsträckning genom överenskommelse (arrangemang) kan fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt förordningen. Under förutsättning att det är tydligt för den registrerade vilka som är personuppgiftsansvariga och vem denne kan vända sig till för att utöva sina rättigheter bör en sådan fördelning inte ha några negativa effekter för den registrerade. Enligt vår uppfattning bör det också i andra svårbedömda situationer finnas utrymme att, även när personuppgiftsansvaret inte är gemensamt, fastställa fördelningen av personuppgiftsansvaret t.ex. i en överenskommelse.[111]

Rättslig grund för personuppgiftsbehandlingen

En myndighet som tillhandahåller en digital tjänst med eget utrymme, och som bedöms vara personuppgiftsansvarig för den behandling av personuppgifter som utförs i det egna utrymmet, behöver ha en rättslig grund för behandlingen i fråga.[112] Den personuppgiftsbehandling som sker i ett eget utrymme omfattas enligt vår uppfattning av den rättsliga grunden allmänt intresse. De förslag som vi har lämnat i kapitel 8.3.3, som innebär ett åliggande för myndigheter att, med vissa undantagsmöjligheter, tillhandahålla digitala mottagningsfunktioner för att ta emot handlingar från enskilda ger en än stabilare rättslig grund också i personuppgiftshänseende.

För egna utrymmen där syftet är att enskilda under längre tid t.ex. ska kunna lagra personuppgifter som är känsliga kan det emellertid, enligt vad vi kan se, behövas särskilda rättsliga överväganden om personuppgiftsbehandlingen har stöd i gällande rätt. Regeringen har också i propositionen om den nya dataskyddslagen anfört att vissa remissinstanser påpekat att det inte är möjligt att tillämpa de bestämmelser i den generella dataskyddslag som Dataskyddsutredningen föreslagit, när känsliga personuppgifter behandlas i myndigheters

[110] Artikel 26 dataskyddsförordningen.
[111] Se även om personuppgiftsbiträdesavtal i kapitel 11.
[112] Artikel 6.1 e dataskyddsförordningen och *Ny dataskyddslag*, prop. 2017/18:105, 2 kap. 2 § punkten 1.

s.k. egna utrymmen. Regeringen konstaterade att de särskilda frågeställningar som rör sådan behandling inte föranletts av dataskyddsförordningen och behandlade dem därmed inte i det lagstiftningsärendet. [113]

8.4.5 Behövs reglering eller annat stöd för ökad rättslig stabilitet?

Utredningens bedömning: Rättsläget avseende digitala tjänster med eget utrymme är i viss mån oklart. Det är angeläget att förbättra de rättsliga förutsättningarna så att utveckling av nya digitala tjänster baserat på användning av eget utrymme inte hindras eller hämmas i onödan.

Utredningens förslag: En myndighet ska ges i uppdrag att, i samverkan med Datainspektionen[114] och Myndigheten för samhällsskydd och beredskap, ta fram allmänna råd eller annat stödmaterial om hur myndigheter i förening med gällande rätt kan utveckla digitala tjänster som innefattar eget utrymme.

Skälen för utredningens bedömning och förslag

Behovet av egna utrymmen i digitala tjänster och rättsläget

I vårt arbete har vi noterat att det inte synes finnas några tecken på en teknik- eller samhällsutveckling som innebär att det inom överskådlig tid kan väntas växa fram helt nya sätt för kommunikation till och från förvaltningen, dvs. som i tekniskt avseende väsentligt skiljer sig från de digitala tjänster för ansökningar eller anmälningar via webben som i dag är kända. Med beaktande av vad som framkommit i kartläggningen och vad som erfarenhetsmässigt är känt bedömer vi tvärtom att bl.a. det egna utrymmet som företeelse kommer att bli mer och mer aktuellt i den digitala förvaltningen. Den offentliga förvaltningen kommer att behöva svara upp mot allmänhetens ökade förväntningar på smidiga och användarvänliga digitala tjänster som inte innebär att ofärdiga ansökningar blir allmänna handlingar.

[113] A. prop. s. 82.
[114] Datainspektionen byter namn till Integritetsskyddsmyndigheten under 2018.

Under kartläggningen har det också framkommit att det finns framtida behov av att, med avstamp i de egna utrymmen för tjänster gentemot enskilda som finns tillgängliga, återanvända de rättsliga koncept som det egna utrymmet innebär för att skapa nya tjänster för digital kommunikation vid verksamhetsmässiga informationsutbyten myndigheter emellan. Myndighetsgemensamma processer kan med andra ord förenklas och effektiviseras genom att en myndighet tillhandahåller ett eget utrymme åt en annan myndighet.

Som framgått av beskrivningen av kartläggningsresultatet och våra inledande överväganden om bl.a. personuppgiftsansvaret är rättsläget avseende sådana utrymmen i viss utsträckning oklart. Vår kartläggning visar också att det, trots befintlig praxis och förarbetsuttalanden, fortfarande finns tveksamhet i frågan om hur digitala tjänster med eget utrymme kan eller bör utformas för att vara förenliga med 2 kap. 10 § första stycket tryckfrihetsförordningen, dvs. hur tjänster kan utformas samtidigt som de rent tekniskt sett omfattas av lokutionen ”endast som led i teknisk bearbetning eller teknisk lagring för annans räkning”. Frågorna gäller också vilken typ av service som kan ges inom ramen för ett eget utrymme utan att allmänna handlingar skapas, eller hur de allmänna handlingar som uppstår ska hanteras av myndigheten. I anknytning till de beskrivna frågeställningarna finns även frågor om eller under vilka förutsättningar särskilt författningsstöd krävs för att tillhandahålla och behandla personuppgifter, bl.a. känsliga sådana, i ett eget utrymme. Vidare föreligger osäkerhet i frågor som rör fördelning av personuppgiftsansvar. En bedömning av personuppgiftsansvarets fördelning uppges sällan ge ett juridiskt helt säkerställt resultat trots att myndigheterna lägger ned mycket tid och kraft i bedömningarna. Flera har också framhållit att de vägledningar som finns i och för sig är av stor praktisk betydelse för myndigheternas utvecklingsarbete men att det kan råda tveksamhet vid tillämpning eftersom det inte av lagstiftaren eller regeringen har pekats ut vilken aktör som ska ge stöd och vägledning, med följd att det kan vara svårt att hänvisa till normgivning eller en etablerad rättskälla om frågor ställs på sin spets vid en rättslig prövning.

Med beaktande inte minst av vilka kostnader som är förenade med de utvecklingsarbeten som bedrivs har vi förståelse för den, här med våra sammanfattande ord, beskrivna osäkerhet som har getts

tillkänna under kartläggningen. Rättsläget är även enligt vår bedömning i viss utsträckning oklart. Den övergripande frågan om vilken fördelning av ansvar och risker som bör göras mellan lagstiftaren, regeringen respektive av enskilda myndigheter i samband med förvaltningens digitalisering ger sig också till känna.

Utgångspunkten att varje myndighet är fristående kan tala för att de myndigheter som känner tveksamhet beträffande de rättsliga förutsättningarna får avvakta till dess att framväxten av författningar, förarbeten, praxis och andra rättskällor ger ett, enligt varje tillämpare, tillräckligt stabilt stöd för att ansvariga i myndigheten ska känna trygghet i att gå vidare med digitaliseringsåtgärder som innefattar ett eget utrymme. Med beaktande av vårt uppdrag bedömer vi emellertid att ökad rättslig stabilitet för utformningen av digitala tjänster med eget utrymme behövs för att den digitala förvaltningen redan i ett kortare tidsperspektiv ska kunna fortsätta utvecklas på ett sätt som är såväl tryggt som effektivt. Det är med andra ord angeläget att förbättra de rättsliga förutsättningarna så att utveckling av nya digitala tjänster baserat på användning av eget utrymme inte hindras eller hämmas i onödan.

Uppdrag att ta fram allmänna råd eller annat stödmaterial

Vi ska enligt våra direktiv inte lämna förslag till författningsändringar i grundlag. Någon förändring vad avser den nu aktuella bestämmelsen i tryckfrihetsförordningen för att åstadkomma ökad rättslig tydlighet kan alltså inte föreslås. Vi ska inte heller lämna några förslag till ändringar i personuppgiftslagstiftningen. Det är alltså inte heller aktuellt att förslå särskild lagreglering inom det området.

Vi har inledningsvis övervägt att i reglering formulera de handlingsdirektiv rörande tillämpningen av tryckfrihetsförordningen som regeringen hittills endast gett uttryck för i förarbetsuttalanden[115] i nya rättsregler. Men vi bedömer också, utöver de ovan beskrivna ramarna för utredningens arbete, att en sådan reglering riskerar att bli alltför handlingsbegränsande i myndigheters framtida utvecklingsarbeten.

[115] Prop. 2016/17:180 s. 141 f. och prop. 2016/17:198 s. 16.

Som ovan nämnts utgår myndigheternas beslutsfattare ofta från de rekommendationer som ges i tillgängliga vägledningar när nya digitala tjänster med eget utrymme utvecklas. Samtidigt har vi under kartläggningen förstått att det finns ett önskemål om stödmaterial med en av lagstiftaren eller regeringen utpekad ansvarig avsändare.

Med beaktande av det ovan anförda och de förutsättningar vi har i vårt uppdrag bedömer vi att ökad rättslig stabilitet kring hur myndigheter i förening med gällande rätt kan utveckla digitala tjänster som innefattar eget utrymme bör kunna uppnås genom en mjukare styrning på uppdrag av regeringen, t.ex. i form av uppdrag för en viss myndighet att ta fram allmänna råd eller annat stödmaterial. På så sätt skulle den myndighetspraxis som har utvecklats, och som i vart fall delvis får anses etablerad med beaktande av förarbetsuttalanden och rättspraxis, fortsatt kunna befästas. I jämförelse med författningsreglering är förutsättningarna dessutom bättre att på ett enklare och mer effektivt sätt anpassa allmänna råd eller annat stödmaterial efter kommande rättsutveckling.

Allmänna råd är inte tvingande. Dess funktion är snarare att förtydliga innebörden i lag, förordning eller myndighetsföreskrifter och att ge generella rekommendationer om dess tillämpning.[116] Inom ramen för allmänna råd eller annat stödmaterial kan t.ex. rekommendationer utfärdas om hur digitala tjänster med eget utrymme kan utformas i förening med gällande rätt. Där kan också rekommendationer lämnas om hur tjänsten kan utformas samtidigt som service till enskilda användare kan ges utan att allmänna handlingar skapas hos myndigheten, alternativt hur myndigheter ska hantera allmänna handlingar som skapas när service tillhandahålls. Där skulle även metodmässiga frågor om eller under vilka förutsättningar en digital tjänst med eget utrymme behöver särskilt lagstöd kunna diskuteras.

I stödmaterial kan myndigheter dessutom ges mer handgripligt stöd för bedömningar av personuppgiftsansvar. Där kan också utfärdas rekommendationer och tillhandahållas verktyg, t.ex. mallar för överenskommelse, som myndigheterna kan använda som ett kompletterande verktyg när exempelvis it-systemen är så komplexa

[116] I 1 § författningssamlingsförordningen (1976:725) definieras allmänna råd som sådana generella rekommendationer om tillämpningen av en författning som anger hur någon kan eller bör handla i ett visst hänseende. Det behövs inget särskilt bemyndigande för att en myndighet ska få besluta allmänna råd på sitt område, se Regeringens proposition 1983/84:119 *om förenkling av myndigheternas föreskrifter, anvisningar och råd*, s. 24.

att det kan vara svårt att med en hög grad av precision fastställa respektive aktörs personuppgiftsansvar utifrån omständigheterna i det enskilda fallet.

Sammanfattningsvis bedömer vi att regeringen bör uppdra åt en myndighet att ta fram rekommendationer i allmänna råd eller i annat stödmaterial om hur myndigheter i förening med gällande rätt kan utveckla digitala tjänster som innefattar eget utrymme. En sådan åtgärd bedömer vi skulle bidra till att öka den rättsliga stabiliteten för utformningen av digitala tjänster med eget utrymme och på det sättet undanröjs också tveksamhet som annars kan fördröja framtagandet av fler sådana tjänster. Det förfarandet hindrar enligt vår bedömning inte att även andra myndigheter i samverkan bidrar till arbetet med att ta fram och förvalta stödmaterialet, tvärtom ser vi det som en förutsättning att även andra aktörer med inblick i pågående utvecklingsarbeten kan bidra. Den myndighet som ges uppdraget bör också samverka med Datainspektionen och Myndigheten för samhällsskydd och beredskap eftersom de frågor som aktualiseras, som framgått, även rör skydd för personuppgifter och informationssäkerhet.

Konsekvenser av förslaget

Som framgått i det ovanstående förväntas förslaget leda till att öka den rättsliga stabiliteten för utformningen av digitala tjänster med eget utrymme och på det sättet undanröja tveksamhet som annars kan fördröja framtagandet av fler sådana tjänster. Samtidigt kan goda förutsättningar ges för enkla och rättssäkra förfaranden i samband med att förvaltningen blir allt mer digitalt tillgänglig.

Förslaget kan medföra att den myndighet som ges uppdraget får extra kostnader för de resurser som kommer att behövas för att ta fram allmänna råd eller annat stödmaterial. För närvarande är Myndigheten för digital förvaltning under bildande och arbete pågår med att tilldela myndigheten resurser.[117] Om den myndigheten ges uppdraget är det svårt att beräkna de ytterligare resurser som krävs med anledning av förslaget i förhållande till myndighetens sammantagna uppdrag. Vi kan därför inte beräkna särskild resursåtgång för denna del och överlämnar också frågan om vilken myndighet som

[117] *Inrättande av en myndighet för digitalisering av den offentliga sektorn* (dir. 2017:117).

bör ges uppdraget till regeringen. Andra myndigheter bör inte drabbas av särskilda kostnader av förslaget, tvärtom kan förvaltningen som helhet förväntas bedriva ett mer kostnadseffektivt digitaliseringsarbete med det stöd som föreslås. För Datainspektionen och Myndigheten för samhällsskydd och beredskap bör den resursåtgång som föreslagen samverkan medför rymmas inom befintliga anslag. För generella konsekvenser av våra förslag hänvisas till kapitel 14.2.

9 Informationssäkerhet

9.1 Informationssäkerhet i en digital förvaltning

God informationssäkerhet är en grundläggande byggsten för den fortsatta utvecklingen av en trygg, innovativ och effektiv digital förvaltning. Hanteringen av information i elektroniska kommunikationsnät och it-system ökar i alla delar av samhället. Om hanteringen av, och säkerheten för, informationen brister riskerar det att få omfattande säkerhets- och integritetsmässiga konsekvenser för samhället i stort och för enskilda. I takt med att den digitala utvecklingen skapar nya möjligheter behöver förvaltningen därför kunna hantera både nationella och globala säkerhetsutmaningar.

Under de senaste åren har frågor om bristande informationssäkerhet och anknytande it-incidenter som drabbat den offentliga förvaltningen orsakat massmedial uppmärksamhet. Här kan t.ex. nämnas en driftstörning hos en av de större leverantörerna under hösten 2011 som fick till följd att vissa verksamheter, både offentliga och privata, i princip inte kunde använda sina it-system under flera veckor.[1] Lite närmare i tiden ligger Transportstyrelsens avsteg från säkerhetsskyddsregleringen vid utkontraktering, vilket bl.a. lett till en anmälan till konstitutionsutskottet om granskning av regeringen.[2] Även andra informationssäkerhetsrelaterade frågor om privata leverantörers tillgång till uppgifter, säkerhetsskyddsavtal och val av krypteringsmetod har varit föremål för diskussion och journalistisk granskning under senare tid.[3]

---

[1] Se t.ex. *Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter, En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011*, Myndigheten för samhällsskydd och beredskap, den 21 februari 2012, MSB 367-12.
[2] Se bl.a. Wikipedia *Transportstyrelsens it-upphandling*, den 11 januari 2018 och *Granskning av regeringen med anledning av Transportstyrelsens it-upphandling*, utskottsdokument 2016/17:dnr2581.
[3] Se t.ex. Sveriges Radios rapportering om polisens beslut om alternativ krypteringsmetod (hämtad den 15 januari 2018). http://sverigesradio.se/sida/artikel.aspx?artikel=6770725

Parallellt med bl.a. den journalistiska granskningen avseende it-incidenter och ifrågasatta säkerhetsrutiner kan vi dock skönja en ökad medvetenhet om vikten av god informationssäkerhet i alla typer av verksamheter liksom uppmärksamhet kring hur säkerhetsförebyggande åtgärder bäst kan utformas. Regeringen har också nyligen föreslagit en ny säkerhetsskyddslag[4] och lagrådsremiss om informationssäkerhet för samhällsviktiga och digitala tjänster.[5] Därtill diskuteras säkerhetsfrågor allt oftare i den offentliga debatten. I någon mening kan även dataskyddsförordningens[6] ikraftträdande antas ha bidragit till detta fokus.

Mot bakgrund av att informationssäkerhet spelar en avgörande roll för den fortsatta utvecklingen av en trygg, innovativ och effektiv digital förvaltning har vi valt att hantera dessa frågor i ett eget kapitel, utöver de hänvisningar och överväganden som genomgående präglar även andra kapitel. Syftet är främst att här närmare belysa det juridiska regelverk som styr informationssäkerhetsarbetet i den offentliga förvaltningen och att undersöka eventuella behov av komplettering eller anpassning av regleringen. Vi vill även åskådliggöra vikten av informationssäkerhet med särskilt fokus på myndigheters utkontraktering av it-drift och andra it-baserade funktioner, både till privata och till offentliga leverantörer.

9.2 Kartläggningsresultatet

Inom ramen för kartläggningsarbetet, och övriga kontakter som utredningen haft, har vi uppmärksammat att många av de informationssäkerhetsmässiga utmaningar myndigheterna står inför är gemensamma för hela förvaltningen. Det har påtalats att en avgörande förutsättning för att informationssäkerhetsfrågorna ska få den uppmärksamhet de förtjänar i en verksamhet är att frågorna prioriteras av myndighetsledningen. Verksamheten behöver därtill avsätta tillräckliga resurser, såväl tidsmässiga som personella, för att kunna arbeta aktivt och löpande med informationssäkerheten. Om det saknas tillräckliga resurser för informationssäkerhetsarbetet finns det en risk för att verksamhetens fokus läggs på leveranserna i

[4] *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag,* prop. 2017/18:89.
[5] Lagrådsremissen *Informationssäkerhet för samhällsviktiga och digitala tjänster*, den 15 februari 2018.
[6] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.

kärnverksamheten i första hand och på säkerheten i andra hand. Våra förslag i kapitel 8 med huvudregler om digital kommunikation ska inte heller förstås som att säkerheten ska komma i andra hand, den är i stället en nödvändig grund.

Flera aktörer har också framhållit behovet av att hantera informationssäkerhetsmässiga aspekter vid myndighetssamverkan. Det gäller särskilt myndighetssamverkan eller som inkluderar informationsutbyten. Information som utbyts mellan myndigheter behöver ha ett tillräckligt skydd hos alla aktörer som hanterar den. Informationsutbyten kan också medföra att nya informationsmängder uppstår. Det behöver finnas en beredskap för att hantera dessa informationsmängder på ett säkert och ansvarsfullt sätt.

När det gäller upphandling av it[7] har komplexiteten i att formulera ett välgrundat och behovsanpassat upphandlingsunderlag som uppfyller samtliga myndighetens krav, inklusive säkerhetsåtgärder, framhållits (se kapitel 11).

Ett par myndighetsrepresentanter har också påtalat att det finns ett regleringsunderskott på informationssäkerhetsområdet. Det har beskrivits att avsaknaden av reglering tenderar att medföra att varje myndighet uppfinner sina egna rutiner för informationssäkerhet när det gäller klassning av informationstillgångar, utformning av roller och behörighetstilldelning för åtkomst till information i it-system, val av tekniska, administrativa och organisatoriska säkerhetsåtgärder etc. En tydligare reglering som lägger grunden till en förvaltningsgemensam syn på informationssäkerheten i den offentliga förvaltningen efterfrågas.

9.3 Säkerhet – en prioriterad fråga

9.3.1 De politiska målen för informationssäkerhet

Regeringens mål för digitaliseringen av den offentliga förvaltningen är en enklare vardag för medborgare, en öppnare förvaltning som stödjer innovation och delaktighet samt högre kvalitet och effektivitet i verksamheten.[8] Det ska också finnas de bästa förutsättningarna för alla att på ett säkert sätt ta del av, ta ansvar för samt ha tillit till det digitala samhället.[9] För att alla ska våga lita på digitala

[7] Med it avses här it-drift och andra it-baserade funktioner.
[8] *Budgetpropositionen för 2018*, prop. 2017/18:1, utg.omr. 2 s. 93.
[9] *För ett hållbart Sverige – en digitaliseringsstrategi*, s. 16 om delmålet D-trygghet.

tjänster krävs säkra digitala system som värnar den personliga integriteten och att identifierade sårbarheter hanteras.

Säkerhet i vid bemärkelse är ett område som prioriteras av regeringen. Under 2017 har regeringen tagit fram dels en nationell säkerhetsstrategi, dels en nationell strategi för samhällets informations- och cybersäkerhet.[10] I den nationella säkerhetsstrategin finns en samlad redovisning av regeringens syn på säkerhet ur ett brett perspektiv. Den anger inriktningen och är samtidigt ett ramverk för det arbete som krävs för att gemensamt värna Sveriges säkerhet. Strategin syftar till att stärka vår förmåga att effektivt och samordnat förebygga och möta omedelbara och långsiktiga hot och utmaningar.

De huvudsakliga syftena med den nationella strategin för samhällets informations- och cybersäkerhet är dels att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet, dels att höja medvetenheten och kunskapen i hela samhället. I strategin har regeringen pekat ut ett antal strategiska prioriteringar varav en är att säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet. Målsättningen i denna del är bl.a. att offentlig förvaltning ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett systematiskt informationssäkerhetsarbete. För att förbättra förutsättningarna för, i första hand, statsförvaltningen att bedriva ett systematiskt informationssäkerhetsarbete på ett mer samordnat sätt uttalar regeringen att det ska finnas en nationell modell till stöd för detta arbete. Vidare ska det finnas en ändamålsenlig tillsyn som skapar förutsättningar för ökad informations- och cybersäkerhet i samhället. Regeringen framhåller att en förutsättning för att reglerna på informationssäkerhetsområdet ska få det genomslag som är avsett är att det finns en tillsyn som kan utföras på ett effektivt och ändamålsenligt sätt.

[10] *Nationell säkerhetsstrategi*, Statsrådsberedningen, januari 2017 och *Nationell strategi för samhällets informations- och cybersäkerhet*, Skr. 2016/17:213. Med begreppet cybersäkerhet avses i skrivelsen informationssäkerhet för digital information.

9.3.2 Pågående regeringsinitiativ kring informationssäkerhet

Informationssäkerhet m.m.

För närvarande pågår ett antal utredningar och andra initiativ som syftar till att stärka säkerheten ytterligare i den offentliga förvaltningen. Flera initiativ är särskilt inriktade på att stärka skyddet för information när myndigheter utkontrakterar, eller överväger att utkontraktera, it-drift.

Regeringen har som ovan nämnts nyligen lämnat en lagrådsremiss med förslag till lag om informationssäkerhet för samhällsviktiga och digitala tjänster.[11] Lagförslaget syftar till att uppfylla kraven i det s.k. NIS-direktivet[12] som träder i kraft i maj 2018 (se även kapitel 9.5.2).

Flera statliga utredningar har under de senaste åren lämnat förslag som syftar till att stärka informationssäkerheten i den offentliga förvaltningen. Utredningen om effektiv styrning av nationella digitala tjänster har i sitt slutbetänkande föreslagit att regeringen inleder ett arbete med att samordna och strukturera reglering inom informationssäkerhetsområdet och tar fram rättsliga krav till stöd för att samtliga offentliga myndigheter ska införa ett systematiskt och riskbaserat informationssäkerhetsarbete. Utredningen föreslår också att Myndigheten för samhällsskydd och beredskap (MSB) ges i uppdrag att utreda hur tillsyn över informationssäkerhetsområdet och incidentrapportering kan genomföras.[13]

Utredningen NISU 2014 lämnade i sitt slutbetänkande förslag på en ny förordning om statliga myndigheters informationssäkerhet. Utredningen föreslog också att tillsynen över den statliga sektorns informationssäkerhet skulle samordnas och förstärkas genom att ge MSB i uppdrag att bedriva tillsyn över statliga myndigheters informationssäkerhetsarbete. Därtill lämnade utredningen ett antal förslag i syfte att utveckla statens beställarkompetens för att kunna upphandla tillfredsställande it-lösningar.[14]

Försäkringskassan har fått ett tidsbegränsat uppdrag av regeringen (som avser åren 2017–2020) att erbjuda samordnad och säker

[11] Lagrådsremissen *Informationssäkerhet för samhällsviktiga och digitala tjänster*, den 15 februari 2018.
[12] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en höggemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.
[13] *reboot – omstart för den digitala förvaltningen*, (SOU 2017:114), kap. 9.
[14] *Informations- och cybersäkerhet i Sverige, Strategi och åtgärder för säker information i staten*, (SOU 2015:23).

it-drift för vissa myndigheter. Uppdraget ska utföras i samverkan med bl.a. MSB. Regeringen beskriver att etableringen av samordnade funktioner för gemensam it-drift mellan myndigheter ska ske stegvis, med fokus på funktioner och myndigheter där åtgärder bedöms leda till högre informationssäkerhet.[15] Därtill har Post- och telestyrelsen, med anledning av ett regeringsuppdrag, utrett och lämnat förslag på en förvaltningsmodell för skyddade it-utrymmen för offentliga aktörer som bedriver säkerhetskänslig verksamhet.[16]

När det gäller myndigheters utkontraktering generellt har det under de senaste åren genomförts olika regeringsuppdrag i syfte att bl.a. utreda olika former för myndigheter att utkontraktera it-drift. Här kan bl.a. nämnas att Statens servicecenter har analyserat förutsättningarna för att skapa en samordnad och gemensam funktion för delar av statliga myndigheters it-verksamhet.[17] Vi redogör närmare för den rapporten i kapitel 9.6.2.

Säkerhetsskydd

Säkerhetsskyddslagstiftningen genomgår för närvarande ett omfattande reformarbete och en ny säkerhetsskyddslag har föreslagits träda i kraft den 1 april 2019 (se kapitel 9.5.3).[18] Justitiedepartementet har därtill i en promemoria föreslagit skärpt kontroll av statliga myndigheters utkontraktering och överlåtelse av säkerhetskänslig verksamhet.[19] De föreslagna ändringarna, som införs i säkerhetsskyddsförordningen (1996:633), kommer att träda i kraft den 1 april 2018.

Den pågående statliga utredningen om vissa säkerhetsskyddsfrågor har därtill i uppdrag att kartlägga behovet av att förebygga att säkerhetsskyddsklassificerade uppgifter eller i övrigt säkerhetskänslig

[15] *Uppdrag att erbjuda samordnad och säker statlig it*-drift, regeringsbeslut den 24 augusti 2017, Fi2017/03257/DF.
[16] *Förslag till en förvaltningsmodell för skyddade it-utrymmen*, Post- och telestyrelsen, den 15 februari 2018, dnr. 17-8280.
[17] *En gemensam statlig molntjänst för myndigheternas it-drift. Delrapport i regeringsuppdrag om samordning och omlokalisering av myndighetsfunktioner*, Statens servicecenter, den 7 februari 2017, dnr 10052-2016/1121.
[18] Prop. 2017/18:89.
[19] *Skärpt kontroll av statliga myndigheters utkontraktering och överlåtelse av säkerhetskänslig verksamhet*, Ju 2017/07544/L4.

verksamhet utsätts för risker i samband med utkontraktering, upplåtelse och överlåtelse av sådan verksamhet och att föreslå olika förebyggande åtgärder, t.ex. tillståndsprövning. Utredaren ska också föreslå ett system med sanktioner i säkerhetsskyddslagstiftningen och hur en ändamålsenlig tillsyn ska vara utformad.[20]

Regeringen har därtill gett Säkerhetspolisen i uppdrag att redovisa dels en samlad bild av vilka generella brister som finns i säkerhetsskyddet hos de myndigheter Säkerhetspolisen har tillsyn över som bedriver mest skyddsvärd verksamhet, dels vilka ytterligare åtgärder som kan behöva vidtas för att hantera dessa brister.[21]

9.3.3 Granskning av informationssäkerhet i offentlig förvaltning

Under de senaste åren har granskningar av informationssäkerheten i offentlig förvaltning visat upp en oroande bild. Riksrevisionen konstaterade i en rapport 2016, efter att ha undersökt informationssäkerhetsarbetet på nio olika myndigheter, att arbetet med informationssäkerhet på de granskade myndigheterna låg på en nivå som var märkbart under vad som var tillräckligt. Riksrevisionen menade att förståelsen för vikten av en god informationssäkerhet överlag var för liten, med följd att arbetet med informationssäkerhet inte prioriteradess tillräckligt högt i förhållande till riskerna.[22]

I en av MSB, under 2014, utförd granskning av informationssäkerheten i kommunerna konstaterades att över 70 procent inte arbetade systematiskt med informationssäkerhet, över 40 procent hade inte någon utpekad funktion för informationssäkerhet och ungefär samma andel inte genomförde riskanalys avseende informationssäkerhet.[23]

---

[20] *Utkontraktering av säkerhetskänslig verksamhet, sanktioner och tillsyn – tre frågor om säkerhetsskydd*, Dir. 2017:32.

[21] *Uppdrag till Säkerhetspolisen om fördjupat kunskapsunderlag om arbetet med säkerhetsskydd hos myndigheterna med mest skyddsvärd verksamhet* , regeringsbeslut den 26 oktober 2017, Ju2017/08266/PO.

[22] *Informationssäkerhetsarbete på nio myndigheter, En andra granskning av informationssäkerhet i staten*, Riksrevisionen, maj 2016, RIR 2016:8.

[23] *En bild av kommunernas informationssäkerhetsarbete 2015*, Myndigheten för samhällsskydd och beredskap, december 2015, MSB943 och *Informationssäkerheten i Sveriges kommuner. Analys och rekommendationer utifrån MSB:s kommunenkät 2015*, Myndigheten för samhällsskydd och beredskap, december 2016, MSB1045.

MSB utförde också under 2014 en kartläggning av informationssäkerhetsarbetet hos samtliga myndigheter som omfattas av MSB:s föreskrifter om statliga myndigheters informationssäkerhet.[24] Det övergripande syftet med kartläggningen, som genomfördes som en enkätundersökning, var att säkerställa att föreskrifternas utformning gav ett ändamålsenligt stöd för statliga myndigheters systematiska arbete med informationssäkerhet. Någon fördjupad analys av resultatet har inte publicerats, men av MSB:s rapport framgår att myndigheterna själva uttryckte ett behov av ökat stöd inom vissa områden bl.a. kravställning, uppföljning, informationsklassning och kontinuitetsplanering.[25]

Under 2016 genomförde Säkerhetspolisen en inventering av säkerhetsskyddet hos myndigheter och institutioner som utifrån sin verksamhet är av högt skyddsvärde t.ex. energiförsörjning, telekommunikation och finanssektor. Resultatet visade att ju mer frekvent en myndighet hanterar generella säkerhetsfrågor i sin kärnverksamhet, desto bättre är den på säkerhetsskydd. Men hos ett flertal myndigheter fanns brister i arbetet med t.ex. den egna säkerhetsanalysen.[26]

9.4 Att möta nya risker

9.4.1 God informationssäkerhet stödjer och skapar tillit

Informationssäkerhetsarbete är en stödjande verksamhet som syftar till att öka kvaliteten hos samhällets funktioner. I och med den ökande digitaliseringen är god informationssäkerhet en förutsättning för att nya företeelser som uppstår, och ny teknik som utvecklas, ska kunna fungera och användas på ett säkert sätt.

Informationssäkerhet innebär en strävan efter att skydda information så att den alltid finns när den behövs (tillgänglighet), att det går att lita på att den är korrekt och inte manipulerad eller förstörd

[24] MSBFS 2009:10, nu ersatt av MSBFS 2016:1.
[25] *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter*, Myndigheten för samhällsskydd och beredskap, augusti 2014, MSB740.
[26] Säkerhetspolisens pressmeddelande den 16 mars 2017, http://www.sakerhetspolisen.se/ovrigt/pressrum/aktuellt/aktuellt/2017-03-16-sakerhetsskyddet-maste-starkas/gapet-mellan-hot-och-skydd-vaxer-sakerhetsskyddet-maste-starkas.html

(riktighet), att endast behöriga personer får ta del av den (konfidentialitet) och att det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet). Informationssäkerheten garanteras genom dels administrativa åtgärder för att skydda information som t.ex. föreskrifter eller behörighetsrutiner, dels tekniska åtgärder för it-säkerhet eller fysiska inpasseringskontroller.

Inom informationssäkerhetsområdet betonas ofta vikten av att verksamheter inför ett ledningssystem för informationssäkerhet, förkortat LIS. Ledningssystem för informationssäkerhet är ett stöd för hur informationssäkerhetsarbetet styrs i en verksamhet.[27] En central del är att verksamheten måste ha (myndighets)ledningens uttalade stöd i sitt arbete med informationssäkerhet. Det finns olika typer av svenska och internationella standarder som underlättar arbetet med ledningssystem för informationssäkerhet. Utifrån sådana standarder tar ledningssystem för informationssäkerhet sin utgångspunkt i en verksamhetsanpassad riskanalys och informationssäkerhetsarbetet följer en tydlig process.[28]

Genom god informationssäkerhet i den offentliga förvaltningen skapas tillit till de digitala tjänster och kommunikationskanaler förvaltningen tillhandahåller enskilda. Privatpersoner och företag har befogade krav på att den digitala förvaltningen upprätthåller en hög säkerhet när myndigheternas informationsmängder bearbetas, lagras och kommuniceras. Men även myndigheter emellan krävs en viss form av tillit till varandras informationssäkerhet för att bl.a. samverkan kring digitala informationsutbyten ska kunna komma till stånd.

God informationssäkerhet bidrar dessutom till att en verksamhet kan bedrivas på ett ändamålsenligt och effektivt sätt, att risken för att drabbas av avbrott eller störningar i driftmiljön minskar och att enskilda, vars uppgifter hanteras, inte utsätts för kränkningar genom att t.ex. obehöriga får åtkomst till uppgifterna eller att uppgifterna sprids på ett otillåtet sätt.

[27] MSB har utvecklat ett metodstöd för systematiskt informationssäkerhetsarbete. Metodstödet finns tillgängligt på webben, informationssakerhet.se
[28] Se t.ex. den svenska och internationella standardserien SS-ISO/IEC 27000.

9.4.2 Informationssäkerhetsrisker i en digital förvaltning

Samtidigt som digitaliseringens fördelar välkomnas står det klart att de risker och hot som behöver hanteras i dessa sammanhang är några av våra mest komplexa säkerhetsutmaningar. Säkerhetspolisen konstaterar i sin årsbok 2016 att den största risken för samhället och totalförsvaret utgörs av bristande informationssäkerhet. Försvarets radioanstalt (FRA) framhåller i sin årsrapport 2016 att säkerheten generellt hos myndigheter och statliga bolag inte är dimensionerad för den befintliga hotbilden.

Ovanstående uttalanden kan betraktas i ljuset av att det sker en ständigt växande hantering av information i elektroniska kommunikationsnät och it-system, både inom det offentliga och inom det privata. Äldre, men framför allt relativt sett nya, företeelser som artificiell intelligens, molntjänster, sakernas internet, sociala medier, stora datamängder (big data) och öppna data är exempel på områden där stora datamängder kan hanteras. Om det uppstår brister i hanteringen av information, och i synnerhet i skyddet av densamma, riskerar detta att få omfattande konsekvenser både för samhället i stort och för enskilda individers integritet. Bristande säkerhetsrutiner kan resultera i ett försämrat förtroende för digitala tjänster och för de myndigheter som tillhandahåller tjänsterna i fråga. Allvarliga och upprepade störningar i myndigheters it-system kan leda till förtroendekriser, som kan sprida sig till fler aktörer och tjänster och även till andra sektorer.

Utvecklingen och användningen av ny teknik och nya innovationer innebär också att nya hot och risker behöver hanteras. Hot- och riskskalan inom det informationsteknologiska området spänner från mindre omfattande risker för den enskilde individen till väl planerade, och med precision riktade, angrepp mot vitala delar av samhällets funktionalitet. Även antagonistiska hot såsom informationsoperationer och elektroniska angrepp mot skyddsvärda informations- och kommunikationssystem t.ex. i form av dataintrång, sabotage eller spionage behöver mötas. Detsamma gäller olika former av störningar i mjuk- eller hårdvara eller störningar i driftmiljö. Yttre fysiska händelser som t.ex. bränder, avgrävda kablar, översvämningar och solstormar utgör också en del av hotbilden. I andra fall är det den mänskliga faktorn som ligger bakom incidenter, eller som utnyttjas vid angrepp.

Teknikutvecklingen har därtill underlättat framväxten av en kriminell, gränsöverskridande, internetbaserad tjänstesektor, s.k. *crime-as-a-service*. Det innebär i princip att vem som helst, på internet, kan köpa t.ex. ett utpressningsprogram[29] som kan användas i brottsliga syften. Ett annat exempel är *malware-as-a-service*[30] där program med skadlig kod säljs som färdiga lösningar och som kan återanvändas i olika sammanhang. Ekonomiskt driven it-brottslighet kan inriktas mot att t.ex. utnyttja den mänskliga faktorn eller angripa datorer som inte har försetts med de senaste säkerhetsuppdateringarna. Även dessa typer av hot och risker behöver hanteras i en allt mer digital förvaltning.

9.5 Gällande rätt om informationssäkerhet

9.5.1 Inledning

Som framgått i kapitel 4 finns bestämmelser om informationssäkerhet i flera olika regelverk. I huvudsak reglerar författningarna antingen skydd för information i viss typ av verksamhet eller särskilt skydd för viss typ av information. I syfte att här närmare åskådliggöra den juridiska kartan inom området följer nedan en redogörelse av ett antal författningar som ur ett informationssäkerhetsperspektiv är mer eller mindre centrala för den offentliga förvaltningen. I detta kapitel går vi dock inte närmare in på den straffrättsliga reglering som innebär kriminalisering av vissa handlingar, t.ex. brottsbalkens reglering av dataintrång.

[29] Ett utpressningsprogram (ransomware) är en skadlig programvara som krypterar filerna på en dator. För att häva krypteringen eller återfå kontrollen över datorn kräver utpressningsprogrammet en lösensumma eller annat som gynnar förövaren som ligger bakom programmet (Wikipedia den 5 januari 2018, ”Ransomware”).

[30] Malware (sabotageprogram) är ett samlingsbegrepp för oönskade datorprogram eller delar av datorprogram som har utvecklats i syfte att störa it-systemet för att samla in information i smyg eller utnyttja för ändamål som inte gagnar användaren (Wikipedia den 5 januari 2018, ”Malware”).

9.5.2 Informationssäkerhet i olika verksamheter

Statliga myndigheter

Krav på statliga myndigheters informationssäkerhet finns i förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Förordningen kompletteras av MSB:s föreskrifter om statliga myndigheters informationssäkerhet och om statliga myndigheters rapportering av it-incidenter.[31]

Av förordningen framgår att varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Behovet av säkra ledningssystem för informationssäkerhet ska särskilt beaktas. Vidare regleras en skyldighet för myndigheterna att rapportera it-incidenter till MSB.[32]

I de till förordningen anknytande föreskrifterna om statliga myndigheters informationssäkerhet finns ytterligare reglering kring utformning av ledningssystem för informationssäkerhet, allmänna krav på myndigheternas informationssäkerhetsarbete samt krav på intern incident- och kontinuitetshantering. Föreskrifterna om statliga myndigheters rapportering av it-incidenter innehåller detaljerade krav på vilka typer av incidenter som ska rapporteras, när och hur rapportering ska ske samt vad som gäller vid utkontraktering. I anslutning till båda föreskrifterna har MSB tagit fram allmänna råd som förtydligar innebörden av bestämmelserna i föreskrifterna och ger generella rekommendationer om tillämpningen.

Kommuner och landsting

För kommuner och landsting gäller lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap med tillhörande förordning. Regleringen omfattar emellertid inte specifika bestämmelser om informationssäkerhet i bemärkelsen säker informationshantering.

[31] MSBFS 2016:1 och 2016:2.
[32] 19 och 20 §§ förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Hälso- och sjukvård

Hälso- och sjukvården hanterar en stor mängd känslig information och informationshanteringen behöver uppfylla kraven på patientsäkerhet och god kvalitet. Hantering av patientinformation regleras av patientdatalagen (2008:355) och patientdataförordningen (2008:360) samt Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården.[33] I föreskrifterna finns detaljerad reglering av kraven på informationssäkerhet när vårdgivare behandlar patienters personuppgifter i hälso- och sjukvården.

Samhällsviktiga tjänster

NIS-direktivet, som ska vara genomfört i svensk lagstiftning senast i maj 2018, syftar till att förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverks- och informationssystem.[34] Direktivet innebär bl.a. skyldigheter för vissa leverantörer av samhällsviktiga tjänster, och vissa leverantörer av digitala tjänster, att vidta säkerhetsåtgärder för att hantera risker samt förebygga och hantera incidenter i nätverk och informationssystem som de är beroende av för att tillhandahålla tjänsterna. Leverantörerna ska också rapportera incidenter som har en betydande eller avsevärd inverkan på kontinuiteten i tjänster.

I direktivet identifieras sju sektorer som tillhandahåller samhällsviktiga tjänster. Dessa är bankverksamhet, digital infrastruktur, energi, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt transport.

Efterlevnaden av regelverket ska enligt direktivet ske genom att en eller flera tillsynsmyndigheter utses. En sådan tillsynsmyndighet ska ha befogenhet och medel för att kontrollera att leverantörerna uppfyller sina skyldigheter samt fastställa regler om sanktioner vid överträdelse av regelverket.

[33] HSLF-FS 2016:40.
[34] Lagrådsremissen *Informationssäkerhet för samhällsviktiga och digitala tjänster*, den 15 februari 2018, vari föreslås en ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster.

9.5.3 Informationssäkerhet för viss typ av information

Allmänna handlingar

Skydd för vissa typer av information finns i flera olika författningar. En del författningar är av mer generell karaktär och omfattar betydande delar av myndigheters informationstillgångar, t.ex. allmänna handlingar. Av 2 kap. tryckfrihetsförordningen framgår vilken typ av information hos myndigheterna som ska betraktas som allmänna handlingar och som huvudregel ska vara offentliga. Vissa allmänna handlingar innehåller dock känsliga uppgifter och i offentlighets- och sekretesslagen (2009:400) regleras därför vilka uppgifter i sådana handlingar som ska beläggas med sekretess.

En myndighets allmänna handlingar bildar myndighetens arkiv och enligt arkivregleringen ska sådana handlingar antingen gallras eller bevaras. Arkivlagen (1990:782), arkivförordningen (1991:446) samt Riksarkivets anknytande föreskrifter[35] syftar bl.a. till att säkra riktigheten hos, och skapa tillgänglighet till, allmänna handlingar. Arkivregleringen är för närvarande föremål för översyn i syfte att bl.a. att modernisera och anpassa regleringen till utvecklingen på området.[36]

Säkerhetsskydd – skydd av säkerhetskänslig verksamhet

Säkerhetsskyddslagen (1996:627) och anknytande förordning (1996:633) ställer krav på särskilda skyddsåtgärder (säkerhetsskydd) för den information som kan påverka rikets säkerhet. Lagen gäller vid verksamhet hos staten, kommunerna och landstingen, men även aktiebolag, handelsbolag, föreningar och stiftelser över vilka staten, kommunerna och landstingen utövar ett rättsligt bestämmande inflytande.[37] Lagen gäller också för enskilda om verksamheten är av betydelse för rikets säkerhet.

Med säkerhetsskydd avses bl.a. skydd av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör

[35] Se t.ex. Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar, RA-FS 2009:1 och Riksarkivets föreskrifter och allmänna råd om tekniska krav på elektroniska handlingar, RA-FS 2009:2.
[36] *Översyn av arkivområdet*, (dir. 2017:106).
[37] 4 § säkerhetsskyddslagen.

rikets säkerhet.[38] Informationssäkerhet är en av tre grundläggande säkerhetsskyddsåtgärder i säkerhetsskyddslagen och ska förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs.[39] Vilka uppgifter som en myndighet ska hålla hemliga med hänsyn till rikets säkerhet avgörs efter en säkerhetsanalys hos respektive myndighet. Ytterligare bestämmelser om kraven på informationssäkerhet finns i säkerhetsskyddsförordningen.[40] Försvarsmakten och Säkerhetspolisen ansvarar för tillsyn och kontroll av säkerhetsskyddet hos myndigheter och andra som lagen gäller för.[41]

Som nämnts i kapitel 9.3.2 pågår för närvarande en reform av säkerhetsskyddslagstiftningen och en ny säkerhetsskyddslag föreslås träda i kraft den 1 april 2019.[42]

Dataskyddsförordningen – skydd för personuppgifter

Dataskyddsförordningens bestämmelser om säkerhet tar sikte på behandlingen av personuppgifter.[43] Den som behandlar personuppgifter (personuppgiftsansvarig och/eller personuppgiftsbiträde) ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen. Vid val av säkerhetsåtgärder ska förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos it-systemen och it-tjänsterna beaktas. Vidare ska även förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en teknisk eller fysisk incident beaktas. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandlingen medför, i synnerhet i form av oavsiktlig eller olaglig förstöring, förlust eller ändring liksom obehörigt röjande av eller obehörig åtkomst till de personuppgifter

[38] 6 § 2 säkerhetsskyddslagen.
[39] 7 § 1 säkerhetsskyddslagen.
[40] 9–13 §§ säkerhetsskyddsförordningen.
[41] 31 § säkerhetsskyddslagen och 39 § säkerhetsskyddsförordningen.
[42] Prop. 2017/18:89.
[43] Personuppgifter är enligt definitionen i artikel 4.1 varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikator eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

som behandlas.[44] Därtill finns en skyldighet för personuppgiftsansvariga att anmäla personuppgiftsincidenter till ansvarig tillsynsmyndighet.[45] Datainspektionen,[46] som är tillsynsmyndighet enligt dataskyddsförordningen, har möjlighet att bl.a. utfärda sanktioner vid överträdelser av regelverket.

9.6 Informationssäkerhet vid utkontraktering

9.6.1 Utkontraktering till privata leverantörer

Förvaltningsmyndigheter under regeringen ska bedriva sin verksamhet effektivt och hushålla väl med statens resurser.[47] Riksdagen och regeringen har även tidigare gett uttryck för att det är önskvärt att en större del av myndigheternas it-behov tillfredsställs med hjälp av outsourcing.[48] Utkontraktering av it-drift och andra it-baserade funktioner har också enligt våra iakttagelser kommit att bli allt mer centralt för en kostnadseffektiv och även i övrigt väl fungerande digital förvaltning.

Ekonomistyrningsverket uppskattar statsförvaltningens samlade it-kostnader till mellan 25 och 30 miljarder per år. Ungefär 14–16 procent av den totala summan beräknas avse kostnad för utkontraktering.[49] Se vidare kapitel 13 om it-kostnader.

Utkontraktering av bl.a. it-drift kan bidra till att åstadkomma en ändamålsenlig, kostnadseffektiv och tillgänglig förvaltning som erbjuder god digital service för privatpersoner och företag. Samtidigt ställer utkontraktering höga krav på både beställarkompetens och säkerhetsmedvetande hos en myndighet för att inte leda till oönskade risker.[50]

---

[44] Artikel 32 dataskyddsförordningen.
[45] Artikel 33 dataskyddsförordningen.
[46] Datainspektionen byter namn till Integritetsskyddsmyndigheten under 2018.
[47] 3 § myndighetsförordningen (2007:515).
[48] Se finansutskottets betänkande 2011/12:FiU2 s. 30 och regeringens skrivelse *Riksrevisionens granskning av it inom statsförvaltningen och statliga it-projekt*, rskr 2010/11:138. Se även Riksrevisionens rapport och *IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet*?, Riksrevisionen, 12 januari 2011, RiR 2011:4.
[49] *Myndigheters strategiska it-projekt och it-kostnader, Delrapport it-användningsuppdraget*, Ekonomistyrningsverket, 21 december 2017, P-2017-77 och *Fördjupat it-kostnadsuppdrag, Delrapport 2: Kartläggning av it-kostnader*, Ekonomistyrningsverket, 23 oktober 2015, 2015:58.
[50] I kapitel 11 om avtal och överenskommelser redogörs mer utförligt för frågor kopplade till beställarkompetens och avtal.

Till stöd för att genomföra upphandling av it där informationssäkerhetsaspekterna hanteras på ett ändamålsenligt sätt har MSB tagit fram en vägledning om informationssäkerhet i upphandling.[51]

FRA har i en av Riksrevisionen utförd granskning uttalat att en hårt styrd it-budget och externa krav på lönsamhet eller sparsamhet kan vara anledningar till att myndigheter väljer att utkontraktera sin it-drift. Utkontraktering i kombination med otillräcklig beställarkompetens leder dock ofta till en kortsiktig besparing. I det långa loppet kan flera brister uppstå som är svåra att värdera i kronor. Många beställare gör dessutom misstaget att förutsätta att säkerhet ingår i avtalet även om detta inte uttryckligen är specificerat.[52]

I Kammarkollegiets ramavtal för it-drift finns aspekter av informationssäkerhet inkluderade för avropande myndigheter. Avtalet används dock främst som mall och en avropande myndighet avgör själv det slutliga innehållet i avtalet. I en undersökning av ett antal avrop från Kammarkollegiets ramavtal framkom att de undersökta avtalen i hög grad saknade relevanta krav på informationssäkerhet. De krav som formulerats var i samtliga fall inriktade på enstaka frågor och inte ett resultat av en systematisk genomgång av myndighetens behov utifrån en genomarbetad riskanalys.[53]

Utredningen NISU 2014 konstaterade i sitt betänkande att beställarkompetensen för informationssäkerhet är alltför svag. Utredningen nämner ett antal olika metoder som kan utveckla beställarkompetensen exempelvis användning av en gemensam standard för informationssäkerhet, successiv infogning av krav på certifiering och hänvisning till internationellt accepterade standarder.[54]

[51] *Vägledning – informationssäkerhet i upphandling, Informationssäkerhet i upphandling av system, outsourcing och molntjänster*, Myndigheten för samhällsskydd och beredskap, april 2013, MSB555.
[52] *Informationssäkerheten i den civila statsförvaltningen*, Riksrevisionen, 10 november 2014, RIR 2014:23 s. 53.
[53] *Outsourcing av it-tjänster i kommuner*, Myndigheten för samhällsskydd och beredskap, augusti 2014, MSB728.
[54] SOU 2015:23 s. 240 f.

9.6.2 Utkontraktering till annan myndighet

Myndighetssamverkan kring it-drift och andra it-baserade funktioner

Utkontraktering som sker inom den offentliga förvaltningen går ofta under benämningen samverkan. Det finns olika anledningar till att en myndighet väljer att utkontraktera sin it-drift till en annan myndighet. Omorganisation i den statliga förvaltningen kan vara en sådan anledning. Här kan bl.a. nämnas att Kronofogden, som innan myndigheten bildades var en avdelning hos Skatteverket, uppdrar åt Skatteverket att handha Kronofogdens it-drift. Pensionsmyndigheten, som vid sitt bildande övertog ansvaret för den allmänna pensionen från Försäkringskassan, delar flera gemensamma system med Försäkringskassan som också handhar driften av dem. En annan form av liknande samverkan inom statlig förvaltning sker inom ramen för Statens servicecenters uppdrag att tillhandahålla tjänster inom löne- och ekonomiadministration.

Inom den kommunala sektorn är det vanligt förekommande med både större och mindre samarbeten kring gemensam it-drift. En granskning utförd av MSB visar att 66 procent av kommunerna ingår i någon form av kommunal samverkan om it. För kommuner finns det uppenbara stordriftsfördelar med gemensam it-drift eller samarbete kring digitala system och tjänster eftersom kommunernas obligatoriska uppgifter utförs på ett likartat sätt.[55] Förslaget om en generell rätt till kommunal avtalssamverkan kan också komma att förenkla förutsättningarna för kommunal avtalssamverkan kring it-drift.[56]

Även länsstyrelserna samverkar kring gemensam it-drift genom att Länsstyrelsen i Västra Götalands län ansvarar för it-stödet för landets samtliga 21 länsstyrelser.

God beställarkompetens och medvetenhet om vilken nivå av säkerhet som krävs för att skydda information vid utkontraktering krävs i regel även vid utkontraktering till, eller samverkan med, annan myndighet kring gemensam it-drift. Precis som vid köp av tjänst från en privat leverantör är det också ofta lämpligt att förhållandet mellan offentliga aktörer regleras av avtal eller annan överenskommelse som anger t.ex. vilken nivå av säkerhet som ska gälla.

[55] Outsourcing av it-tjänster i kommuner, MSB728.
[56] Lagrådsremissen *En generell rätt till kommunal avtalssamverkan*, den 22 februari 2018.

Gränsen mot upphandlingsplikten

I vårt kartläggningsarbete har frågor ställts om var gränsen går för när samarbete mellan myndigheter faller inom ramen för upphandlingslagstiftningen. Enligt upphandlingsregelverket är viss upphandling mellan två eller flera myndigheter undantagen från upphandlingsplikt. Det gäller sådan upphandling som syftar till att upprätta eller reglera formerna för ett samarbete mellan myndigheter som ska säkerställa att de offentliga tjänster som myndigheterna ska utföra, tillhandahålls för att uppnå myndigheternas gemensamma mål. För att undantaget ska vara tillämpligt krävs att samarbetet styrs endast av överväganden som hänger samman med allmänintresset och att myndigheterna på den öppna marknaden utövar mindre än 20 procent av den verksamhet som berörs av samarbetet.[57]

Upphandlingslagstiftningen följer av EU-rätt. Det behöver därför enligt vår uppfattning framhållas i det här sammanhanget att det alltjämt är upp till varje medlemsstat att bestämma hur statsförvaltningen ska organiseras. Att frågor har ställts inom detta område under vår kartläggning beror bl.a. på att Kammarrätten i Stockholm i en dom från 2017 bedömde att den överenskommelse som Kungliga biblioteket ingått med Riksarkivet om digitalisering av pliktlevererade dagstidningar inte var undantagen från upphandlingsplikten.[58]

Upphandlingsmyndigheten har i en rapport analyserat undantaget från upphandlingsreglerna vid samarbeten mellan upphandlande myndigheter och enheter. Även av den rapporten kan utläsas att det finns en osäkerhet kring tillämpningsområdet för avtalsbaserade samarbeten, inte minst vid samarbeten kring användning av it och digitalisering, vilket gör tillämpningsområdet svårbedömt.[59]

Kommunutredningen poängterade i sitt delbetänkande att kommuner och landsting som överväger att ingå kommunala samverkansavtal med andra kommuner och landsting måste ta ställning till upphandlingslagstiftningens tillämplighet.[60]

---

[57] 3 kap. 17 § lagen (2016:1145) om offentlig upphandling.
[58] Se Kammarrätten i Stockholms dom den 21 juni 2017, mål nr 7355-16. Målet överklagades till Högsta förvaltningsdomstolen som inte meddelade prövningstillstånd, mål nr 4106-17.
[59] *Offentlig avtalssamverkan – om s.k. Hamburgsamarbeten och inköpscentralers möjlighet att bedriva grossistverksamhet*, Upphandlingsmyndigheten, mars 2017, 2017:3, s. 4.
[60] Kommunutredningens delbetänkande, *En generell rätt till kommunal avtalssamverkan*, (SOU 2017:77), s. 20.

Som framgår av det ovan sagda föreligger det en viss rättslig osäkerhet som rör upphandlingslagstiftningen, vilken kan ha en hindrande eller hämmande inverkan på förvaltningens digitaliseringsåtgärder. Lagstiftningen på området har emellertid nyligen genomgått en reform och andra aktörer utför, respektive har utfört, arbete enligt redogörelsen ovan. Klargöranden kan också komma att göras av såväl nationella domstolar som av EU-domstolen. Vi ser därför inte förutsättningar för att inom ramen för vår utredning nå framgång med att ytterligare försöka klargöra dessa gränser.[61] Det torde emellertid finnas anledning för regeringen att noga följa hur praxis inom området utvecklas för att, vid behov, kunna vidta lämpliga åtgärder.

Tidigare analys av gemensam statlig it-drift

Statens servicecenter har i ett regeringsuppdrag analyserat förutsättningarna för att skapa en samordnad eller gemensam funktion för delar av statliga myndigheters it-verksamhet. I Statens servicecenters rapport föreslås sammanfattningsvis att en statlig myndighet ska tillhandahålla skalbar och flexibel datorkraft och lagring genom en statlig molntjänst för samordnad it-drift.[62] I rapporten beskrivs bl.a. att inrättandet av en statlig molntjänst skulle kunna bidra till förstärkt it-säkerhet och driftsäkerhet, sänkta kostnader för it-drift i den offentliga förvaltningen och till att förenkla och effektivisera anslutna myndigheters processer för inköp av it-drift eftersom upphandling inte behövs.

Inom ramen för uppdraget genomförde Statens servicecenter en enkät riktad till samtliga myndigheter under regeringen och dialogmöten med företrädare för de 15 största myndigheterna. Resultatet av enkäten och dialogmötena visade att många myndigheter efterfrågar en samordnad, dynamisk och flexibel statlig it-drift. Gemensam statlig it-drift skulle kunna hantera många av myndigheternas utmaningar, inte minst genom att it-säkerheten och driftsäkerheten förstärks. I rapporten beskrivs också hur sex med Sverige jämförbara länder har valt att samordna statsförvaltningens it-drift (Danmark, Finland, Frankrike, Kanada, Nederländerna och Storbritannien).

[61] Jfr Kommunutredningens slutsatser, SOU 2017:77 s. 136 f.
[62] En gemensam statlig molntjänst för myndigheternas it-drift, dnr10052-2016/1121.

Fördelar som lyfts fram av de länder som har etablerat någon form av gemensam it-drift för statsförvaltningen beskrivs vara dels förenklade beställnings- och inköpsprocesser, dels förbättrad it- och informationssäkerhet.

9.7 Våra överväganden och förslag

9.7.1 Inledande överväganden

Vårt uppdrag

I våra utredningsdirektiv betonas att vi i vårt arbete särskilt ska beakta behovet av informationssäkerhet. Rättsliga förutsättningar för en digital och samverkande förvaltning måste också stå i samklang med behovet av informationssäkerhet i förvaltningen.

Under kartläggningsarbetet, och utifrån övriga kontakter vi har haft inom ramen för utredningen, har det tydliggjorts för oss att god informationssäkerhet är en förutsättning för den fortsatta utvecklingen av en trygg, innovativ och effektiv digitalt samverkande förvaltning. Om enskilda saknar förtroende för säkerheten i den offentliga förvaltningen kommer det att påverka deras vilja att använda de digitala tjänster som tillhandahålls. Det krävs tillit till en digital förvaltning för att enskilda ska välja att lämna ifrån sig privata uppgifter och annan information via digitala kanaler.

Som vi har redogjort för i kapitel 9.3.3 har det under de senaste åren påtalats att det finns brister i informationssäkerhetsarbetet i den offentliga förvaltningen. Granskningar har visat att informationssäkerhet inte alltid är, eller har varit, ett prioriterat område. Det handlar bl.a. om att det har saknats förståelse för vikten av god informationssäkerhet och att informationssäkerhetsarbetet inte har haft tillräckligt hög prioritet i verksamheten.

Vi kan emellertid också skönja en utveckling i positiv riktning där säkerhetsfrågorna får mer uppmärksamhet och där det allmänna medvetandet om behovet av säkerhet för att skydda samhällets informationstillgångar har höjts. Det förefaller finnas en allt ökande förståelse för att både personer i myndighetsledande befattning, övriga tjänstemän och även allmänheten behöver ha kunskap om informationssäkerhet. En bidragande orsak torde vara att regeringen uttryckligen prioriterar säkerhetsfrågor.

Rättsligt stöd för informationssäkerhetsarbetet i offentlig förvaltning

Som vi har redogjort för i kapitel 4 och kapitel 9.5 träffar den befintliga regleringen avseende informationssäkerhet olika aktörer och information, med delvis olika syften, samtidigt som regleringen finns spridd på olika håll. Det finns också en tydlig trend, både på EU-nivå och nationellt, att i allt större utsträckning ställa rättsliga krav på informationssäkerhet. Här kan exempelvis nämnas vad som ovan redovisats om NIS-direktivets och dataskyddsförordningens uttalade krav på säkerhet och förslaget till en reformerad säkerhetsskyddslag. Samtidigt kan det emellertid också konstateras att det med avseende på styrningen av informationssäkerhetsarbetet i offentlig förvaltning, framstår som att det även efter genomförandet av NIS-direktivet och införandet av en ny säkerhetsskyddslag kommer att finnas ett visst underskott av reglering på informationssäkerhetsområdet.

För kommun- och landstingssektorns informationssäkerhetsarbete saknas generellt tillämpliga rättsliga krav på att arbeta riskbaserat och systematiskt och att rapportera it-incidenter. För de statliga myndigheterna gäller MSB:s föreskrifter om statliga myndigheters informationssäkerhet och rapportering av it-incidenter.[63] Regeringen har vidare en uttalad ambition att det ska finnas en ändamålsenlig tillsyn som skapar förutsättningar för ökad informationssäkerhet. För närvarande finns emellertid ingen myndighet som har till uppdrag att utöva ändamålsenlig tillsyn över hela den offentliga förvaltningens generella informationssäkerhetsarbete.

Den viljeriktning regeringen ger uttryck för i informations- och cybersäkerhetsstrategin är ett steg i riktning mot ökad informationssäkerhet i den offentliga förvaltningen. Att t.ex. skapa en nationell modell till stöd för ett systematiskt informationssäkerhetsarbete ser även vi som ett välkommet initiativ för hela den offentliga sektorn, även om modellen i första hand riktar sig till myndigheterna inom statsförvaltningen. Vägledningar och metodstöd utgör ett instrument för att åstadkomma god informationssäkerhet i offentlig förvaltning. Men vägledningar och metodstöd är inte juridiskt bindande. Avsaknad av rättslig bundenhet kan leda till att krav på informationssäkerhet ges lägre prioritet. För att säkra ett gott informationssäkerhetsarbete i hela den offentliga förvaltningen bör enligt

[63] MSBFS 2016:1 och 2016:2.

oss övervägas ytterligare styrning genom rättsregler som omfattar den offentliga förvaltningen i stort.

Samordnad it-drift i den offentliga förvaltningen

Som framgått har utkontraktering av it-drift och andra it-baserade funktioner enligt våra iakttagelser kommit att bli allt mer centralt för en kostnadseffektiv och även i övrigt väl fungerande digital förvaltning. Sådan utkontraktering kan ske antingen till en privat leverantör eller till en annan myndighet.

I syfte att förbättra de rättsliga förutsättningarna för utkontraktering till privata leverantörer, när det är lagligt, säkert och lämpligt, föreslår vi i kapitel 10 en ny reglering avseende tystnadsplikt. Det förekommer emellertid situationer där det av olika skäl inte är lämpligt att utkontraktera t.ex. it-drift till privata leverantörer. När detta inte är lämpligt, och en myndighet inte själv har förutsättningar att handha sin it-drift, behöver det finnas andra alternativ tillgängliga. Ett sådant alternativ är att skapa bättre förutsättningar för att utkontraktera viss it-drift till en annan myndighet i den offentliga förvaltningen.

Som vi tidigare har beskrivit i kapitel 9.6.2 har förutsättningarna för samordnad it-drift, i det här fallet inom ramen för en molntjänst, analyserats av Statens servicecenter.[64] Vidare har Försäkringskassan för närvarande i uppdrag att erbjuda samordnad och säker statlig it-drift för vissa statliga myndigheter under åren 2017–2020.[65] Det övergripande syftet med uppdraget är att pröva och utvärdera former för samordnad och säker it-drift för lämpliga myndigheter. Försäkringskassans uppdrag är därmed begränsat såväl i tid som i omfattning.

Vi menar att det finns fördelar med att tillhandahålla viss samordnad och säker it-drift till den offentliga förvaltningen. Samordnad it-drift kan t.ex. bidra till en enhetlig användning av informationssäkerhetsåtgärder och tillämpning av olika former av

[64] *En gemensam statlig molntjänst för myndigheters it-drift. Delrapport i regeringsuppdrag om samordning och omlokalisering av myndighetsfunktioner*, Statens servicecenter, 7 februari 2017, dnr 10052-2016/1121.
[65] *Uppdrag att erbjuda samordnad och säker statlig it*-drift, regeringsbeslut 24 augusti 2017, Fi2017/03257/DF.

standarder, vilket i sin tur ökar förutsättningarna för interoperabilitet även i andra sammanhang. Samordnad it-drift kan emellertid också föra med sig vissa informationssäkerhetsmässiga risker om myndigheters informationshantering koncentreras både organisatoriskt, tekniskt och fysiskt till en och samma aktör. Sådana risker behöver identifieras och omhändertas om en sådan samordning kommer till stånd.

Även med beaktande av de eventuella risker som kan uppstå finns anledning att överväga i vilken omfattning myndigheter i den offentliga förvaltningen borde kunna ansluta sig till en sådan samordnad it-drift som tillhandahålls av en myndighet. Statens servicecenters förslag, som tidigare redogjorts för, omfattar enbart myndigheter i statsförvaltningen. Även Försäkringskassans uppdrag om samordnad och säker it-drift riktas till statliga myndigheter. Enligt vår uppfattning finns det emellertid fördelar att vinna både ur effektivitets- och informationssäkerhetssynpunkt om hela den offentliga förvaltningen, dvs. även kommuner och landsting, skulle erbjudas att ansluta sig till en offentligt tillhandahållen it-drift. Det finns därför anledning att överväga om kommuner och landsting, som ansvarar för en betydande del av den offentliga förvaltningen i landet och därtill hanterar en mängd känslig information, borde ges möjlighet att ansluta sig till en samordnad it-drift.

Vi anser sammantaget att förutsättningarna att tillhandahålla viss samordnad it-drift till den offentliga förvaltningen i stort bör fortsatt övervägas. Det fortsatta arbetet kan t.ex. ta avstamp i Statens servicecenters förslag om en statlig molntjänst och det uppdrag Försäkringskassan har att tillhandahålla samordnad och säker statlig it-drift. Enligt vår uppfattning bör också behovet av författningsreglering avseende en sådan samordnad it-drift övervägas i detta sammanhang. Reglering torde bl.a. ge ökad rättslig tydlighet vad avser förhållandet till upphandlingsregelverket. Här kan som jämförelse nämnas att Statens servicecenters uppdrag att tillhandahålla lönerelaterade tjänster till statliga myndigheter är reglerat.[66]

[66] 1 § förordningen (2012:208) med instruktion för Statens servicecenter och förordningen (2015:665) om statliga myndigheters användning av Statens servicecenters tjänster.

9.7.2 Rättsligt stöd för god informationssäkerhet

Utredningens bedömning: Inom informationssäkerhetsområdet saknas viss reglering som träffar hela den offentliga förvaltningen.

Utredningens förslag: Regeringen ska låta utreda förutsättningarna för att ta fram en kompletterande reglering om informationssäkerhet som omfattar hela den offentliga förvaltningen.

Skälen för utredningens bedömning och förslag

Ett gemensamt förhållningssätt till informationssäkerhet

För att uppnå nödvändig säkerhet och skydd för information och upprätthålla enskildas förtroende för den digitala utvecklingen i hela den offentliga förvaltningen är det enligt vår uppfattning angeläget att etablera ett gemensamt förhållningssätt till informationssäkerhetsfrågorna som omfattar den offentliga förvaltningen i stort. Informationssäkerheten bör som utgångspunkt angripas på ett enhetligt sätt av samtliga myndigheter. Ett mer sammanhållet arbete med informationssäkerhet i den offentliga förvaltningen har potential att effektivisera den digitala utvecklingen i offentlig förvaltning utan att säkerheten åsidosätts. Det gäller inte minst när myndigheter samarbetar i gemensamma utvecklingsarbeten som innefattar informationsutbyte. Myndighetssamverkan i gemensamma utvecklingsarbeten kan t.ex. medföra att de samverkande aktörerna skapar beroenden av varandra i sin informationshantering. För att reducera risker och behålla en god säkerhetsnivå hos alla samverkande myndigheter ser vi det som angeläget att myndigheter vidtar samordnade informationssäkerhetsåtgärder. Frågan är om en för förvaltningen gemensam reglering om informationssäkerhet kan bidra till ett sådant mer sammanhållet informationssäkerhetsarbete?

En kompletterande informationssäkerhetsreglering för offentlig förvaltning

De granskningar av offentlig förvaltnings informationssäkerhet som har genomförts (se kapitel 9.3.3) visar att befintligt regelverk och annat tillgängligt stöd hittills inte har varit ett tillräckligt styrmedel för att hela den offentliga förvaltningen ska arbeta systematiskt och riskbaserat med informationssäkerhet. Exempelvis är den nuvarande avsaknaden av generellt tillämplig reglering för kommun- och landstingssektorn bekymmersam. Det saknas i dagsläget generella möjligheter, annat än med stöd av frivilliga insatser från kommuner eller landsting, att t.ex. fånga upp it-incidenter på ett samlat sätt. Därtill saknas generell möjlighet att genom ändamålsenlig tillsyn bidra till utvecklingen av en god informationssäkerhet i hela den offentliga förvaltningen.

Kommuner och landsting är aktörer som hanterar en stor mängd känslig information och sekretessreglerade uppgifter. Därtill tillhandahåller kommuner och landsting ett stort antal digitala tjänster till enskilda. Det rör sig om t.ex. direktåtkomst till patientjournaler på internet, anmälan om barnomsorg och lärplattformar i skolverksamhet. I syfte att stärka informationssäkerheten i kommun och landsting anser vi att det, även efter bl.a. genomförandet av NIS-direktivet och ikraftträdandet av en ny säkerhetsskyddslag, kommer att vara angeläget att utforma en generellt tillämplig, kompletterande, informationssäkerhetsreglering som omfattar också dessa aktörer.

Utredningen om effektiv styrning av nationella digitala tjänster föreslår i sitt slutbetänkande att regeringen tar fram rättsliga krav för ett systematiskt och riskbaserat informationssäkerhetsarbete för samtliga offentliga myndigheter.[67] Vi ansluter oss till de bedömningar som den utredningen har gjort men anser att det finns skäl för oss att utveckla förslaget ytterligare.

Enligt vår bedömning behövs ett rättsligt styrmedel som utgör ett tydligt incitament för myndighetsledningar att prioritera och ge nödvändiga resurser till arbetet med informationssäkerhet, samtidigt som ledning ges i fråga om vilka åtgärder som behöver vidtas. Ytterligare förvaltningsgemensamma rättsregler kan alltså ge såväl styrning som stöd inom informationssäkerhetsområdet. Vissa generella

[67] SOU 2017:114 kap. 9.

och grundläggande krav på informationssäkerhetsarbetet för hela den offentliga förvaltningen skulle kunna regleras i form av lag. En sådan informationssäkerhetslag, för den offentliga förvaltningen i stort, i kombination med föreskriftsrätt, bör enligt vår uppfattning vara en lämplig form för ytterligare styrning och stöd inom informationssäkerhetsområdet.

En sådan reglering bör enligt vår bedömning innefatta generella och grundläggande krav på myndigheters arbete med informationssäkerhet och krav på rapportering av it-incidenter som kan påverka säkerheten i myndigheters informationshantering. I regleringen kan också ingå befogenhet för utpekad aktör att utöva ändamålsenlig tillsyn över den offentliga förvaltningens informationssäkerhetsarbete.

I syfte att stärka informationssäkerheten i hela den offentliga förvaltningen föreslår vi därför att regeringen låter utreda förutsättningarna för att ta fram en lag om informationssäkerhet som omfattar hela den offentliga förvaltningen.

Konsekvenser av förslaget

En lag om informationssäkerhet har potential att lägga grunden till en fortsatt trygg, innovativ och effektiv utveckling av en digital förvaltning och kan förväntas få positiva effekter både för enskilda och för offentlig förvaltning i stort. Enskilda har befogade krav på att den offentliga förvaltningen håller en tillräckligt hög säkerhet när myndigheternas informationsmängder bearbetas, lagras och kommuniceras. God informationssäkerhet i den offentliga förvaltningen skapar tillit till de digitala tjänster som tillhandahålls enskilda.

En lag om informationssäkerhet har därtill möjlighet att lägga grunden till en mer enhetlig ansats i informationssäkerhetsarbetet inom den offentliga förvaltningen. Ett större mått av enhetlighet ger bättre förutsättningar att t.ex. effektivisera gemensamma utvecklingsarbeten i den offentliga förvaltningen.

Statliga myndigheter är redan i dag ålagda att bedriva ett systematiskt informationssäkerhetsarbete och en ny lag om informationssäkerhet förväntas inte medföra några ytterligare kostnader i detta hänseende. Förslaget har också bäring på kommuner och landsting som i dagsläget saknar motsvarande generellt tillämplig reglering avseendearbete med informationssäkerhet. Det betyder

emellertid inte att kommuner och landsting inte bedriver ett sådant informationssäkerhetsarbete redan i dag. Huruvida en för den offentliga förvaltningen generellt gällande lag om informationssäkerhet kommer att innebära ökade kostnader för kommuner och landsting är svårt att nu uttala sig om. Eventuella kostnader för att uppfylla nya lagkrav kommer dock att behöva ställas i relation till andra, mer oförutsedda, kostnader som kan uppstå till följd av otillräcklig informationssäkerhet i verksamheten.

Förslaget medför möjligen inte minskad brottslighet men högre säkerhet i den offentliga förvaltningen kan förväntas leda till färre angrepp i it-miljön som innebär skada för verksamheten eller till att enskilda individer kränks t.ex. genom att deras personliga information sprids. För generella konsekvenser av våra förslag hänvisas till kapitel 14.2.

10 Tystnadsplikt för privata leverantörer

10.1 Offentlig sektors utkontraktering av it-drift och andra it-baserade funktioner

10.1.1 Innebörden av utkontraktering

Utkontraktering, eller outsourcing som är det mer vardagligt använda begreppet, innebär att en myndighet eller annan aktör via avtal uppdrar åt en utomstående part, privat leverantör eller annan myndighet, att för dennes räkning utföra en eller flera arbetsuppgifter, processer eller funktioner.

Den utkontraktering som närmast är relevant att undersöka för vår utredning rör uppdrag att sköta it-drift, t.ex. lagring av uppgifter i ett datacenter, eller att tillhandahålla andra it-baserade funktioner, t.ex. e-arkiv eller bearbetning av uppgifter i applikationer eller molntjänster.[1] Även storskalig skanning för digitalisering av dokument kan vara exempel på ett uppdrag som lämnas till en privat leverantör att utföra med hjälp av it-baserade funktioner.

Utkontraktering kan också avse mer sammansatta tjänster på så sätt att den privata leverantören inte enbart ska stå för viss stödverksamhet t.ex. it-drift, utan också utföra en arbetsuppgift som snarare rör uppdragsgivarens kärnverksamhet, t.ex. vissa arbetsmoment som journalföring.

Med utkontraktering avses däremot inte köp av varor, t.ex. hårdvara för datorer. Om leverantören också ska sköta drift och

[1] Molntjänster är tjänster som tillhandahålls med nätverksåtkomst och där resursdelning, möjlighet till snabb skalbarhet, självbetjäning och betalning efter användning eller volym är några av de centrala kännetecknen. Se *Molntjänster i staten, en ny generation av outsourcing*, Pensionsmyndigheten, januari 2016, s. 9.

underhåll av hårdvaran ska dock den transaktionen ses som en utkontraktering. När en myndighet anlitar en osjälvständig uppdragstagare[2] för en arbetsuppgift är detta inte att anse som utkontraktering i nu aktuellt avseende eftersom en sådan uppdragstagare inte är en utomstående part, se vidare kapitel 10.4.1.

10.1.2 En kostnadseffektiv förvaltning

Förvaltningsmyndigheter under regeringen ska bedriva sin verksamhet effektivt och hushålla väl med statens resurser.[3] I offentligt bedrivna verksamheter behöver det därför analyseras om alla arbetsuppgifter bör utföras inom den egna organisationen eller om varor och tjänster i stället ska upphandlas. Ett av regeringens mål för digitaliseringen av den offentliga förvaltningen är högre kvalitet och effektivitet i verksamheten. I budgetpropositionen för 2018 aviserade regeringen också en förstärkt styrning och samordning av övergripande it-användning i statsförvaltningen, i syfte att stimulera digitaliseringen av den offentliga förvaltningen.[4]

Riksdagen och regeringen har tidigare gett uttryck för att det är önskvärt att en större del av myndigheternas it-behov tillfredsställs med hjälp av outsourcing.[5] Bakgrunden till detta har angetts vara att förutsättningarna har ökat för myndigheterna att köpa mer färdiga och standardiserade it-tjänster från externa leverantörer i stället för att myndigheterna producerar dessa tjänster på egen hand. Kostnader relaterade till it utgör en betydande del av myndigheternas totala kostnader. Kostnadsbesparingar har därför angetts kunna göras genom att öka inslaget av externt köpta it-tjänster.[6]

Utkontraktering av it-drift och andra it-baserade funktioner har enligt våra iakttagelser kommit att bli allt mer centralt för en kostnadseffektiv och även i övrigt väl fungerande digital förvaltning. It-

[2] En osjälvständig uppdragstagare är en fysisk person som har ett personligt uppdrag hos en myndighet och som har en sådan anknytning till myndigheten att han eller hon kan sägas delta i dennas verksamhet.
[3] 3 § myndighetsförordningen (2007:515).
[4] Prop. 2017/18:1, utg. omr. 2, s. 93 f.
[5] Se finansutskottets betänkande 2011/12:FiU2 s. 30 och regeringens skrivelse *Riksrevisionens granskning av it inom statsförvaltningen och statliga it-projekt*, rskr 2010/11:138. Se även *IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet?* Riksrevisionen, 12 januari 2011, RiR 2011:4.
[6] Se finansutskottets betänkande 2011/12:FiU2 s. 30.

kostnader är i dag det andra största utgiftsslaget i den offentliga förvaltningens verksamhetskostnader. För statsförvaltningen beräknas it-kostnaderna uppgå till mellan 25 och 30 miljarder kronor per år. Omkring 14 till 16 procent av it-verksamheten är utkontrakterad, mätt i andel av de totala it-kostnaderna.[7] För kommuner och landsting saknas motsvarande uppgift om it-kostnadernas storlek och andel utkontrakterad it-verksamhet, men det har nämnts att sammanlagt 45 miljarder kronor läggs på it varje år i myndigheter, kommuner och landsting.[8]

Det finns anledning att framhålla att vi inom ramen för denna rättsligt orienterade utredning utgår från de politiska mål och den inriktning som riksdag och regering givit (se utöver det ovan anförda bl.a. kapitel 6.8 och 9.3.1). Det är emellertid enligt vår mening en naturlig utgångspunkt att inte alla digitala funktioner kan skötas inom varje enskild myndighet när förvaltningen samtidigt ska vara kostnadseffektiv. Vi återkommer till frågor om it-kostnader i kapitel 13.

10.1.3 En lägesbild

Även vårt kartläggningsarbete har visat att flera myndigheter i dag saknar förutsättningar för att inom ramen för den egna verksamheten utveckla ändamålsenliga, säkra och kostnadseffektiva lösningar för it-drift eller andra it-baserade funktioner. Vissa myndigheter utkontrakterar därför driften av sina it-system,[9] antingen enstaka it-funktioner eller hela driftmiljöer, till andra myndigheter eller privata aktörer. Möjligheten att få tillgång till ny kunskap, idéer och innovationer är också faktorer som bidrar till myndigheters behov av att kunna anlita privata leverantörer.

[7] *Myndigheters strategiska it-projekt och it-kostnader, Delrapport it-användningsuppdraget*, Ekonomistyrningsverket, 21 december 2017, P-2017-77 och *Fördjupat it-kostnadsuppdrag, Delrapport 2: Kartläggning av it-kostnader*, Ekonomistyrningsverket, 23 oktober 2015, 2015:58.
[8] Se presentation på e-legitimationsdagen 2018 på www.elegnamnden.se/download/18.769a0b711614b669f29c3/1517927834469/Ardalan_Shekarabi-Digitalt_forst-nu_okar_vi_takten_i_det_offentliga_Sverige.pdf
[9] Med begreppet it-system avses i betänkandet ett system som används för att samla in, lagra, bearbeta och distribuera information med allmänt utformade eller specialanpassade datorprogram och/eller hårdvara.

En allt vanligare företeelse synes också vara att myndigheter utkontrakterar informationshantering till molntjänstleverantörer. Molntjänster kan svara mot temporära behov i verksamheten, t.ex. vid verksamhetstoppar eller vid genomförande av ett visst utvecklingsarbete. En molntjänst kan emellertid också svara mot myndighetens mer långsiktiga behov av tjänster t.ex. kontorsstöd i form av e-post, ordbehandling eller presentationsverktyg.[10]

Privata leverantörer inom it-branschen, inklusive molntjänstleverantörer, använder sig inte sällan av underleverantörer för att genomföra det uppdrag som myndigheten har upphandlat eller på annat sätt avtalat om. Såväl leverantörer som deras underleverantörer kan ha sitt säte utomlands. Även delar av leverantörernas personal kan vara placerade utomlands. Rättsliga bedömningar behöver mot denna bakgrund göras inte bara i förhållande till leverantören, utan också i förhållande till dennes underleverantörer.

10.1.4 Privata utförare av offentligt finansierad verksamhet

I det nu aktuella kapitlet vill vi särskilt markera att vi inte enbart förhåller oss till den offentliga förvaltningen (förvaltningsmyndigheter, domstolar, kommuner och landsting, jfr. kapitel 6.1). Vi behandlar även frågor som rör utkontraktering på initiativ av privata utförare av offentligt finansierad verksamhet, exempelvis privata utförare av skolverksamhet som uppdrar åt en privat leverantör att sköta skolans it-drift.[11] Våra överväganden och förslag i detta kapitel har alltså också bäring på utkontraktering från enskild verksamhet som är offentligt finansierad. När vi fortsättningsvis hänvisar till myndigheters utkontraktering avses också utkontraktering från sådan enskild verksamhet.

[10] *Molntjänster i staten, en ny generation av outsourcing*, Pensionsmyndigheten, januari 2016.
[11] Exempelvis inom sektorerna vård och omsorg samt utbildning överlämnas ofta offentligrättsliga förvaltningsuppgifter till privata utförare.

10.2 Några rättsområden som aktualiseras vid utkontraktering

10.2.1 Inledning

Ett flertal rättsliga frågeställningar uppstår och behöver bedömas när myndigheter står i begrepp att utkontraktera it-drift eller andra it-baserade funktioner till en privat leverantör. De rättsliga frågeställningarna har bäring på möjligheten att åstadkomma en förvaltning som är såväl trygg som innovativ och effektiv.

Vårt huvudsakliga fokus i det nu aktuella kapitlet är överväganden och förslag som rör myndigheters förutsättningar enligt sekretesslagstiftningen att uppdra åt privata leverantörer att sköta myndighetens it-drift eller tillhandahålla andra it-baserade funktioner. Angränsande frågor om säkerhetsskyddslagstiftningen och annan reglering om informationssäkerhet behöver emellertid också belysas. Även dataskyddsregleringen behöver hållas i åtanke vid de förfaranden som utkontraktering innebär, men presenteras här endast kortfattat. Att också arkivlagstiftningen är av betydelse har framgått under vår kartläggning.

10.2.2 Säkerhetsskydd

För de mest skyddsvärda verksamheterna i samhället gäller säkerhetsskyddslagen (1996:627). Säkerhetsskyddslagen ställer krav på särskilda skyddsåtgärder (säkerhetsskydd) för den information som kan påverka rikets säkerhet. Säkerhetsskyddet ska förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Vilka uppgifter som en myndighet ska hålla hemliga med hänsyn till rikets säkerhet avgörs efter en säkerhetsanalys hos respektive myndighet.

Förekommer det vid överväganden om utkontraktering att uppdraget skulle omfatta sekretessbelagda uppgifter som har betydelse för rikets säkerhet ska myndigheten försäkra sig om att uppgifterna inte får ett sämre skydd hos den privata leverantör som uppgifterna kommer att lämnas ut till än vad de skulle ha haft hos myndigheten.

Från och med den 1 april 2018 behöver en myndighet som ska genomföra en utkontraktering som kräver ingående av säkerhetsskyddsavtal också göra en särskild säkerhetsanalys av det aktuella

uppdraget. Myndigheten ska även samråda om den planerade utkontrakteringen med ansvarig tillsynsmyndighet. Tillsynsmyndigheten får förelägga myndigheten att vidta åtgärder eller, under vissa förutsättningar, besluta att utkontrakteringen inte får genomföras.[12]

Säkerhetsskyddslagen har nyligen varit föremål för översyn[13] och en särskild utredare har i uppdrag att överväga kompletterande förslag i säkerhetsskyddslagstiftningen.[14] Utredaren ska bl.a. kartlägga behovet av att förebygga att säkerhetsskyddsklassificerade uppgifter utsätts för risker i samband med utkontraktering och föreslå olika förebyggande åtgärder t.ex. förhandskontroll vid ingående av säkerhetsskyddsavtal och tillståndsprövning. Uppdraget ska redovisas senast den 31 oktober 2018. Våra överväganden och förslag förhåller sig till säkerhetsskyddslagstiftningen i den utsträckning vi nu kan överblicka med hänsyn tagen till att den lagstiftningen är föremål för översyn. Lagstiftningen i fråga står emellertid inte i fokus för vår utredning.

10.2.3 Sekretess

Sekretess kan uppställa hinder mot att en myndighet lämnar ut uppgifter till en privat leverantör, om det innebär att uppgifter som omfattas av sekretess röjs för leverantören.

I förarbetena till den numera upphävda sekretesslagen (1980:100) förordas att om en myndighet anlitar ett enskilt företag för att utföra ett uppdrag och vars personal inte omfattas av sekretesslagen bör myndigheten ställa krav på att det utförande företaget ska sluta avtal om tystnadsplikt med sina anställda.[15] Efter ett beslut från Riksdagens ombudsmän (JO) den 9 september 2014 som handlade om utkontraktering av journalföring till ett privat företag, uppfattas dock rättsläget av flera vara oklart i frågan om en avtalsreglerad tystnadsplikt är tillräcklig och vilka sekretessreglerade uppgifter som kan lämnas ut vid utkontraktering till privata leverantörer.[16] I nämnda beslut kom JO fram till att avtalsreglerad tystnadsplikt och den tystnadsplikt som följer av personuppgiftslagen (1998:204) inte gav tillräckligt skydd

[12] 16 a § säkerhetsskyddsförordningen (1996:633).
[13] *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag*, prop. 2017/18:89.
[14] *Utredningen om vissa säkerhetsskyddsfrågor*, dir. 2017:32.
[15] Regeringens proposition 1981/82:186 *om ändring i sekretesslagen (1980:100) m.m.*, s. 41 f.
[16] JO:s beslut från den 9 september 2014, dnr 3032-2011.

för enskilda, eftersom sådana alternativa tystnadsplikter inte är straffsanktionerade. JO konstaterade att det inte stod klart att ett utlämnande av de sekretessreglerade uppgifterna till företagets anställda kunde ske utan men för den enskilde eller någon närstående till denne. JO:s bedömning var således att det saknades rättsligt stöd för ett utlämnande av de mycket integritetskänsliga och sekretessbelagda uppgifterna. Se vidare kapitel 10.5.1 för en närmare beskrivning av beslutet.

Efter JO:s beslut uppstod en diskussion rörande myndigheters rättsliga möjlighet att utkontraktera tjänster till privata leverantörer (se vidare kapitel 10.5.2). Den diskussionen har lyfts fram även under vårt kartläggningsarbete. Flera myndighetsrepresentanter har framfört att det finns en tvekan kring hur röjandebegreppet i sekretesslagstiftningen ska tolkas. Kan myndigheten lämna ut sekretessbelagda uppgifter utan att uppgifterna röjs för leverantören, genom att ställa upp avtalsvillkor som förhindrar personal hos denne att ta del av myndighetens information?[17] Finns det t.ex. lagringstjänster där leverantören inte behöver få tillgång till myndighetens sekretessreglerade uppgifter? Eller behöver det mer eller mindre alltid finnas möjligheter för leverantörens personal att ta del av myndighetens uppgifter för att t.ex. felsöka, korrigera felaktigheter eller ge annan support? Behöver det finnas en straffsanktionerad och författningsreglerad tystnadsplikt även för leverantörer?

I det följande kommer vi att närmare analysera förutsättningarna för utlämnande av sekretessreglerade uppgifter till leverantörer vid utkontraktering av it-drift och andra it-baserade funktioner. Det finns emellertid anledning att först också kort beskriva några andra rättsområden som aktualiseras vid utkontraktering av it-drift och andra it-baserade funktioner. Den korta presentationen av dessa rättsområden gör dock inte anspråk på att vara fullständig.

10.2.4 Informationssäkerhet

Uppgifter som kan komma att hanteras av privata leverantörer vid utkontraktering av it-drift eller andra it-baserade funktioner kan omfattas av såväl dataskyddslagstiftningen (se kapitel 10.2.5) som av informationssäkerhetsregleringen. Regleringarna utgår emellertid

[17] Jfr *Outsourcing – en vägledning om sekretess och persondataskydd*, eSam, januari 2016 s.16 f.

från olika perspektiv. Ett renodlat informationssäkerhetsperspektiv innebär att all slags information har någon form av skyddsvärde. De säkerhetskrav som finns i dataskyddsförordningen träffar endast personuppgifter.

I kapitel 9 har vi belyst vilka författningar som närmare anger regler om informationssäkerhet, liksom området för viss avsaknad av förvaltningsgemensam reglering. Av kapitlet har bl.a. framgått att alla statliga myndigheter ansvarar för att deras informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Behovet av säkra ledningssystem för informationssäkerhet[18] ska särskilt beaktas.

Det beskrivna ansvaret gäller även när myndighetens information hanteras av en extern aktör.[19] En myndighet som väljer att utkontraktera informationshantering till en utomstående leverantör, privat eller offentlig, behöver säkerställa att leverantören kan leva upp till de informationssäkerhetsmässiga krav som ställs på hanteringen av myndighetens information. Myndigheten behöver också säkerställa att det finns förutsättningar att kontrollera, följa upp och utvärdera leverantörens informationshantering på samma sätt som om myndigheten själv hade hanterat sin information. Har myndigheten tydligt specificerat sina skyddsåtgärder och krav på kontroll och uppföljning i upphandlingsprocessen och därtill formulerat samtliga krav i avtal, finns goda förutsättningar för myndigheten att följa upp leverantörens informationssäkerhetsarbete.

Vi återkommer i det följande till vissa aspekter som närmast avser att säkerställa god informationssäkerhet, även inom ramen för våra överväganden som rör sekretesslagstiftningen. I kapitel 11 återkommer vi också till vikten av uppföljning av avtal med privata leverantörer. Informationssäkerhetslagstiftningen som sådan står dock inte i fokus i det nu aktuella kapitlet.

[18] Ledningssystem för informationssäkerhet är grunden för att bedriva ett systematiskt informationssäkerhetsarbete i en organisation, se kapitel 9.4.1 och www.informationssakerhet.se

[19] 19 § förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och 3 § första stycket MSBFS 2016:1.

10.2.5 Dataskydd

Dataskyddsförordningen[20] gäller inom sitt område generellt för alla personuppgiftsansvariga och i viss omfattning även för personuppgiftsbiträden. Förordningen ställer krav på att den personuppgiftsansvarige ska kunna visa att en behandling av personuppgifter utförs i enlighet med dess bestämmelser.[21] Ur ett säkerhetsperspektiv kan det t.ex. innebära att en personuppgiftsansvarig ska kunna visa att lämpliga tekniska och organisatoriska åtgärder har vidtagits för att upprätthålla rätt nivå av skydd för personuppgifterna. För att identifiera vilka säkerhetsåtgärder som aktualiseras vid behandling av en viss mängd uppgifter behöver den personuppgiftsansvarige göra en analys där hänsyn tas till vilka risker och hot som finns för behandlingen. I dataskyddsförordningen exemplifieras vilka typer av säkerhetshöjande åtgärder det kan röra sig om.[22] Regleringen är också förenad med en sanktionsbestämmelse vid bristande efterlevnad som träffar både personuppgiftsansvariga och personuppgiftsbiträden.[23]

Datainspektionen[24] är tillsynsmyndighet för behandling av personuppgifter. Tillsynen omfattar även kontroll av att personuppgiftsansvariga ser till att en utkontrakterad personuppgiftsbehandling omgärdas av de säkerhetsåtgärder som dess integritetskänslighet kräver. Här finns anledning att framhålla att dataskyddsregleringen också gäller i förhållande till kommuner, landsting och andra aktörer som utför uppdrag inom det offentliga åtagandet och som i övrigt inte omfattas av samma krav på informationssäkerhet som statliga myndigheter gör.

I det följande kommer vi inte närmare att gå in på rättsfrågor om utkontraktering och skydd för personuppgifter. Det finns emellertid ytterligare frågor vid utkontraktering som behöver bedömas utifrån dataskyddsregleringen, t.ex. vad gäller överföring av personuppgifter till s.k. tredje land (utanför EU).

[20] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[21] Artikel 24.1.
[22] Artikel 32.
[23] Artikel 83.4 a.
[24] Datainspektionen byter namn till Integritetsskyddsmyndigheten under 2018.

10.2.6 Arkiv

Som framgått i kapitel 5.9 behöver även arkivregleringen hållas i åtanke vid utkontraktering, inte minst när det gäller frågor om rensning, gallring eller möjlighet att återfå information från leverantören för långtidsbevarande. Vi belyser emellertid inte dessa frågor närmare i detta kapitel där sekretessregleringen står i fokus.

10.3 Gällande rätt om tystnadsplikt

10.3.1 Straffsanktionerad tystnadsplikt

Personal inom såväl allmän verksamhet som privat verksamhet kan omfattas av bestämmelser om tystnadsplikt. Reglering av tystnadsplikt i det allmännas verksamhet finns i offentlighets- och sekretesslagen (2009:400).[25] Bestämmelser om tystnadsplikt för funktionärer inom den privata sektorn finns i allmänhet i de författningar som reglerar den verksamhet i vilken tystnadsplikten gäller (se vidare kapitel 10.3.3).[26] Föreskrifter om tystnadsplikt som följer av offentlighets- och sekretesslagen är förenade med straffansvar för brott mot tystnadsplikt i 20 kap. 3 § brottsbalken. Även i andra författningar än offentlighets- och sekretesslagen förekommer det föreskrifter om tystnadsplikt. En sådan föreskrift är som regel straffsanktionerad i 20 kap. 3 § brottsbalken, förutsatt att det inte i författningen eller på annat håll finns ett särskilt stadgat straff för åsidosättande av föreskriften. Straffansvaret gäller för var och en som röjer en uppgift som han eller hon har skyldighet att hemlighålla enligt lag eller annan författning.

10.3.2 Tystnadsplikt i offentlighets- och sekretesslagen

Enligt 2 kap. 1 § första stycket offentlighets- och sekretesslagen gäller lagens förbud att röja eller utnyttja en uppgift för myndigheter. I andra stycket anges att förbudet också gäller för en person som fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet på grund av anställning eller

[25] En beskrivning av offentlighets- och sekretessregleringen finns i kapitel 4.6.
[26] Exempelvis tystnadsplikt för hälso- och sjukvårdspersonal inom den enskilda hälso- och sjukvården regleras i 6 kap. 12 § patientsäkerhetslagen (2010:659).

uppdrag hos myndigheten, på grund av tjänsteplikt eller på annan liknande grund. Av 2 kap. 2–5 §§ och i bilagan till offentlighets- och sekretesslagen följer att vissa organ som inte är myndigheter ska jämställas med sådana vid tillämpningen av offentlighets- och sekretesslagen.

I offentlighets- och sekretesslagen finns bestämmelser som syftar till att säkerställa skyddet för uppgifter om enskildas personliga eller ekonomiska förhållanden, liksom skyddet för allmänna intressen, vid användning av digitala tjänster och vid utkontraktering av it-drift mellan myndigheter.[27] Bestämmelserna reglerar bl.a. tystnadsplikt hos en myndighet som för någon annans räkning hanterar dennas uppgifter för enbart teknisk bearbetning eller teknisk lagring. För uppgift om enskilds personliga eller ekonomiska förhållanden är sekretessen absolut.[28] För uppgifter som är sekretessreglerade av hänsyn till ett allmänt intresse gäller samma sekretesskydd hos den mottagande myndigheten som hos den myndighet för vars räkning teknisk bearbetning eller lagring sker, s.k. sekundär sekretess. Om den mottagande myndigheten har att tillämpa en primär sekretessbestämmelse på uppgifterna i fråga gäller dock den bestämmelsen oavsett om sekretessen är starkare eller svagare än den sekundära sekretessen.[29]

De ovan beskrivna sekretessbestämmelserna är bara tillämpliga när behandlingen av uppgifterna sker i verksamhet för enbart teknisk bearbetning eller teknisk lagring för annans räkning dvs. enligt 2 kap. 10 § första stycket tryckfrihetsförordningen. Regleringen träffar således bara uppgifter som inte blir allmänna handlingar hos den mottagande myndigheten. Av denna anledning är tystnadsplikt hos den mottagande myndigheten det skydd som aktualiseras för uppgifterna i fråga.

10.3.3 Tystnadsplikt i privat verksamhet

I flera författningar har tystnadsplikt reglerats specifikt för privata utförare. Här kan bl.a. nämnas tystnadsplikt för den som är eller har varit verksam i enskilt bedriven förskola, fritidshem eller förskoleklass, tystnadsplikt för den som är eller har varit verksam inom

[27] 11 kap. 4 a § och 40 kap. 5 § offentlighets- och sekretesslagen.
[28] 40 kap. 5 § offentlighets- och sekretesslagen.
[29] 11 kap. 4 a och 8 §§ offentlighets- och sekretesslagen.

yrkesmässigt bedriven enskild verksamhet som avser insatser enligt socialtjänstlagen (2001:453) eller färdtjänstlagen (1997:736) och tystnadsplikt inom den privata hälso- och sjukvården.[30] Gemensamt för regleringen av denna tystnadsplikt är dels att den träffar enskilda verksamheter vars uppdrag omfattas av det offentliga åtagandet gentemot allmänheten, dels att sekretessens föremål är enskilds personliga förhållanden. Bestämmelser om tystnadsplikt i enskild verksamhet som kompletterar offentlighets- och sekretesslagen finns även i flera andra regleringar, t.ex. i viss lagstiftning till skydd för rikets säkerhet.[31] Syftet med tystnadspliktsbestämmelserna är bl.a. att uppgifter som behandlas inte ska få ett sämre skydd när de hanteras i enskild verksamhet än när motsvarande hantering sker hos en myndighet.

Det finns också exempel på tystnadsplikt som träffar privat sektor och som inte har någon motsvarighet i det allmännas verksamhet. Det rör sig ofta om skydd för uppgifter som lämnas till personer i olika slag av förtroendeställning t.ex. tystnadsplikt för revisorer och den tystnadsplikt som följer av den s.k. banksekretessen.[32]

Vid tolkning av bestämmelserna om tystnadsplikt i speciallagstiftningen kan ledning sökas i offentlighets- och sekretesslagens motsvarande bestämmelser. Utgångspunkten är att det ska vara en nära överensstämmelse vad gäller innebörden av de olika bestämmelserna om tystnadsplikt för offentlig respektive enskild verksamhet. Privata utförare i vars verksamhet tystnadsplikt råder bör därför ha samma möjligheter att utkontraktera it-drift och andra it-baserade funktioner som offentliga aktörer som verkar inom samma område. Syftet är t.ex. att en enskild vårdgivare ska kunna lämna ut uppgifter i samma utsträckning som en offentlig vårdgivare.[33]

[30] 29 kap. 14 § skollagen (2010:800), 15 kap. 1 § socialtjänstlagen (2001:453), 15 § färdtjänstlagen (1997:736) och 6 kap. 12–14 och 16 §§ patientsäkerhetslagen.
[31] 16 § elberedskapslagen (1997:288), 29 § skyddslagen (2010:305), 11 kap. 65 § plan- och bygglagen (2010:900) och förslag till 5 kap. 1 och 2 §§ ny säkerhetsskyddslag, prop. 2017/18:89.
[32] 26 § revisorslagen (2001:883) och 1 kap. 10 § lag (2004:297) om bank och finansieringsrörelse.
[33] Se bl.a. Proposition 1980/81:28 *om följdlagstiftning till den nya sekretesslagen i fråga om hälso- och sjukvården samt den allmänna försäkringen*, s. 23 och 28, prop. 1981/82:186 s. 26 och *Sekretessfrågor – Skyddade adresser, m.m.*, prop. 2005/06:161, s. 82 och 93.

10.3.4 Tystnadsplikt i dataskyddsregleringen

I den upphävda datalagen (1973:289) reglerades att registeransvarig (numera personuppgiftsansvarig) eller annan som tagit befattning med personregister eller med uppgifter som samlats in för att ingå i sådant register inte obehörigen får röja vad han till följd därav fått veta om enskilds personliga förhållanden.[34] Tystnadsplikten, som var förenad med straffansvar, träffade således både personuppgiftsansvarig och den eventuella aktör som den personuppgiftsansvarige anlitat för att ha hand om den praktiska bearbetningen av registret (personuppgiftsbiträde).[35]

Tystnadsplikten i datalagen fördes inte över till personuppgiftslagen (1998:204). Av 30 § personuppgiftslagen följer i stället en mer allmänt hållen bestämmelse om tystnadsplikt, t.ex. för den som är anställd hos ett personuppgiftsbiträde, eftersom personuppgifter bara får behandlas i enlighet med den personuppgiftsansvariges instruktioner. Bestämmelsen medför emellertid inte att det nämnda straffstadgandet om brott mot tystnadsplikt i 20 kap. 3 § brottsbalken kan bli tillämpligt.[36]

I dataskyddsförordningen regleras tystnadsplikt för personuppgiftsbiträden i artikel 28.3 b. Av bestämmelsen framgår att ett personuppgiftsbiträdes behandling av uppgifter ska regleras i ett avtal eller i en rättsakt som särskilt ska föreskriva att personuppgiftsbiträdet säkerställer att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt. Personuppgiftsbiträden omfattas därmed av krav på tystnadsplikt enligt unionsrätten.

När det gäller nödvändig behandling av känsliga personuppgifter på områdena hälso- och sjukvård och social omsorg har frågan om krav på tystnadsplikt varit föremål för diskussion. Enligt artikel 9.1 i dataskyddsförordningen är det förbjudet att behandla särskilda kategorier av personuppgifter (känsliga personuppgifter), t.ex. uppgifter om hälsa. Från förbudet finns emellertid vissa undantag bl.a. när det gäller områdena hälso- och sjukvård och social omsorg (artikel 9.2 h). Av artikel 9.3 i dataskyddsförordningen framgår att en förutsättning för att känsliga personuppgifter ska få behandlas i verksamheter på

[34] 13 § datalagen.
[35] *Kungl. Maj:ts proposition med förslag till ändringar i tryckfrihetsförordningen m.m.*, prop. 1973:33 s. 140.
[36] *Personuppgiftslag*, prop. 1997/98:44, s. 91.

områdena hälso- och sjukvård och social omsorg är att personuppgifterna behandlas av eller under ansvar av en yrkesutövare eller av en annan person som omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ. Datainspektionen har ansett att det bör utredas om den behandling av personuppgifter som i dag sker inom hälso- och sjukvård och social omsorg är förenlig med artikel 9.2 h och 9.3 i dataskyddsförordningen eller om det behöver införas en lagstadgad tystnadsplikt för de personuppgiftsbiträden som i dag inte omfattas av en sådan. [37]

Dataskyddsutredningen har inte föreslagit någon särskild reglering av tystnadsplikt, utan menat att eftersom artikel 9.3 i dataskyddsförordningen är direkt tillämplig får den närmare innebörden av kravet på tystnadsplikt ytterst uttolkas av EU-domstolen.[38] I propositionen *Ny dataskyddslag* anförde regeringen att frågan om behov av tystnadsplikt utöver den som gäller för den offentliga sektorn enligt offentlighets- och sekretesslagen och den som gäller för privata utförare enligt bl.a. patientsäkerhetslagen (2010:659) och socialtjänstlagen, bör övervägas i samband med anpassningen till dataskyddsförordningen av den sektorslagstiftning som finns på hälso- och sjukvårdsområdet. Regeringen ansåg emellertid att en bestämmelse om att känsliga personuppgifter på områdena hälso- och sjukvård och social omsorg får behandlas om behandlingen är nödvändig, bör erinra om att sådan behandling endast får ske under förutsättning att kravet på tystnadsplikt i artikel 9.3 i dataskyddsförordningen är uppfyllt.[39]

I den senare lagrådsremissen *Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning* bedömde regeringen att kravet på tystnadsplikt i artikel 9.3 inte avser personuppgiftsbiträde. Regeringen ansåg att syftet med artikeln får antas vara att de personer i bl.a. hälso- och sjukvårdsverksamhet som behandlar känsliga personuppgifter ska ha tystnadsplikt enligt t.ex. nationell rätt, eller i vart fall arbeta under någon som har sådan tyst-

[37] Skrivelsen *Vissa frågor om sekretess med anledning av EU:s dataskyddsreform*, Datainspektionen, den 7 juli 2017, dnr 1704-2017.
[38] *Ny dataskyddslag, Kompletterande bestämmelser till EU:s dataskyddsförordning*, (SOU 2017:39), s. 185 f.
[39] *Ny dataskyddslag*, prop. 2017/18:105 s. 92 f. och 3 kap. 5 § förslag till lag med kompletterande bestämmelser till EU:s dataskyddsförordning.

nadsplikt. Ett personuppgiftsbiträde torde inte anses utföra personuppgiftsbehandlingen för ett hälsorelaterat syfte, utan ska endast behandla personuppgifter för den personuppgiftsansvariges räkning. Biträdet torde därmed inte heller anses omfattas av kravet på yrkesmässig tystnadsplikt i den mening som avses i artikel 9.3. Regeringen konstaterade sedan att bestämmelser om tystnadsplikt för personer verksamma inom hälso- och sjukvården och social omsorg redan finns i 25 och 26 kap. offentlighets- och sekretesslagen, 6 kap. 12–14 och 16 §§ patientsäkerhetslagen, 15 kap. socialtjänstlagen och 29 § lagen (1993:387) om stöd och service till vissa funktionshindrade. Avslutningsvis anförde regeringen att frågan om behov av att ändra i lagstiftningen till följd av det ställningstagande som JO gjort i beslutet från den 9 september 2014[40] inte primärt bedöms vara en fråga som rör dataskyddsförordningen.[41]

10.3.5 Tystnadsplikt i säkerhetsskyddslagen

Det har hittills inte funnits några särskilda bestämmelser i säkerhetsskyddslagen som reglerar tystnadsplikt för utomstående leverantörer vid utkontraktering av drift eller andra liknande tjänster. Tystnadsplikt regleras i stället i avtal. Säkerhetsskyddslagen är emellertid som tidigare nämnts föremål för översyn och regeringen föreslog i februari 2018 en ny säkerhetsskyddslag som med ikraftträdande den 1 april 2019.[42] Där föreslås bl.a. en utvidgning av tillämpningsområdet så att fler verksamheter och funktioner samt mer information ska bedömas vara säkerhetskänslig. Vidare föreslås två nya bestämmelser om tystnadsplikt.[43] Den ena bestämmelsen om tystnadsplikt gäller för enskilda verksamhetsutövare som har fått del av uppgifter som lämnats ut för säkerhetsprövning. Den andra bestämmelsen om tystnadsplikt gäller för den som på grund av anställning eller på annat sätt deltar eller har deltagit i säkerhetskänslig verksamhet och som där fått kännedom om säkerhetsskyddsklassificerade uppgifter.

[40] Dnr 3032–2011.
[41] Lagrådsremissen *Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning*, den 8 februari 2018, s. 100 f.
[42] *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag*, prop. 2017/18:89.
[43] Förslag till 5 kap. 1 och 2 §§ ny säkerhetsskyddslag.

10.4 Sekretessöverväganden vid utkontraktering

10.4.1 Osjälvständiga uppdragstagare

I 2 kap. offentlighets- och sekretesslagen anges en närmare avgränsning av vilka organ som omfattas av sekretessregleringen och vilka personer, knutna till dessa organ, som ska följa reglerna (personkretsen). En fysisk person som på grund av uppdrag eller på annan liknande grund deltar i myndighetens verksamhet omfattas av samma tystnadsplikt som myndighetens anställda.[44] För att en person som agerar i rollen som uppdragstagare mot myndigheten ska omfattas av personkretsen krävs att denne är en s.k. osjälvständig uppdragstagare. En osjälvständig uppdragstagare är en fysisk person som har ett personligt uppdrag hos en myndighet och som har en sådan anknytning till myndigheten att han eller hon kan sägas delta i dennas verksamhet. Det innebär att uppdragstagare som primärt representerar enskilda rättssubjekt faller utanför bestämmelsens tillämpningsområde.

Offentlighets- och sekretesslagen gäller alltså i princip inte för den som är anställd hos ett företag som i sin tur har ett uppdragsavtal med en myndighet. I förarbetena till den tidigare gällande sekretesslagen anges dock att om en myndighet har träffat avtal med ett enskilt företag, kan det i undantagsfall te sig naturligt att arbetstagare hos företaget får lyda under lagens bestämmelser, nämligen då arbetstagaren ställs till myndighetens förfogande och deltar i dess verksamhet på samma sätt som om myndigheten hade ingått uppdragsavtal med vederbörande själv.[45] Med avseende på sådana situationer omfattas även den som på *annan liknande grund* deltar i myndighets verksamhet av personkretsen.

Gränsen för när en person ingår i personkretsen eller inte kan i praktiken vara svår att dra. Utredningens kartläggning tyder på att det finns en osäkerhet hos myndigheterna om vilka förutsättningar som behöver vara för handen för att en person ska anses ingå i personkretsen enligt offentlighets- och sekretesslagen. Vid utkontraktering till privata leverantörer ställs dock i regel inte en *enskild* fysisk person hos leverantören till den utkontrakterande myndighetens förfogande och deltar i verksamheten på samma sätt som om myndigheten hade ingått uppdragsavtal med den enskilde själv.

[44] 2 kap. 1 § andra stycket offentlighets- och sekretesslagen.
[45] *Regeringens proposition med förslag till sekretesslag m.m.*, prop. 1979/80:2 Del A, s. 128.

I dessa fall omfattas inte leverantörens personal av offentlighets- och sekretesslagen.

10.4.2 Utlämnande utan röjande av sekretessbelagda uppgifter

Om det finns rättsliga förutsättningar för att under vissa omständigheter lämna ut sekretessbelagda uppgifter utan att ett röjande av uppgifterna faktiskt sker är omtvistat.

Sekretess innebär ett förbud mot att röja uppgifter oavsett om det görs muntligen, genom utlämnande av allmän handling eller på något annat sätt.[46] Förbudet att röja uppgifter träffar varje form av röjande. Att en uppgift inte får röjas betyder att den inte får berättas vidare eller att den allmänna handlingen där uppgiften förekommer inte får lämnas ut. Otillåtet röjande av en sekretessbelagd uppgift är enligt 20 kap. 3 § brottsbalken straffsanktionerat. Ordet röja bör enligt kommentaren till brottsbalken ha samma betydelse i straffbestämmelsen som i offentlighets- och sekretesslagens bestämmelse. Ett röjande sker när uppgift eller allmän handling som omfattas av sekretess lämnas ut. Enligt kommentaren finns inget krav på att ett avslöjande faktiskt ska ha skett.[47] Stöd för denna bedömning finns enligt kommentaren i uttalanden från regeringen och lagrådet i förarbetena till vissa ändringar i 20 kap. 3 § brottsbalken i samband med sekretesslagens tillkomst.[48]

Enligt E-delegationens och eSamverkansprogrammets (eSam)[49] mening finns det däremot skäl att överväga en mer nyanserad tolkning av offentlighets- och sekretesslagens röjandebegrepp, i vart fall när det gäller utkontraktering av vissa tekniska arbetsuppgifter såsom it-drift, skanning eller kommunikationstjänster. Avsikten med att uppgifterna görs tillgängliga vid sådan utkontraktering är inte att mottagaren ska tillgodogöra sig informationsinnehållet, utan syftet är att mottagaren tekniskt ska bearbeta eller lagra informationsmängden. I sådana situationer kan det enligt denna mening vara

[46] 3 kap. 1 § offentlighets- och sekretesslagen.
[47] Nils-Olof Berggren m.fl. Brottsbalken (10 november 2017, Zeteo), kommentaren till 20 kap. 3 § brottsbalken.
[48] Prop. 1979/80:2 del A s. 402 f. och s. 488.
[49] eSam är ett medlemsdrivet program för samverkan mellan 21 myndigheter och SKL och är en frivillig fortsättning efter E-delegationen. Samarbetet syftar till att underlätta och påskynda digitaliseringen av det offentliga Sverige, se mer på www.esamverka.se.

möjligt och lämpligt att i avtal införa krav på tekniska och rättsliga begränsningar som hindrar utföraren och utförarens personal från att faktiskt ta del av eller vidarebefordra de uppgifter som myndigheten har gjort tillgängliga genom utkontrakteringen.[50]

I förarbetena till den tidigare sekretesslagen beskrivs innebörden av röjandeförbudet på ett sätt som skulle kunna indikera att ett röjande inte bara innebär att befattningshavaren gör uppgiften tillgänglig för annan, utan också att mottagaren förutsätts ta del av uppgiften i fråga eller åtminstone har rätt att göra det.[51] Förespråkare för att ett utlämnande i de nu aktuella situationerna kan äga rum utan att ett röjande sker menar att det också finns stöd för denna uppfattning i rättsfallet NJA 1991 s. 103. I rättsfallet behandlas innebörden av uttrycket röjer uppgift i 19 kap. 9 § brottsbalken (vårdslöshet med hemlig uppgift). Rättsfallet kan enligt kommentaren till offentlighets- och sekretesslagen vara vägledande också vid tillämpningen av offentlighets- och sekretesslagen och brott mot tystnadsplikt.[52] Högsta domstolen uttalade följande.

> Uttrycket ”röjer uppgift” i bestämmelsen innebär enligt vanligt språkbruk att en uppgift avslöjas eller uppenbaras. Detta förutsätter att det finns någon person, för vilken uppgiften görs tillgänglig. Det torde dock inte alltid kunna krävas att denne faktiskt har fått kännedom om uppgiften. Det bör sålunda som regel vara tillräckligt att en handling med hemliga uppgifter har kommit i någon obehörigs besittning. Även vissa andra, närliggande situationer bör omfattas. Däremot kan inte varje möjlighet att ta del av en uppgift, som har beretts någon obehörig, medföra att uppgiften skall anses ha röjts; en sådan ordning skulle i realiteten innebära att det oaktsamma handlandet i sig ofta skulle medföra straffansvar. Avgörande för straffansvar bör främst vara om uppgiften har blivit tillgänglig för någon obehörig under sådana omständigheter, att man måste räkna med att den obehörige kommer att ta del av uppgiften.

Rättsfallet kan innebära att straffansvar för sekretessbrott inte skulle komma i fråga om uppgifter gjorts tillgängliga för en leverantör under sådana omständigheter att myndigheten inte har anledning att räkna med att denne eller någon annan obehörig kommer att ta del av uppgifterna. I ett rättsligt uttalande från aktörer i eSam framförs

[50] *En förvaltning som håller ihop* (SOU 2015:66), s. 47 f. och *Outsourcing – en vägledning om sekretess och persondataskydd*, eSam, januari 2016, s.16 f.
[51] Prop. 1979/80:2 del A s. 119.
[52] Eva Lenberg m.fl., Offentlighets- och sekretesslagen (24 november 2017, Zeteo), kommentaren till 3 kap. 1 § offentlighets- och sekretesslagen.

att det inte ska anses vara ett röjande i offentlighets- och sekretesslagens mening, om uppgifter görs tekniskt tillgängliga för en leverantör som enligt ett avtal inte får ta del av eller vidarebefordra uppgifterna och omständigheterna i övrigt medför att det är osannolikt att detta ändå sker. Det har emellertid framhållits i en vägledning avseende aktuell fråga att rättsläget ännu inte kan anses vara klarlagt när det gäller möjligheten att lämna ut sekretessbelagda uppgifter utan att ett rättsligt röjande av uppgifterna sker.[53]

Flera myndighetsrepresentanter har under vår kartläggning gett uttryck för osäkerhet kring det beskrivna förfarandet eftersom frågan inte är prövad av domstol. En sådan osäkerhet kring tolkningen av röjandebegreppet framkom även under remissförfarandet avseende E-delegationens slutbetänkande *En förvaltning som håller ihop*, där delegationen presenterade sin tolkning av röjandebegreppet.[54]

Det finns också skäl som talar för att det är tveksamt om sekretessbelagda uppgifter kan lämnas ut till en leverantör utan att ett röjande av uppgifterna sker. Detta gäller oavsett om det endast är ett s.k. tekniskt tillgängliggörande av uppgifter och att leverantörens personal har förbjudits i avtal att ta del av eller vidarebefordra informationen. Kommentaren till brottsbalken anger att det alltid är ett röjande att göra en uppgift tillgänglig för någon annan, oavsett om det sker ett faktiskt avslöjande av informationen. Enligt vår bedömning bör också viss försiktighet iakttas avseende att hämta ledning i Högsta domstolens resonemang i det angivna rättsfallet, eftersom resonemanget där avser gränsdragningen för straffansvar. Enligt förarbetena till den tidigare sekretesslagen föreligger det nämligen en viss marginal mellan det handlingsutrymme som följer av rekvisitens utformning i sekretesslagen och området där ansvar för sekretessbrott inträder.[55]

I sammanhanget kan även nämnas Transportstyrelsens rapport till regeringen om hur myndigheten har hanterat vissa skyddsvärda uppgifter i sina it-system i samband med utkontraktering av it-drift till en privat leverantör under tidsperioden maj 2015 – oktober 2017. I rapporten analyseras om sekretessbelagda uppgifter har röjts för

[53] *Röjandebegreppet enligt offentlighets- och sekretesslagen*, eSams rättliga uttalande, den 17 december 2015, dnr/ref. VER 2015-190 och *Outsourcing – en vägledning om sekretess och persondataskydd*, eSam, januari 2016, s. 16 f.
[54] Se t.ex. Livsmedelsverkets remissyttrande över betänkandet *En förvaltning som håller ihop* (SOU 2015:66), den 14 december 2015, dnr 2015/07920.
[55] Prop. 1979/80:2 del A s. 85.

obehöriga. Transportstyrelsens slutsats är att de i det pågående och fortsatta säkerhetsarbetet betraktar samtliga hemliga uppgifter som har varit tillgängliga för obehöriga som i formell mening röjda även om det inte förekommer några indikationer på att uppgifterna kommit i orätta händer. Vidare har Transportstyrelsen redovisat att ingen av de myndigheter[56] som Transportstyrelsen enligt uppdraget skulle samråda med, har framfört att de har indikationer på att den röjda informationen skulle ha kommit i orätta händer, utan att de har sett sig tvingade att vidta åtgärder i förebyggande syfte eftersom uppgifterna betraktas som röjda.[57]

Se vidare i kapitel 10.6.1 om utredningens överväganden i frågan.

10.4.3 Utlämnande av sekretessbelagda uppgifter med stöd av förbehåll

Offentlighets- och sekretesslagen innehåller bestämmelser om undantag från sekretess. Bestämmelsen om utlämnande av uppgift med förbehåll (10 kap. 14 § offentlighets- och sekretesslagen) möjliggör för myndigheter att i förhållande till en enskild lämna ut uppgifter som är sekretessbelagda enligt en sekretessbestämmelse som har ett skaderekvisit. Ett utlämnande av uppgifterna kan ske under förutsättning att den risk för skada, men eller annan olägenhet som hindrar att uppgifterna lämnas till den enskilde kan undanröjas genom förbehållet. Uppgifter som omfattas av absolut sekretess[58] kan därmed inte lämnas ut med förbehåll. Ett förbehåll kan t.ex. avse ett förbud mot att lämna uppgifterna vidare eller utnyttja dem. Förbehållet medför att tystnadsplikt uppkommer för den som tagit emot uppgifterna som inskränker rätten att meddela och offentliggöra uppgifterna (meddelarfrihet). Ett röjande av uppgifterna kan medföra straffansvar för brott mot tystnadsplikt.

Det finns emellertid avsevärda begränsningar kring hur och när ett förbehåll får ställas upp. För det första får ett förbehåll inte meddelas i förväg utan ska föregås av en prövning i varje särskilt fall

[56] Försvarsmakten, Säkerhetspolisen, Försvarets radioanstalt, Polisen, Post- och telestyrelsen, Myndigheten för samhällsskydd och beredskap, Datainspektionen och Skatteverket.
[57] *Kartlägga hanteringen av vissa uppgifter*, Transportstyrelsen, 23 januari 2018, dnr TSG 2017-2515, s. 10 f.
[58] Sekretessbestämmelser som saknar skaderekvisit, vilket innebär att de uppgifter som omfattas av bestämmelsen ska hemlighållas utan någon skadeprövning om uppgifterna begärs ut.

och avse konkreta uppgifter. För det andra ska ett förbehåll meddelas som ett formligt beslut, dvs. det ska dokumenteras och innehålla en överklagandehänvisning. För det tredje ska uppgiftsutlämnandet ske till en utpekad fysisk person. Det går alltså inte att i avtal reglera generella förbehåll.[59]

Det har under kartläggningen framkommit att bestämmelsen om förbehåll i de flesta fall inte kan tillämpas vid utkontraktering av tjänster till privata leverantörer på grund av de begränsningar som finns för när utlämnande av uppgift med förbehåll är möjligt.

10.4.4 Nödvändigt utlämnande av sekretessbelagda uppgifter

Offentlighets- och sekretesslagen innehåller även ett antal sekretessbrytande bestämmelser som tillåter att en uppgift röjs trots att den är sekretessbelagd. En sekretessbrytande bestämmelse som myndigheter kan tillämpa vid utlämnande av uppgifter till privata leverantörer är bestämmelsen om nödvändigt utlämnande (10 kap. 2 § offentlighets- och sekretesslagen). Bestämmelsen innebär att sekretess inte hindrar att en myndighet lämnar ut en uppgift om det är nödvändigt för att myndigheten ska kunna fullgöra sin verksamhet. Av förarbetena framgår emellertid att bestämmelsen ska tillämpas restriktivt. Det är inte tillräckligt att myndighetens arbete blir mer effektivt.[60] JO har i ett flertal ärenden haft anledning att resonera kring bestämmelsens räckvidd och anser att det handlar om situationer av undantagskaraktär.[61]

Andra menar att röjande av uppgifter i samband med sådan utkontraktering som sker i syfte att dra nytta av utförarens expertkompetens eller tekniska utrustning i särskilda fall kan anses utgöra ett sådant nödvändigt utlämnande som kan ske utan hinder av sekretess. Som exempel på sådan utkontraktering nämns it-support, storskalig skanning av dokument, it-drift och e-arkivering.[62] Denna tolkning synes göras utifrån ett uttalande i de ursprungliga för-

[59] Se bl.a. JO 1992/93:JO1 s. 197, dnr 145-90, JO 1994/95:JO1 s. 574, dnr 2079-1993 och JO 2009/10:JO1 s. 194, dnr 4150-2007.
[60] Prop. 1979/80:2 Del A s. 465 och 494.
[61] Se t.ex. JO 1982/83:JO1 s. 238, dnr 149-1980, JO 1984/85:JO1 s. 265, dnr 2616-1983 och JO:s beslut den 9 september 2014, dnr 3032-2011.
[62] *Outsourcing – en vägledning om sekretess och persondataskydd*, eSam, januari 2016, s. 27 f.

arbetena till sekretesslagen om att det i särskilda fall kan vara nödvändigt för en tjänsteman att vända sig till en utomstående expert och upplysa denne om hemliga omständigheter.[63] Detta resonemang fördes även i E-delegationens slutbetänkande,[64] vilket möttes av invändningar av några remissinstanser som ansåg att delegationens tolkning var mer vidsträckt än vad uttalanden från JO och förarbetsuttalanden gav stöd för.[65] Det är också enligt vår bedömning långtgående att hitta stöd för en sådan tolkning i ovan nämnda förarbetsuttalande. Bestämmelsens ordalydelse i ljuset av förarbetsuttalandena om att bestämmelsen ska tillämpas restriktivt tyder på att det är fråga om fall då det inte finns någon annan realistisk utväg för myndigheten att fullgöra en arbetsuppgift. Se vidare i kapitel 10.6.1 om utredningens överväganden i frågan.

I våra kontakter med myndigheter med anledning av kartläggningsarbetet framkommer att det finns en betydande tveksamhet inför att lämna ut uppgifter till privata leverantörer med stöd av den aktuella bestämmelsen. Det bör även framhållas att uppgifter som lämnas ut med stöd av bestämmelsen inte heller får samma skydd hos leverantören, eftersom de medarbetare hos leverantörerna som tar del av uppgifterna inte omfattas av en författningsreglerad tystnadsplikt.

10.4.5 Avtalsreglerad tystnadsplikt

En civilrättsligt avtalsreglerad tystnadsplikt är sedan länge gängse vid kommersiella avtalsförhållanden mellan myndigheter och privata leverantörer. Avtalet innehåller ofta krav på att medarbetare hos leverantören undertecknar individuella sekretessförbindelser där de förbinder sig att inte avslöja eller på annat sätt sprida sekretessreglerade uppgifter som de tar del av när de utför sina arbetsuppgifter. Medarbetarnas sekretessförbindelser gäller emellertid enbart i förhållande till arbetsgivaren. Eventuella sanktioner som påförs en medarbetare som brustit i sitt sekretessåtagande beslutas och verkställs således av arbetsgivaren. En avtalsreglerad tystnadsplikt innebär dock inte att ansvar kan uppkomma för brott mot tystnadsplikt.

[63] Prop. 1979/80:2 Del A, s. 122.
[64] SOU s. 2015:66 s. 48 f.
[65] Se bl.a. Livsmedelsverkets remissyttrande, den 14 december 2015, dnr 2015/07920 och Transportstyrelsens remissyttrande, den 14 december 2015, dnr TSG 2015-1422.

Traditionellt sett har den avtalsreglerade tystnadsplikten ofta ansetts innebära att myndigheten vid skadeprövningen kan komma fram till att de sekretessreglerade uppgifterna inte omfattas av sekretess i förhållande till de privata leverantörerna och därför kan lämnas ut till dem. I förarbetena till äldre sekretesslagen framgår att behov av tystnadsplikt för andra personkategorier än de som omfattas av sekretesslagens tillämpningsområde får tillgodoses genom lagstiftning vid sidan av sekretesslagen eller i rent civilrättslig ordning, eventuellt genom avtal om tystnadsplikt.[66] Det finns således en bakgrund till att en avtalsreglerad tystnadsplikt har beskrivits vara i de allra flesta fall tillräcklig för att skaderekvisitet inte ska anses vara uppfyllt vid skadeprövningen gällande sekretessreglerade uppgifter som varit av mindre integritetskänsligt slag. Det betyder att sekretess i det enskilda fallet inte har ansetts gälla gentemot den privata leverantören och att uppgifterna därför har lämnats ut i samband med utkontraktering.[67]

Vårt kartläggningsarbete och samlade erfarenhet talar för att myndigheter regelmässigt reglerar tystnadsplikt i avtal vid utkontraktering till privata leverantörer. Kartläggningsarbetet har emellertid också visat att det finns en påtaglig osäkerhet hos myndigheter om i vilken utsträckning en avtalsreglerad tystnadsplikt nu och framöver ska anses vara tillräcklig för att uppgifterna inte ska anses omfattas av sekretess i det enskilda fallet och därmed kunna lämnas ut till en privat leverantör.

10.5 Behovet av en författningsreglerad tystnadsplikt för privata leverantörer

10.5.1 JO:s beslut

Behov av en författningsreglerad tystnadsplikt för privata leverantörer började diskuteras mer intensivt i samband med att JO riktade allvarlig kritik mot vissa vårdgivare för att de ingått avtal om journalföring med ett företag trots att detta inte varit förenligt med regelverket om sekretess inom hälso- och sjukvården.[68] Beslutet rörde två vårdgivare (tillika personuppgiftsansvariga) som ingått

[66] Prop. 1979/80:2 Del A s. 128.
[67] *Outsourcing – en vägledning om sekretess och persondataskydd*, eSam, januari 2016, s. 21 f.
[68] JO:s beslut från den 9 september 2014, dnr 3032-2011.

avtal med ett företag (tillika personuppgiftsbiträde) om journalföring av patientuppgifter. Journalföringen skulle utföras av läkarsekreterare som var anställda av företaget. Läkarsekreterarna hade en avtalsreglerad tystnadsplikt i förhållande till sin arbetsgivare (företaget). För patientuppgifter[69] råder stark sekretess[70] och JO konstaterade inledningsvis att läkarsekreterarna inte omfattades av tystnadsplikt vare sig enligt offentlighets- och sekretesslagen eller patientsäkerhetslagen. De alternativa tystnadsplikter som följde dels av avtal, dels av personuppgiftslagen menade JO inte var tillräckliga för att ett utlämnande kunde ske utan att det innebär men för den som skyddades av sekretessen. Vid bedömningen av betydelsen av de alternativa tystnadsplikterna beaktade JO det förhållandet att vårdgivarens egen personal, som omfattades av författningsreglerad tystnadsplikt, kunde dömas för brott mot tystnadsplikt om en sekretessbelagd uppgift felaktigt röjs. För läkarsekreterarna som främst var bundna av en avtalsreglerad tystnadsplikt saknades straffrättslig sanktionsmöjlighet.

I kölvattnet av JO-beslutet uppstod som tidigare nämnts en rättslig diskussion om när och under vilka omständigheter myndigheter kan lämna ut sekretessreglerade uppgifter till privata aktörer. Diskussionen har också gällt frågan om det finns behov av författningsreglerad tystnadsplikt för privata leverantörer av bl.a. it-drift och andra it-baserade funktioner. Diskussionen kom främst att kretsa kring om sekretessregleringen och avsaknaden av en författningsreglerad tystnadsplikt för anställda hos leverantörer hindrar myndigheter från att utkontraktera verksamhet och använda molntjänster.[71] Även förhållandet om läkarsekreterarna kunde anses tillhöra hälso- och sjukvårdspersonal i patientsäkerhetslagens mening och därmed omfattas av tystnadsplikten enligt denna lag diskuterades efter JO-beslutet.[72]

[69] 25 kap. 1 § offentlighets- och sekretesslagen.
[70] Uppgifter som skyddas av ett omvänt skaderekvisit; sekretess för en uppgift gäller om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men, vilket innebär att det finns en presumtion för sekretess.
[71] Se t.ex. Conny Larsson, *Sekretess utgör därmed ett generellt hinder för myndigheter att använda 'molntjänster' inom IT*, den 2 oktober 2014, Dagens Juridik och Daniel Westman, *Nej, advokaten – sekretess utgör inget generellt hinder för molntjänster hos myndigheter*, den 12 november 2014, Dagens Juridik.
[72] Se bl.a. *Sekretess vid outsourcing – en förstudie*, Fi 2009:01/2015/4, 9 mars 2015, s. 61 f.

10.5.2 Behovet av författningsreglerad tystnadsplikt förs fram av olika aktörer

E-delegationen har resonerat kring frågan om sekretess vid utkontraktering, dels i en förstudie som syftade till att klarlägga rättsläget, dels i sitt slutbetänkande.[73] E-delegationen menade att de bedömningar rörande sekretess som en myndighet måste göra inför en planerad utkontraktering i vissa fall kan framstå som komplicerade att utföra och att det finns risk för en oriktig rättstillämpning. Den omständigheten att gällande rätt på området är delvis otydlig kunde vidare enligt E-delegationen medföra en oro för att en rättlig analys vid utlämnande av uppgifter visar sig vara felaktig vid en senare rättslig prövning. E-delegationens slutsats var emellertid att det torde vara mycket få fall av utkontraktering som inte skulle kunna komma till stånd på grund av offentlighets- och sekretesslagens utformning. E-delegationen menade att det på sikt kunde vara önskvärt om regelverket kunde förtydligas i syfte att förenkla förfarandet vid utlämnande av uppgifter till en leverantör, men ansåg inte att det fanns tillräckligt starka skäl att då lämna förslag till författningsändringar.[74] Flera remissinstanser ansåg emellertid att det fanns ett tydligt behov av en skyndsam översyn av regelverket.[75]

Frågan om författningsreglerad tystnadsplikt för privata leverantörer har också uppmärksammats av andra aktörer och utredningar.

Pensionsmyndigheten föreslog i rapporten Molntjänster i staten – en ny generation av outsourcing, att regeringen skulle utreda om det är lämpligt och ändamålsenligt att införa en lagreglerad och

[73] A.a. och *En förvaltning som håller ihop* (SOU 2015:66), kapitel 3.
[74] SOU 2015:66 s. 50.
[75] Se följande remissyttranden över betänkandet *En förvaltning som håller ihop* (SOU 2015:66): CSN:s yttrande, den 7 december 2015, dnr 2015-110-7277, Datainspektionens yttrande, den 10 december 2015, dnr 1618-2015, Livsmedelsverkets yttrande, den 14 december 2015, dnr 2015/07920, Läkemedelsverkets yttrande, den 10 december 2015, dnr 3.4-2015-082897, Länsstyrelsens i Kronobergs län yttrande, den 10 december 2015, dnr 100-4636-15, Naturvårdsverkets yttrande, den 10 december 2015, dnr NV-05786-15, Post- och telestyrelsens yttrande, den 10 december 2015, dnr 15-9487, Region Östergötlands yttrande, den 7 oktober 2015, dnr RS 2015-684, Sjöfartsverkets yttrande, den 2 december 2015, dnr 15-03317, Socialstyrelsens yttrande, den 8 december 2015, dnr 10.1-24014/2015, Sveriges Kommuner och Landstings yttrande, den 27 november 2015, dnr 15/4610, Trafikverkets yttrande, den 1 december 2015, dnr TRV 2015/81121, Transportstyrelsens yttrande, den 14 december 2015, dnr TSG 2015-1422 och Upphandlingsmyndighetens yttrande, den 14 december 2015, dnr UHM/2015-110-1.

straffsanktionerad tystnadsplikt för privata leverantörer av it-tjänster till offentlig sektor, i syfte att underlätta för myndigheter att uppdra åt dessa aktörer att hantera myndighetens sekretessreglerade information.[76]

Av Integritetskommitténs slutbetänkande framgår att kommittén i sina kontakter med myndigheter har fått veta att avsaknaden av tystnadsplikt för leverantörer både ger ett sämre integritetsskydd och försvårar digitaliseringen, genom att det råder tveksamhet om när en myndighet får överlåta åt ett personuppgiftsbiträde att hantera uppgifter. Integritetskommittén har bedömt att det behövs en utökning av tystnadsplikten och har därför föreslagit att regeringen låter utreda hur ett regelverk för tystnadsplikt för leverantörer av molntjänster och andra personuppgiftsbiträden skulle kunna utformas. Förslaget bör dock enligt kommittén utformas så att det utgör en balanserad avvägning mellan tystnadsplikten respektive meddelarfriheten.[77]

Även Datainspektionen har hemställt om att regeringen utreder behovet av att införa en lagstadgad tystnadsplikt för privata leverantörer av it-tjänster.[78]

10.5.3 Vår kartläggning

Vårt kartläggningsarbete har visat att flera representanter för myndigheter och andra aktörer upplever osäkerhet om det i vissa situationer finns rättsligt stöd i sekretesslagstiftningen för att lämna ut uppgifter som omfattas av sekretess i samband med utkontraktering till privata leverantörer. När det gäller frågan om det är möjligt att under vissa omständigheter lämna ut sekretessbelagda uppgifter utan att ett röjande av uppgifterna faktiskt sker, (se kapitel 10.4.2), har flera myndighetsrepresentanter anfört att det råder osäkerhet i frågan, inte minst eftersom den inte är prövad av domstol. Likaså har det framförts tvekan om hur den sekretessbrytande bestämmelsen i 10 kap. 2 § offentlighets- och sekretesslagen ska tolkas och i vilken utsträckning sekretessbelagda uppgifter kan lämnas ut med stöd av bestämmelsen, (se kapitel 10.4.4).

[76] *Molntjänster i staten – en ny generation av outsourcing* s. 76, Pensionsmyndigheten.
[77] *Så stärker vi den personliga integriteten* (SOU 2017:52), s. 140 f.
[78] Skrivelsen *Vissa frågor om sekretess med anledning av EU:s dataskyddsreform*, Datainspektionen, den 7 juli 2017, dnr 1704-2017.

Frågor om förhållandet mellan dataskyddsförordningen och nationella tystnadsplikter har också lyfts fram för oss under kartläggningsarbetet, särskilt vad gäller vård- och omsorgssektorn. Det har även framkommit under kartläggningen att myndigheter har avstått från digitalisering på grund av att de inte själva kan utveckla och hantera driften av ändamålsenliga och kostnadseffektiva tjänster och att det råder osäkerhet kring om det finns rättsliga förutsättningar för att utkontraktera förfarandet. Denna osäkerhet kring lagligheten av viss utkontraktering har bl.a. lett till separata manuella rutiner för intern hantering av ett fåtal sekretessreglerade uppgifter i en större informationsmängd som i övrigt hanteras digitalt av en privat leverantör. Flera myndighetsrepresentanter har påpekat att de generellt är tveksamma till att anlita privata leverantörer om det inte står klart att offentlighets- och sekretesslagen inte hindrar ett utlämnande av de uppgifter som ska hanteras av leverantören och att det finns behov av antingen ett vägledande uttalande i frågan eller en förtydligande reglering.

Det har även framförts till utredningen att avtalen mellan den utkontrakterande myndigheten och den privata leverantören och avtalen mellan leverantören och dess personal kan vara bristfälligt utformade vad avser tystnadsplikt och att man önskar stöd i avtalsarbetet. Det har också framhållits att det finns svårigheter med att följa upp avtalen genom bl.a. kontroll av att villkoren efterlevs, (se vidare i kapitel 11).

10.6 Överväganden och förslag

10.6.1 Behov av klara och tydliga regler

Utredningens bedömning: 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 skulle undanröja en rättslig osäkerhet som nu hindrar eller hämmar digitaliseringen och möjliggöra en effektivare offentlig sektor.

Skälen för utredningens bedömning: Som anförts i kapitel 10.1.3. är utkontraktering av it-drift och andra it-baserade funktioner för flera myndigheter en förutsättning för att verksamheten ska kunna bedrivas ändamålsenligt och kostnadseffektivt. Uppgifter som lämnas ut i samband med utkontraktering kan emellertid vara mycket integritetskänsliga, liksom omfattas av stark eller absolut sekretess. Därtill är det ofta fråga om stora uppgiftssamlingar när it-drift eller andra it-baserade funktioner utkontrakteras.

Flera myndigheter har under kartläggningsarbetet pekat på att det är angeläget att sekretessfrågorna kring utkontraktering av it-drift och andra it-baserade funktioner till privata leverantörer får en tydligare lösning, eftersom rättsläget upplevs som oklart när det gäller rättsliga förutsättningar för att lämna ut sekretessreglerade uppgifter. Även händelser under utredningstiden har visat behov av ett tydligare regelverk kring sådan utkontraktering. Ett exempel är det s.k. Göteborgsfallet där Göteborgs stad tillfälligt avbröt installationen av en molnbaserad tjänst som bl.a. innefattade e-post och dokumentlagring, eftersom man ansåg att det fanns en möjlighet att anställda hos leverantören kunde ta del av uppgifter som skyddas av sekretess. Trots att det huvudsakligen var algoritmer med anknytande datorprogram som hanterade informationen kunde emellertid människor behöva tillgång till uppgifterna, t.ex. för supportärenden. Göteborgsfallet ledde till en diskussion om rättsläget och om informationen skulle anses röjd för leverantörens anställda, varvid andra myndigheter som installerat funktionen gjorde olika bedömningar i frågan. Leverantören bistod sedan med att hänvisa till en teknisk lösning, en s.k. ”Customer Lockbox”, som innebär att innan en anställd hos leverantören får tillgång till informationen ska en chef kontrollera att den anställde har behov av informationen och ge sitt godkännande. Därefter får den utkontrakterande myndigheten göra en sekretessprövning av informationen för att avgöra om den kan lämnas ut till den anställde hos leverantören.[79]

Som beskrivits i kapitel 10.4 har det framkommit att flera av de rättsliga förutsättningarna för utlämnande av sekretessreglerade uppgifter vid utkontraktering till privata leverantörer snarare är av undantagskaraktär än generellt fungerande lösningar. Enligt vår uppfattning är det bra att myndigheter och andra aktörer får vägledning i hur sekretesslagstiftningen förhåller sig till en informationshantering som

[79] *Microsoft till försvar för Office 365*, Ny Teknik, nr 42, den 19 oktober 2017.

blir alltmer digital. Det finns emellertid en fara med att tolkningsmässigt steg för steg anpassa tillämpningen av äldre regler efter en verklighet som de inte har skapats för. Ett sådant förfarande riskerar att medföra en alltför extensiv tolkning av lagstiftningen som i slutändan kan leda till en urholkning av skyddet för uppgifterna. En myndighets utlämnande av sekretessreglerade uppgifter vid utkontraktering måste baseras på klara och otvetydiga rättsliga regler. Det är därför angeläget att det finns tydliga regler för under vilka förutsättningar utkontraktering till privata leverantörer kan göras och vilket ansvar som åligger parterna vid ett sådant förfarande. Detta skulle enligt vår uppfattning undanröja den rättsliga osäkerhet som nu i vissa fall hindrar eller hämmar digitaliseringen av den offentliga sektorn.

10.6.2 Tystnadsplikt för privata leverantörer bör regleras i lag

Utredningens bedömning: För att skapa en långsiktigt hållbar rättslig reglering som ger stöd för den offentliga sektorns digitalisering, finns det behov av en i lag reglerad tystnadsplikt för de som är verksamma hos en privat leverantör för uppgifter som omfattas av sekretess och som lämnas ut till leverantören i samband med utkontraktering av it-drift eller andra it-baserade funktioner.

Regleringen medför att uppgifter som lämnas ut i samband med sådan utkontraktering får samma sekretesskydd hos leverantören som hos den utkontrakterande myndigheten.

Skälen för utredningens bedömning

Behov av en författningsreglerad tystnadsplikt

Att myndigheter har möjlighet att anlita privata leverantörer för utkontraktering av it-drift eller andra it-baserade funktioner kan vara en förutsättning för digitalisering.

Vår kartläggning har visat att flera myndighetsföreträdare är osäkra på om sekretesslagstiftningen i vissa situationer medger att it-drift och andra it-baserade funktioner utkontrakteras till en privat leverantör och att det har efterfrågats att sekretessfrågorna får en tydligare lösning, (se kapitel 10.5.3).

Enligt vår bedömning kan det i allt ökande grad nu ifrågasättas om det är tillräckligt att den privata leverantörens personal omfattas av en avtalsreglerad tystnadsplikt. Frågan gäller om en myndighet vid en skadeprövning har stöd för att uppgifter som är sekretessreglerade inte omfattas av sekretess i det enskilda fallet, särskilt om uppgifterna är av mycket integritetskänsligt slag och dessutom omfattas av stark sekretess. Bedömningen görs främst mot bakgrund av JO:s beslut från den 9 september 2014 och uttalanden i anledning av Transportstyrelsens granskning (se kapitel 10.4.2). Det förhållandet att vi befinner oss i ett säkerhetspolitiskt läge där den it-relaterade hotbilden i form av attacker, it-brott, spionage och kränkningar blir allt mer påtaglig, samtidigt som den nya tekniken för att bearbeta och lagra uppgifter i vissa fall kan öka riskexponeringen för känsliga och skyddsvärda uppgifter, bidrar också till vår bedömning. Ett annat skäl är de förändringar i rättsläget som ägt rum genom den nya säkerhetsskyddslagen som föreslås träda i kraft den 1 april 2019. Där har det, till skillnad från tidigare, ansetts nödvändigt att komplettera avtalsregleringen i säkerhetsskyddsavtalen med en författningsreglerad och straffsanktionerad tystnadsplikt för enskilda verksamheter. Vi kan alltså skönja en inriktning mot att det nu anses finnas skäl att stärka skyddet för sekretessreglerade uppgifter som hanteras av myndigheter eller dess avtalspartners.

Utredningen konstaterar i likhet med JO att en straffsanktion är samhällets starkaste reprimand och att en sådan sanktion därför ger uppgifterna ett starkare skydd än en avtalsbaserad tystnadsplikt. Med andra ord får risken för att skyddsvärda uppgifter felaktigt lämnas ut anses vara lägre om leverantörens personal agerar under straffansvar när de behandlar uppgifterna. Avtalen mellan den utkontrakterande myndigheten och den privata leverantören och avtalen mellan leverantören och dess personal kan vidare vara otillräckliga eller t.o.m. bristfälliga när det avser utformning av tystnadsplikt, vilket kan få till följd att uppgifterna, med avtal som grund, inte alltid har ett fullgott skydd mot obehörigt röjande hos leverantören.[80] Dessa förhållanden stärker vår uppfattning att avtal inte alltid är tillräckligt för att skydda känsliga och skyddsvärda

[80] Jfr kommittédirektiven *Utkontraktering av säkerhetskänslig verksamhet, sanktioner och tillsyn – tre frågor om säkerhetsskydd* (Dir 2017:32), där det anförs på s. 5 att i vissa fall har avtalsförhållanden reglerats genom säkerhetsskyddsavtal som varit otillräckligt utformade, se även promemorian *Skärpt kontroll av statliga myndigheters utkontraktering och överlåtelse av säkerhetskänslig verksamhet*, Ju 2017/07544/L4, s. 16.

uppgifter och att det finns behov av en författningsreglerad tystnadsplikt.

Av intresse är emellertid att först undersöka om det redan finns någon annan straffbestämmelse än brott mot tystnadsplikt (20 kap. 3 § brottsbalken) som ger ett tillräckligt skydd för uppgifterna i form av en straffsanktionerad befogenhetsinskränkning.

En straffbestämmelse som ibland nämns i dessa sammanhang är trolöshet mot huvudman (10 kap. 5 § brottsbalken). För att ansvar för detta brott ska komma i fråga krävs emellertid att det är fråga om ett åliggande på grund av en förtroendeställning, vilket kräver en direkt relation mellan den utkontrakterande myndigheten och den person som röjer uppgifterna hos leverantören och att röjandet är ett uppsåtligt missbruk av denna ställning. Dessutom ska myndigheten i egenskap av huvudman ha lidit skada för att ansvar för trolöshet mot huvudman ska aktualiseras. Om uppgifter om enskilda röjs så är det dock i första hand dessa som lider skada, inte myndigheten.

En annan straffbestämmelse som ibland diskuteras i dessa sammanhang är dataintrång (4 kap. 9 § c brottsbalken). Det brottet innebär att någon olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift. För att en handling ska leda till ansvar för dataintrång krävs att handlingen har skett olovligen med uppsåt. Ett förfarande är olovligt om det sker utan tillstånd av den som har rätt att förfoga över uppgiften och saknar stöd i gällande rätt.[81] En förutsättning för straffansvar är således att det finns ett förbud att ta del av uppgiften i ett datamedium. Sekretessbelagda uppgifter skyddas således inte mot spridning om en anställd hos leverantören tar del av en uppgift som behövs för att utföra en arbetsuppgift eller om det inte har uppställts något förbud mot att ta del av uppgiften.

Mot denna bakgrund finns det enligt vår mening inte någon straffbestämmelse i gällande rätt som ger ett likvärdigt skydd för uppgifter vid utkontraktering som en straffsanktionerad tystnadsplikt skulle göra. Det finns också ytterligare skäl som talar för en straffsanktionerad tystnadsplikt.

JO:s uppfattning i det beslut som vi redogör för i kapitel 10.5.1 var att de aktuella uppgifterna, som var av mycket integritetskänsligt

[81] *Angrepp mot informationssystem*, prop. 2006/07:66, s. 23.

slag och som omfattades av stark sekretess (omvänt skaderekvisit), inte var tillräckligt skyddade av en avtalsreglerad tystnadsplikt vid utlämnandet till det privata företaget. Denna uppfattning tycks JO grunda på bedömningen att det saknades ett straffrättsligt ansvar för personalen hos företaget. Detta tyder på att en författningsreglerad tystnadsplikt skulle ha varit tillräcklig för att kunna lämna ut de uppgifter det var fråga om. Vid skadeprövningen ska emellertid även omständigheter i det enskilda fallet såsom mottagarens identitet och dennes avsikter med uppgifterna beaktas.[82] Detta innebär enligt vår bedömning att det inte går att dra en generell slutsats om att en författningsreglerad tystnadsplikt medför att uppgifter som omfattas av stark sekretess vid varje tillfälle kan lämnas ut till en privat leverantör vid utkontraktering. Enligt vår bedömning är emellertid en författningsreglerad tystnadsplikt i vart fall i de flesta fall tillräcklig för att skydda uppgifterna och skulle leda till att myndigheter vid prövningen av ett omvänt skaderekvisit i större utsträckning skulle komma fram till att uppgifterna inte omfattas av sekretess i förhållande till den privata leverantören. De rättsliga förutsättningarna för utkontraktering till privata leverantörer skulle därmed förbättras.

Det kan också diskuteras om det är tillräckligt med en avtalsreglerad tystnadsplikt för att mindre integritetskänsliga uppgifter som skyddas av en sekretessbestämmelse försedd med ett rakt skaderekvisit ska kunna lämnas ut till en privat aktör. Det är enligt vår mening inte uteslutet att det vid skadeprövningen i vissa fall skulle kunna anses föreligga skada även i de situationerna. En författningsreglerad tystnadsplikt skulle därför under alla förhållanden väsentligen bidra till att undanröja den osäkerhet kring rättsläget som finns hos myndigheter och andra aktörer.

Det är angeläget att uppgifter som lämnas ut i samband med utkontraktering får samma skydd hos leverantören som hos den utkontrakterande myndigheten. För det fall att uppgifterna lämnas ut till en privat leverantör med stöd av t.ex. bestämmelsen om nödvändigt utlämnande i 10 kap. 2 § offentlighets- och sekretesslagen får uppgifterna i dag inte det skydd hos leverantören som uppgifterna hade fått om personalen omfattats av en straffsanktionerad tystnadsplikt. Detta medför att det finns en viss risk för bristande sekretesskydd. Integritetskänsliga och sekretessreglerade uppgifter

[82] Prop. 1979/80:2 Del A s. 82.

som utkontrakteras bör enligt oss utan tvekan ha samma sekretesskydd oavsett om uppgifterna förekommer i uppdragsgivarens verksamhet som omfattas av offentlighets- och sekretesslagen eller i leverantörens verksamhet som inte omfattas av den lagen.

På grund av det anförda, och mot bakgrund av den ur bl.a. effektivitetssynpunkt påkallade utkontrakteringen av it-drift och andra it-baserade funktioner till privata leverantörer, finns det enligt vår bedömning behov av en författningsreglerad tystnadsplikt för de som är verksamma hos privata leverantörer. En författningsreglerad tystnadsplikt kommer enligt utredningens mening att skapa en långsiktigt hållbar rättslig reglering som ger stöd för den offentliga sektorns digitalisering.

Intresseavvägning

En tystnadsplikt medför en begränsning av yttrandefriheten enligt regeringsformen och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Enligt 2 kap. 21 § regeringsformen får begränsningar i yttrandefriheten endast göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En begränsning får vidare aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Inte heller får en begränsning göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning. Av 2 kap. 23 § regeringsformen följer vidare att yttrandefriheten får begränsas endast med hänsyn till rikets säkerhet, folkförsörjningen, allmän ordning och säkerhet, enskildas anseende, privatlivets helgd eller förebyggandet och beivrandet av brott. Yttrandefrihet får dessutom endast begränsas om särskilt viktiga skäl föranleder det. Regleringen i regeringsformen syftar till att nödvändiga begränsningar inte ska träffa yttrande- och informationsfriheternas kärna.

Vid bedömningen av behovet av tystnadsplikt bör den enskildes intresse av att uppgifterna skyddas mot obehörigt röjande och nyttjande från leverantörens personal därför vägas mot intresset av yttrandefrihet för personalen. När leverantörens personal behandlar

uppgifter för enbart teknisk bearbetning eller lagring för en myndighets räkning är avsikten att de i normalfallet inte ska ta del av själva informationsinnehållet i uppgifterna. Det är endast i undantagsfall som personalen behöver ta del av uppgifterna för att upprätthålla funktionalitet i tjänsten. De privatanställda tjänstemännens intresse av yttrandefrihet när det gäller uppgifter av aktuellt slag torde därför enligt vår bedömning vara ytterst begränsat. Motsvarande bedömning har gjorts av regeringen vid den utvidgning av tystnadsplikten som gäller i det allmännas verksamhet för enbart teknisk bearbetning eller lagring som nyligen genomfördes.[83] En begränsning i form av en tillkommande tystnadsplikt med förbud att avslöja uppgifter av det aktuella slaget skulle vidare inte träffa yttrandefrihetens kärna. För att it-drift och andra it-baserade funktioner ska kunna utkontrakteras till privata leverantörer utan ett bristande sekretessskydd, är en tystnadsplikt inte mer långtgående än vad som behövs med hänsyn till regleringens ändamål. För enskilda är det däremot av mycket stor betydelse att uppgifter om deras personliga förhållanden, som kan vara väldigt integritetskänsliga, skyddas vid en utkontraktering. Vår bedömning är därför att behovet av en bestämmelse om tystnadsplikt för privata leverantörer väger tyngre än intresset av yttrandefrihet för personalen hos den privata leverantören. Det finns därför inte skäl av denna anledning att avstå från att införa en bestämmelse om tystnadsplikt för anställda och uppdragstagare hos privata leverantörer.

Sammanfattningsvis menar vi att det bör införas en reglerad tystnadsplikt för de som är verksamma hos privata leverantörer för uppgifter som omfattas av sekretess och som lämnas ut till leverantören i samband med utkontraktering av it-drift eller andra it-baserade funktioner. Bestämmelsen bör införas i lag, eftersom en inskränkning av yttrandefriheten endast får ske genom lag.[84]

[83] *Utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring*, prop. 2016/17:198, s. 20.
[84] 2 kap. 20 § regeringsformen.

10.6.3 Utformning av bestämmelsen om tystnadsplikt

Utredningens förslag: Den som på grund av anställning eller uppdrag hos en privat leverantör tekniskt bearbetar eller tekniskt lagrar uppgifter för en myndighets räkning, får inte obehörigen röja eller utnyttja dessa uppgifter.

I det allmännas verksamhet ska i stället bestämmelserna i offentlighets- och sekretesslagen tillämpas.

Skälen för utredningens förslag

Teknisk bearbetning och lagring

Tystnadsplikten bör enligt vår mening gälla i samband med att privata leverantörer utför tjänster som endast innebär teknisk bearbetning eller teknisk lagring för myndighetens räkning. Detta med utgångspunkt i utredningens uppdrag att lämna förslag till författningsändringar som har störst potential att stödja den fortsatta digitaliseringen av hela, eller stora delar, av den offentliga förvaltningen.

Begreppet teknisk bearbetning eller teknisk lagring härrör från 2 kap. 10 § tryckfrihetsförordningen och 9 kap. 7 § sekretesslagen (numera 40 kap. 5 § offentlighets- och sekretesslagen). I förarbetena till dessa bestämmelser nämns som exempel på teknisk bearbetning överlämnande av maskinskrivet manuskript till en datacentral för överföring av texten till magnetband eller överlämnande av manuskript för tryckning eller kopiering. Vidare nämns redigering av ljudupptagningar på magnetband och överföringar av sådana upptagningar till grammofonskiva. Med teknisk lagring avses enligt förarbetena sådana former av lagring som kräver särskilda tekniska anordningar, t.ex. lagring av information i skivminne eller på magnetband.[85]

Innebörden av begreppet teknisk bearbetning eller teknisk lagring har dock förändrats på grund av den omfattande tekniska utveckling som skett sedan begreppet infördes. Under kartläggningen har vi också uppfattat en problematik i att relatera detta begrepp till nutida teknikanvändning. I det förslag som vi nu lämnar innefattar vi i begreppet åtgärder såsom utveckling, införande, drift, förvaltning eller avveckling av en it-relaterad tjänst där tjänsten kan avse

[85] Regeringens proposition 1975/76:160 *om nya grundlagsbestämmelser angående allmänna handlingars offentlighet*, s. 137 och prop. 1979/80: 2 Del A s. 272.

både teknisk funktionalitet och arbete utfört av personal som är hänförligt till den tekniska bearbetningen eller lagringen, t.ex. support. Exempel på tjänster som omfattas av nämnda begrepp är bearbetning eller lagring av uppgifter i ett datacenter eller av uppgifter i e-arkiv, molntjänster eller andra it-baserade funktioner. Även storskalig skanning av dokument är exempel på en tjänst som enligt vår mening faller in under begreppet. Någon uttömmande beskrivning är emellertid svår att lämna, inte minst mot bakgrund av den snabba tekniska utvecklingen.

Avgränsningen till tjänster eller funktioner som *enbart* innebär teknisk bearbetning eller teknisk lagring för myndighetens räkning innebär att tjänster som visserligen innefattar moment av teknisk bearbetning eller teknisk lagring, men som inte *enbart* avser sådan bearbetning eller lagring inte omfattas av bestämmelsen. Exempelvis ansåg regeringen att en myndighets tillhandahållande av hjälptjänster[86] till enskilda inte endast utgjorde teknisk bearbetning eller teknisk lagring för annans räkning.[87]

Det sagda innebär vidare att utkontraktering av arbetsuppgifter som är hänförliga till vård- och omsorgssektorns behandling av personuppgifter vid t.ex. journalföring, bedömning av röntgenbilder eller patientrådgivning, faller utanför tillämpningsområdet. Vi anser att eventuella behov av tystnadsplikt för personer som behandlar uppgifter för vårdgivares räkning utöver den som redan finns i t.ex. patientsäkerhetslagen och socialtjänstlagen lämpligen bör omhändertas i den sektorslagstiftning som redan finns på området.

Den nu föreslagna regleringen medför inte några nya hinder för utkontraktering avseende sådana arbetsuppgifter som faller utanför tillämpningsområdet. De rättsliga bedömningarna avseende när sekretessreglerade uppgifter kan lämnas till privata leverantörer vid sådan utkontraktering kommer dock inte heller att förenklas på det sätt som blir fallet för den utkontraktering som faller inom tillämpningsområdet.

[86] En hjälptjänst är när en myndighet erbjuder ett anpassat stöd till företag och privatpersoner för att de på ett effektivt sätt ska kunna använda en viss digital tjänst i kontakt med myndigheten, se vidare prop. 2016/17:198 s. 8 f.
[87] A.prop. s. 24.

Tystnadsplikten bör inte begränsas till personuppgifter

Utredningens kartläggning har visat att det inte bara är personuppgifter som behöver skyddas vid utkontraktering till en privat leverantör, utan även uppgifter om juridiska personer. Uppgifter om juridiska personer behandlas ofta med anknytning till någon personuppgift, t.ex. uppgift om företrädare för en juridisk person. Det förekommer emellertid även att uppgifter som rör företag, ideella föreningar och andra juridiska personer behandlas utan anknytning till någon personuppgift.

Det finns enligt utredningens bedömning ett betydande skyddsintresse i samband med utkontraktering av it-drift och andra it-baserade funktioner även för vissa uppgifter om juridiska personer, t.ex. uppgifter som omfattas av skattesekretess eller förundersökningssekretess.[88] Ett liknande resonemang fördes i lagstiftningsärendet som ledde till att bestämmelsen om tystnadsplikt i det allmännas verksamhet som avser teknisk bearbetning eller teknisk lagring för någon annans räkning den 1 januari 2018 utvidgades från att omfatta endast personuppgifter till att omfatta alla uppgifter om en enskilds personliga eller ekonomiska förhållanden i sådan verksamhet.[89]

Vi anser därför att omfattningen av den föreslagna tystnadsplikten inte bör begränsas till att enbart avse personuppgifter, utan även uppgifter om juridiska personer.

Tystnadsplikten bör inte begränsas till uppgifter om enskildas personliga eller ekonomiska förhållanden

En annan fråga att ta ställning till är om bestämmelsen om tystnadsplikt bör omfatta alla myndighetens sekretessreglerade uppgifter eller enbart uppgifter om enskilds personliga eller ekonomiska förhållanden. Utgångspunkten vid utformningen av en ny bestämmelse om sekretess är att det inte ska gälla mer sekretess än vad som är nödvändigt för att skydda det intresse som har föranlett bestämmelsen.[90] Ett alternativ som vi har övervägt är en reglering som begränsas till att avse enbart uppgifter om enskilds personliga eller

[88] 27 kap. respektive 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen.
[89] Utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring, prop. 2016/17:198.
[90] Prop. 1979/80:2 Del A s. 78.

ekonomiska förhållanden. Begreppet enskild omfattar både fysiska och juridiska personer. En sådan begränsning innebär emellertid att uppgifter som omfattas av sekretess till skydd för ett allmänt intresse faller utanför tystnadsplikten. Mot bakgrund av kartläggningen ser vi att myndigheter även har behov av att lämna ut uppgifter som är sekretessreglerade med hänsyn till ett allmänt intresse i samband med utkontraktering. Utkontraktering av it-drift har som framgått blivit en central del för den digitala förvaltningen. Vid sådan utkontraktering, dvs. när alla eller stora delar av en myndighets verksamhetssystem omfattas, kan systemen innehålla uppgifter av känslig beskaffenhet som hos myndigheten omfattas av sekretess till skydd för ett allmänt intresse. Det kan vid en sådan utkontraktering vara mycket svårt att särskilja de delar av verksamhetsstödet där känsliga uppgifter förekommer för att själv bearbeta och lagra dessa uppgifter.

Den sekretess och tystnadsplikt som gäller för utkontraktering av it-drift till en *annan myndighet* är absolut för uppgift om enskilds personliga eller ekonomiska förhållanden för driftmyndigheten.[91] När det gäller uppgifter som är sekretessreglerade på grund av ett allmänt intresse gäller sedan den 1 januari 2018 sekundär sekretess för driftmyndigheten såvida denna inte omfattas av en egen primär sekretessbestämmelse som i så fall ska tillämpas.[92] Regeringen fann i lagstiftningsärendet att det fanns behov av en reglering för att skydda uppgifter som är sekretessreglerade av hänsyn till ett allmänt intresse vid utkontraktering av enbart teknisk bearbetning eller teknisk lagring från en myndighet till en annan myndighet. På grund därav övervägdes en reglering med absolut sekretess även för uppgifter som skyddas på grund av ett allmänt intresse, dvs. sekretessens föremål i 40 kap. 5 § offentlighets- och sekretesslagen skulle vidgas till att omfatta alla uppgifter och inte bara uppgifter om personliga och ekonomiska förhållanden. Konsekvenserna av en sådan bestämmelse ansågs emellertid vara svåra att överblicka och det var inte heller klarlagt om regleringen var förenlig med bestämmelserna i 2 kap. 21 och 23 §§ regeringsformen om inskränkningar i yttrandefriheten.[93]

[91] 40 kap. 5 § offentlighets- och sekretesslagen.
[92] 11 kap. 4 a och 8 §§ offentlighets- och sekretesslagen.
[93] Prop. 2016/17:198 s. 22 f.

Uppgifter som är sekretesskyddade till följd av ett allmänt intresse omfattas i viss utsträckning av regleringen i säkerhetsskyddslagstiftningen där särskilda hanteringsregler gäller för utkontraktering. Som tidigare nämnts är utkontraktering av säkerhetskänslig verksamhet föremål för översyn, (se kapitel 10.2.4). Alla uppgifter som omfattas av sekretess till skydd för ett allmänt intresse faller emellertid inte under säkerhetsskyddslagstiftningen. Det finns därför enligt oss en risk för bristfälligt sekretesskydd vid utkontraktering av it-drift eller andra it-baserade funktioner till en privat leverantör om inte alla sekretessreglerade uppgifter i myndighetens verksamhet skyddas av tystnadsplikt. En bestämmelse om tystnadsplikt som avgränsas till personliga och ekonomiska förhållanden kan också leda till svåra avvägningar i fråga om vad som omfattas av den privata leverantörens tystnadsplikt.

I avsnitt 10.6.2 har vi kommit fram till att begränsningen av yttrandefriheten för de privatanställda tjänstemännen inte är av sådan karaktär att den träffar kärnan i rättigheten. Vi menar därför att även ett skydd för uppgifter som omfattas av sekretess av hänsyn till ett allmänt intresse och som lämnas ut till en privat leverantör enbart för teknisk bearbetning eller lagring för en myndighets räkning, är berättigat för att skydda känslig information i den offentliga verksamheten. Begränsningen är inte heller mer långtgående än vad som är nödvändigt med hänsyn till regleringens ändamål.[94] Mot denna bakgrund finner vi att omfattningen av den föreslagna tystnadsplikten inte bör begränsas till att avse enbart uppgifter som är sekretessreglerade hos myndigheten till skydd för enskilds personliga eller ekonomiska förhållanden, utan även uppgifter som är sekretessreglerade till skydd för ett allmänt intresse.

Bestämmelsen bör innehålla en upplysning om att vid utkontraktering i det allmännas verksamhet gäller förbuden mot att röja eller utnyttja en uppgift som finns i offentlighets- och sekretesslagen, eller lag eller förordning som offentlighets- och sekretesslagen hänvisar till.

[94] Jfr 2 kap. 21 § regeringsformen.

Vem omfattas av tystnadsplikten?

Tystnadsplikten bör gälla för de personer som på grund av anställning hos den privata leverantören tekniskt bearbetar eller tekniskt lagrar uppgifter för en myndighets räkning. Även de som har uppdrag hos leverantören, t.ex. inhyrda konsulter, bör omfattas av tystnadsplikten. En anställd eller en uppdragstagare hos en underleverantör till leverantören bör också omfattas av tystnadsplikten om denne tekniskt bearbetar eller lagrar uppgifter, eftersom det görs för den utkontrakterande myndighetens räkning.

Tystnadsplikten är förenad med straffansvar

En författningsreglerad tystnadsplikt är förenad med straffansvar för brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken. Eventuella negativa konsekvenser av att införa en straffsanktionerad tystnadsplikt måste ställas mot de intressen som förbudet avser att skydda. I det här fallet anser vi att skyddet för sekretessintressena väger tungt. En enskild person vars uppgifter lämnas ut inom ramen för utkontraktering till en privat leverantör har en berättigad förväntan på att uppgifterna inte obehörigen röjs eller utnyttjas, oavsett om uppgifterna finns i en verksamhet som omfattas av offentlighets- och sekretesslagen eller i en verksamhet som inte omfattas av den lagen. Även intresset av att vid utkontraktering skydda de uppgifter som omfattas av sekretess till skydd för ett allmänt intresse väger enligt utredningen tungt.

Krav måste också ställas på precision och förutsebarhet avseende det straffbara området, även i det enskilda fallet. Det är därför lämpligt att den utkontrakterande parten (dvs. myndigheten) tydligt redogör för den utförande parten (dvs. den privata leverantören) vilka typer av uppgifter som omfattas av sekretess hos myndigheten och därmed av tystnadsplikten.

I begreppet obehörigen ligger att det enbart är uppgifter som vid en prövning skulle bedömas vara sekretessbelagda som omfattas av den straffsanktionerade tystnadsplikten. Som ett obehörigt röjande räknas därmed inte när uppgifter lämnas ut med samtycke eller som en följd av skyldighet i lag eller förordning t.ex. utlämnande av uppgifter till en tillsynsmyndighet.

10.6.4 En ny sekretessbrytande bestämmelse

Utredningens bedömning: Det finns behov av en sekretessbrytande bestämmelse för att myndigheter i samband med utkontraktering av it-drift eller andra it-baserade funktioner ska kunna lämna ut vissa sekretessbelagda uppgifter till privata eller offentliga leverantörer.

Utredningens förslag: En sådan sekretessbrytande bestämmelse ska införas i offentlighets- och sekretesslagen.

Skälen för utredningens bedömning och förslag

Behov av en sekretessbrytande bestämmelse

Nästa fråga att överväga är om det finns behov av att också införa en sekretessbrytande regel för att myndigheter, när det är lämpligt, ska kunna lämna ut uppgifter som omfattas av sekretess till privata leverantörer.

Utredningen har i kapitel 10.6.2 konstaterat behov av en författningsreglerad tystnadsplikt för privata leverantörer för att bl.a. möjliggöra utlämnande av sekretessreglerade uppgifter i vissa fall. Enligt vår bedömning är en lagreglerad tystnadsplikt i de flesta fall tillräcklig för att lämna ut integritetskänsliga uppgifter som omfattas av stark sekretess till en privat leverantör vid utkontraktering, utan att det innebär men för den enskilde. En bestämmelse som, under vissa förutsättningar, uttalat bryter sekretessen om uppgifterna lämnas ut i samband med utkontraktering till en privat aktör skulle emellertid vara lättare att tillämpa, eftersom det då inte krävs någon skadeprövning i varje enskilt fall.

Uppgifter som omfattas av absolut sekretess kan bara lämnas ut med stöd av en sekretessbrytande bestämmelse. Absolut sekretess gäller t.ex. för anbud i offentlig upphandling, för omhändertagande av patientjournal, för kommunal familjerådgivning eller inom beskattningsverksamheten för uppgift om en enskilds personliga eller ekonomiska förhållanden.[95] Även statistiksekretessen är absolut,

[95] 19 kap. 3 §, 25 kap. 5 §, 26 kap. 3 § och 27 kap. 1 § offentlighets- och sekretesslagen.

men det finns vissa undantag för att möjliggöra utlämnande t.ex. för forsknings- eller statistikändamål.[96]

I kartläggningsarbetet har vi funnit att myndigheter även har behov av att utkontraktera uppgifter som omfattas av absolut sekretess. Sådana uppgifter kan finnas i en myndighets verksamhetssystem, vilket medför att det vid utkontraktering av it-drift i praktiken kan vara svårt eller närmast omöjligt att skilja ut uppgifterna. Som precis nämnts gäller absolut sekretess för anbud i samband med offentlig upphandling. För upphandlande myndigheter finns särskilda digitala upphandlings- och avtalsstöd som tillhandahålls av privata leverantörer. Det finns emellertid en osäkerhet hos vissa myndigheter under vilka förutsättningar det är förenligt med sekretesslagstiftningen att hantera anbud i ett sådant stöd, när absolut sekretess gäller för uppgift som rör anbud till dess att alla anbud offentliggörs eller beslut om leverantör och anbud fattats eller ärendet har slutförts.[97]

Det rättsliga stöd som främst aktualiseras vid ett utlämnande av uppgifter som omfattas av absolut sekretess till en privat leverantör är bestämmelsen om nödvändigt utlämnande i 10 kap. 2 § offentlighets- och sekretesslagen. Som tidigare anförts upplevs emellertid bestämmelsens tillämpningsområde som oklar av myndigheter och andra aktörer, särskilt i ljuset av att bestämmelsen ska tillämpas restriktivt enligt förarbetena.

Utlämnande av sekretessbelagda uppgifter ska ha stöd i en klar och tydlig rättslig grund. Vi anser därför att det finns behov av en sekretessbrytande bestämmelse för att myndigheter, när det är lämpligt, ska kunna lämna ut uppgifter som omfattas av absolut sekretess till privata leverantörer. En sådan bestämmelse skulle även klargöra under vilka förutsättningar myndigheter kan lämna ut uppgifter som omfattas av stark sekretess, eftersom en bedömning om huruvida skaderekvisitet är uppfyllt i det enskilda fallet inte behöver göras.

Den sekretessbrytande bestämmelsen bör även omfatta utlämnande av uppgifter till myndigheter. Samma skäl som anförts ovan gör sig även gällande när en myndighet utkontrakterar it-drift eller andra it-baserade funktioner till en annan myndighet.

[96] 24 kap. 8 § offentlighets- och sekretesslagen.
[97] 19 kap. 3 § andra stycket offentlighets- och sekretesslagen.

Intresseavvägning

När sekretessgenombrott övervägs måste stor hänsyn tas till rätten till skydd för den personliga integriteten och övriga intressen som sekretessbestämmelserna avser att skydda. Enligt förarbetena från den tidigare sekretesslagens tillkomst är en utgångspunkt att information om enskilda som omfattas av sekretess inte ska vidarebefordras utanför den verksamhet i vilken den har hämtats in. Det anförs, när frågan om utbyte av information mellan myndigheter diskuteras, att den omständigheten att ett större antal tjänstemän får kunskap om ett känsligt förhållande kan upplevas som menligt av den som uppgiften rör. Vidare anförs att även om de funktionärer hos den andra myndigheten som får del av informationen i sin tur har tystnadsplikt, ökar risken för obehörig vidarespridning.[98]

I vissa fall är det ofrånkomligt att myndigheter eller enskilda kan ta del av sekretessbelagda uppgifter hos en myndighet. I sådana fall kan det finnas skäl för en sekretessbrytande regel. Här avses i första hand intresset av att offentlig sektor kan bedriva den ändamålsenliga och kostnadseffektiva verksamhet som förväntas, men också vikten av att främja digitala förfaranden som möjliggör nya processer, funktioner och tjänster till privatpersoner och företag (se kapitel 10.1.2). Mot detta intresse ska ställas graden av integritetsstrång för enskilda vid utlämnandet av uppgifterna, ändamålet för utlämnandet och hur uppgifterna skyddas efter utlämnandet.

Avsikten med det utlämnande som här diskuteras är att mottagaren endast ska tekniskt bearbeta eller tekniskt lagra uppgifterna. Det innebär att mottagarens personal i normalfallet inte ska ta del av uppgifterna, utan det är endast i undantagsfall som det görs i syfte att upprätthålla funktionalitet i tjänsten. Häri ligger en avsevärd begränsning i fråga om vilken personkrets och antalet personer som tar faktisk del av uppgifterna. Uppgifterna ska inte användas i leverantörens egna verksamhet. Till detta kommer att vi avseende de privata leverantörerna föreslår en straffsanktionerad tystnadsplikt, utöver den hittills tillämpade avtalsbaserade tystnadsplikten, för de personer som tar faktisk del av uppgifterna. Den straffsanktionerade tystnadsplikten motsvarar också det skydd som uppgifterna har hos myndigheten. För de myndigheter som utför teknisk bearbetning

[98] Prop. 1979/80:2 Del A s. 90.

eller lagring för en annan myndighets räkning finns bestämmelser om sekretess och tystnadsplikt i offentlighets- och sekretesslagen.[99] Uppgifterna som lämnas ut kommer därför ha ett sekretesskydd hos mottagaren, dvs. leverantören.

Sammantaget menar vi att det finns förutsättningar för att nu föreslå en sekretessbrytande bestämmelse. Bestämmelsen bör införas i 10 kap. i offentlighets- och sekretesslagen.

Finns behov av undantag från tystnadsplikt i privat verksamhet?

Vissa privata utförare av offentligt finansierad verksamhet omfattas av tystnadsplikt i sektorslagstiftningen, (se kapitel 10.3.3). Vid tolkning av bestämmelserna om tystnadsplikt i speciallagstiftningen kan som tidigare nämnts ledning sökas i bestämmelserna i offentlighets- och sekretesslagen. Utgångspunkten är att det ska vara en nära överensstämmelse vad gäller innebörden av de olika bestämmelserna om tystnadsplikt för offentlig respektive enskild verksamhet. Regeringen har i ett tidigare lagstiftningsärende anfört att nya sekretessbrytande regler på områdena socialtjänst och hälso- och sjukvård i sekretesslagen, bör medföra att obehörighetsrekvisitet i tystnadspliktsreglerna i socialtjänstlagen och lagen (1998:531) om yrkesverksamhet på hälso- och sjukvårdens område[100] tolkas på motsvarande sätt.[101] Mot denna bakgrund anser vi att det inte finns behov av en särskild bestämmelse som medger undantag från tystnadsplikt i speciallagstiftning, för att den som omfattas av denna ska kunna lämna ut uppgifter till privata leverantörer i samma utsträckning som myndigheter i samband med utkontraktering av it-drift eller andra it-baserade funktioner. Om ett sådant behov skulle komma fram anser vi att det lämpligen bör omhändertas i aktuell sektorslagstiftning.

[99] 11 kap. 4 a och 40 kap. 5 § offentlighets- och sekretesslagen.
[100] Lagen är numera upphävd och har ersatts av patientsäkerhetslagen.
[101] Prop. 2005/06:161, s. 82 och 93.

10.6.5 Utformning av en sekretessbrytande bestämmelse

Utredningens förslag: Sekretess ska inte hindra att en uppgift lämnas ut till en enskild eller till en annan myndighet som utför uppdrag för enbart teknisk bearbetning eller teknisk lagring för den utlämnande myndighetens räkning, om uppgiften behövs för att utföra uppdraget.

En uppgift ska inte lämnas ut om

1. övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut, eller
2. det av andra skäl är olämpligt.

Skälen för utredningens förslag

Förutsättningar för sekretessgenombrott

En förutsättning för att en sekretessbelagd uppgift ska kunna lämnas ut med stöd av den sekretessbrytande bestämmelsen är att leverantören har behov av uppgiften för att utföra uppdraget som denne har fått av myndigheten. Behovet ska vara konkret. Det är den utlämnande myndigheten som ytterst avgör om leverantören behöver uppgifterna. Enligt vår mening krävs inte att det görs en behovsprövning i varje enskilt fall utan en bedömning kan göras utifrån de behov som typiskt sett finns för en kategori av uppgifter.[102]

För att en sekretessbrytande bestämmelse av aktuellt slag inte ska få ett för vidsträckt tillämpningsområde krävs emellertid begränsningar av när en uppgift får lämnas ut. Sådana begränsningar syftar till att skydda enskilda och allmänna intressen och att se till att uppgiftsutlämnandet i övrigt inte är olämpligt.

Skydd för sekretessintressen genom en intresseavvägning

Uppgifter som omfattas av sekretess kan vara mycket känsliga och en bestämmelse om sekretessgenombrott bör därför utformas så att det finns möjlighet att beakta starka integritetsintressen rörande

[102] Jfr prop. 1979/80:2 Del A s. 80 f. och 326 f.

enskilda, men även intressen av skydd för det allmänna. En uppgift bör därför inte lämnas ut om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut.

Precis som vid behovsprövningen så krävs inte att det görs en prövning i varje enskilt fall utan en bedömning kan göras utifrån de behov av sekretess som typiskt sett finns för en kategori av uppgifter.[103] Vid intresseavvägningen bör sekretesskyddet hos mottagaren vägas in i bedömningen. Uppgifterna skyddas hos en enskild leverantör genom den föreslagna tystnadsplikten och hos en offentlig leverantör genom sekretessbestämmelserna i 11 kap. 4 a § och 40 kap. 5 § offentlighets- och sekretesslagen.

De samhällsutmaningar som det offentliga Sverige möter kräver att digitaliseringens möjligheter tillvaratas på bästa sätt så förvaltningens resurser används effektivt och förtroendet för förvaltningen upprätthålls. I linje med vad som tidigare framförts i förvaltningspolitiska uttalanden om inslag av utkontraktering av it-drift och andra it-baserade funktioner är det påkallat att myndigheterna utkontrakterar en del sådan verksamhet för att åstadkomma en ändamålsenlig, kostnadseffektiv och tillgänglig förvaltning som erbjuder digitala förfaranden som möjliggör nya former och sätt att erbjuda service och tjänster till privatpersoner och företag (se kapitel 10.1.2). Även om ett utlämnande av uppgifter endast görs till ett mindre antal personer för att enbart tekniskt bearbeta eller lagra dem och avsikten är att de i normalfallet inte ska ta del av uppgifterna, kan emellertid vissa kategorier av uppgifter vara särskilt känsliga till sin natur och det kan därför finnas starka skäl till att inte lämna ut dem. Bestämmelsen innebär att en avvägning ska göras mellan nämnda intressen. Om sekretessintresset väger tyngre än intresset av att lämna ut uppgiften för teknisk bearbetning eller lagring får uppgiften inte lämnas ut.

Olämplighetsprövning

Ett utlämnande av uppgifter bör inte heller få göras om det är olämpligt. Det kan finnas flera olika anledningar till att det är olämpligt att lämna ut vissa uppgifter i samband med utkontraktering. Det kan t.ex. röra sig om en mycket stor mängd uppgifter där de flesta

[103] Jfr prop. 1979/80:2 Del A s. 80 f. och 326 f.

enskilda uppgifterna inte är känsliga, men den totala informationsmängden i sig är så skyddsvärd att ett utlämnande av uppgifterna bedöms vara olämpligt. Med en oinskränkt tillgång till stora informationsmängder kan det finnas risk för åtgärder och analyser som av säkerhetsskäl inte bör få förekomma. Ett utlämnande av uppgifter kan också vara olämpligt om flera myndigheters system och information samlas i samma lagringsmedium, t.ex. en molntjänst, vilket kan innebära en ökad riskexponering för känsliga uppgifter. Även en tänkt geografisk lokalisering av uppgifterna kan medföra att ett utlämnande av vissa känsliga uppgifter till leverantören bedöms vara olämpligt.

En del av de sekretessbelagda uppgifter som kan vara aktuella att lämna ut till leverantörer omfattas av säkerhetsskyddslagen. Förslaget till ny säkerhetsskyddslag innebär att tillämpningsområdet för lagen kommer att utökas och framöver kommer därför ännu fler uppgifter att omfattas av de krav som ställs i denna lag. Utan att här föregripa kommande lagstiftning kan konstateras att det vore olämpligt att, med stöd av aktuell sekretessbrytande bestämmelse, lämna ut uppgifter som även omfattas av säkerhetsskyddslagstiftningen, om det skulle vara oförenligt med de krav som ställs i den lagstiftningen.

10.6.6 En särskild lag om tystnadsplikt införs

Utredningens förslag: Det ska införas en ny lag som gäller när en myndighet uppdrar åt en privat leverantör att behandla uppgifter för enbart teknisk bearbetning eller teknisk lagring för myndighetens räkning. Lagen ska även gälla för vissa organ och verksamheter som trätt i stället för en myndighet. Lagen ska benämnas lag om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring.

Bestämmelsen om tystnadsplikt för de som är verksamma hos den privata leverantören ska införas i lagen.

Skälen för utredningens förslag

En ny lag

Bestämmelsen om tystnadsplikt för de som är verksamma hos en privat leverantör bör införas i en ny lag. Lagen bör gälla när en myndighet uppdrar åt en privat leverantör att behandla uppgifter för enbart teknisk bearbetning eller teknisk lagring för myndighetens räkning. Vad begreppet teknisk bearbetning eller teknisk lagring innebär och avgränsningen till *enbart* sådan bearbetning eller lagring, har behandlats i kapitel 10.6.3. Lagen bör benämnas lag om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring.

Lagen bör vara subsidiär till den nya säkerhetsskyddslagen som föreslås träda i kraft den 1 april 2019 och säkerhetsskyddsförordningen (1996:633). Finns det bestämmelser i nämnda lag eller förordning som avviker från den lag vi nu föreslår, ska de bestämmelserna tillämpas i stället.

Lagens tillämpningsområde för vissa organ och verksamheter

Lagen bör även gälla för vissa organ eller verksamheter som trätt i stället för en myndighet, när ett sådant organ eller en sådan verksamhet uppdrar åt en privat leverantör att behandla uppgifter för enbart teknisk bearbetning eller teknisk lagring för organets eller verksamhetens räkning. Vid tillämpningen av lagen bör därför aktiebolag, handelsbolag, ekonomiska föreningar och stiftelser där kommuner, landsting eller kommunalförbund utövar ett rättsligt bestämmande inflytande enligt 2 kap. 3 § offentlighets- och sekretesslagen och de organ som anges i bilagan till offentlighets- och sekretesslagen beträffande den verksamhet som anges där, jämställas med en myndighet.

Även en yrkesmässigt bedriven enskild verksamhet som till någon del är offentligt finansierad och som anges i 2 § första stycket lagen (2017:151) om meddelarskydd i vissa enskilda verksamheter, bör jämställas med en myndighet vid tillämpningen av lagen. Hänvisningen till nämnda bestämmelse innebär att enskilda verksamheter som finns inom skolväsendet, hälso- och sjukvård, tandvård eller social omsorg, kommer att omfattas av den av oss föreslagna lagen. Den nämnda bestämmelsen i lagen om meddelarskydd

i vissa enskilda verksamheter är emellertid föremål för översyn. Utredningen om ett stärkt meddelarskydd för privatanställda i verksamheter som är helt eller delvis offentligt finansierade har under våren 2017 lämnat förslag på en utvidgning av bestämmelsens tillämpningsområde så att den även omfattar kollektivtrafik, färdtjänst, riksfärdtjänst och skolskjuts.[104] Enligt vår uppfattning bör tillämpningsområdet för den av oss föreslagna lagen vid varje tillfälle vara tillämplig för de verksamheter som kommer att omfattas av lagen om meddelarskydd i vissa enskilda verksamheter. En dynamisk hänvisning till den lagens tillämpningsområde bör därför göras.

För att en enskild verksamhet ska omfattas av den av oss föreslagna lagen krävs vidare att den är offentligt finansierad. Med offentlig finansiering bör avses ett direkt stöd eller betalning från det allmänna för att driva verksamheten inom de aktuella verksamhetsområdena som nämns ovan. Ett krav bör vara att finansieringen är kopplad till själva driften av verksamheten.

Vi har övervägt om den utkontrakterande verksamheten bör vara helt offentligt finansierad eller om det är tillräckligt att den delvis är det för att omfattas av lagen. Enligt vår mening skulle ett krav på att den enskilda verksamheten är helt offentligt finansierad leda till att många verksamheter, t.ex. fristående skolor och privata läkarmottagningar, inte omfattas av lagen eftersom de sällan är helt offentligt finansierade. Det är inte heller enligt vår bedömning lämpligt att ställa upp ett krav på att endast sådan teknisk bearbetning eller lagring som rör uppgifter som enbart finansieras av allmänna medel bör omfattas av lagen, eftersom denna behandling eller lagring inte går att särskilja i en verksamhet som finansieras av såväl allmänna som privata medel. Ett sådant krav skulle riskera att medföra svårigheter avseende gränsdragningen för lagens tillämpningsområde. Vi anser därför att lagen bör tillämpas i alla verksamheter inom skola, vård och omsorg som till någon del är offentligt finansierad.

[104] *Meddelarskyddslagen – fler verksamheter med stärkt meddelarskydd* (SOU 2017:41).

10.6.7 Konsekvenser av förslagen

Ett förstärkt skydd och en klar rättslig grund för utlämnande

Den föreslagna författningsreglerade tystnadsplikten för de som är verksamma hos en privat leverantör innebär ett förstärkt skydd för sekretessreglerade uppgifter som lämnas ut i samband med utkontraktering av teknisk bearbetning eller lagring, eftersom uppgifterna får samma sekretesskydd hos leverantören som hos den utkontrakterande myndigheten. En straffsanktionerad tystnadsplikt är ett starkt incitament för leverantören och dess anställda att hantera myndighetens information med varsamhet. Regleringen är därför av väsentlig betydelse för att säkerställa att uppgifterna skyddas mot obehörigt röjande och nyttjande av den privata leverantörens personal. Enskilda har ett betydande intresse av att integritetskänsliga uppgifter inte blir åtkomliga för obehöriga. Det skulle riskera ett sviktande förtroende för myndigheten och i förlängningen även för hela den offentliga sektorn. Regleringen är också av vikt för att upprätthålla sekretessen för uppgifter som omfattas av ett allmänt intresse. En brist i sekretesskyddet när sådana uppgifter utkontrakteras skulle kunna skada centrala samhälleliga intressen.

Den föreslagna sekretessbrytande bestämmelsen innebär att myndigheter får en klar och tydlig rättslig grund för att lämna ut uppgifter som omfattas av sekretess till privata eller offentliga leverantörer och därmed undanröjs den rättsliga osäkerhet som i dag råder vid viss utkontraktering.

Förslagen innebär sammantaget ett främjande av digitala förfaranden i den offentliga sektorn genom att undanröja den osäkerhet som finns hos myndigheter kring de rättsliga förutsättningarna för utkontraktering av vissa digitala förfaranden till privata leverantörer. Vidare innebär förslagen en mer effektiv och innovativ offentlig förvaltning eftersom det ger stabila rättsliga förutsättningar för att it-drift och andra it-baserade funktioner utförs av privata företag, med expertkompetens på området. Det är resurskrävande för en myndighet att själv inneha sådan kompetens och förslagen kan därmed förväntas medföra besparingar för det allmänna.

Internationell räckvidd av brott mot tystnadsplikt

Som nämnts under kapitel 10.1.3 kan såväl leverantörer som underleverantörer ha sitt säte utomlands och även delar av leverantörernas personal kan vara placerade utomlands. En konsekvens av detta är att det är relevant att undersöka om personer som har hemvist utanför Sverige och inte är svenska medborgare omfattas av den straffsanktion som tystnadsplikten för med sig.

Straffbudet i 20 kap. 3 § brottsbalken utgår från att gärningen är ett åsidosättande av en tystnadsplikt som är grundad på svensk författning. Om gärningen begåtts utom riket måste den enligt 2 kap. 2 § brottsbalken som regel begåtts av svensk medborgare eller av utlänning med hemvist i Sverige[105] och det ska dessutom föreligga s.k. dubbel straffbarhet[106] för att det ska föreligga svensk straffrättslig jurisdiktion.

Från kraven i 2 kap. 2 § görs emellertid i 2 kap. 3 § 4 brottsbalken undantag för det fall att brottet har förövats mot Sverige, svensk kommun eller annan menighet eller svensk allmän inrättning.[107] Uttrycket brott mot Sverige innefattar enligt kommentaren brott som omedelbart riktar sig mot ett sådant intresse beträffande vilket den svenska staten uppfattas som bärare. Dit hör brott mot svenska statens yttre eller inre säkerhet eller dess offentliga myndigheter. Med brott mot svensk kommun eller annan menighet avses enligt kommentaren brott mot kommuner, men också mot landsting, kommunalförbund, och andra kommunala bildningar. Även brott mot en svensk allmän inrättning omfattas av undantaget. För att bedöma om en inrättning är allmän ska enligt kommentaren flera skilda omständigheter beaktas. Av betydelse är om inrättningen utövar en offentlig funktion eller om inrättningen tjänar ett allmännyttigt ändamål och inte drivs för att bereda affärsvinst. Betydelse ska dessutom tillmätas frågan om hur inrättningen finansieras t.ex.

[105] Gärningen kan också begåtts av utlänning utan hemvist i Sverige, som efter brottet blivit svensk medborgare eller tagit hemvist här i riket eller som är dansk, finsk, isländsk eller norsk medborgare och finns här eller av annan utlänning som finns här i riket och på brottet enligt svensk lag kan följa fängelse i mer än sex månader.
[106] Med dubbel straffbarhet avses att gärningen även är straffbar enligt lagen i det land där den begicks.
[107] Nils-Olof Berggren m.fl. Brottsbalken (10 november 2017, Zeteo), kommentaren till 20 kap. 3 § brottsbalken.

om inrättningen har grundats med hjälp av allmänna medel eller om den åtnjuter understöd av sådana medel.[108]

Med det ovan anförda i beaktande kan, enligt vår bedömning, en svensk medborgare eller en utlänning enligt brottsbalkens reglering dömas för brott mot tystnadsplikt som har begåtts utomlands men som utövats mot svenska offentliga myndigheter, kommuner och landsting, trots att det inte föreligger dubbel straffbarhet. Detta gäller även om brottet har utövats mot en svensk privat aktör som utför offentligt finansierad verksamhet under förutsättning att aktören omfattas av begreppet svensk allmän inrättning i ovan nämnda bestämmelse.

10.7 Informationssäkerhetsfrågor vid utkontraktering

Det offentligas utkontraktering av it-drift och andra it-baserade funktioner som tillhandahålls av den privata marknaden sätter, förutom sekretessfrågorna, också ljuset på behovet av ett stabilt informationssäkerhetsarbete som ett fundament i myndigheternas informationshantering.

En författningsreglerad tystnadsplikt med en anknytande sekretessbrytande bestämmelse syftar inte till att bli ett frikort för utkontraktering av känslig informationshantering. Även om sekretesslagstiftningen medger ett utlämnande av uppgifter kan ett sådant utlämnande i vissa fall betraktas som olämpligt ur informationssäkerhetssynpunkt. En utkontraktering får aldrig innebära att uppgifterna får ett sämre skydd ur informationssäkerhetssynpunkt än om de hade hanterats internt hos myndigheten. Framför allt behöver enskilda känna sig trygga med att uppgifter som rör deras privata förhållanden behandlas på ett rättsenligt och säkert sätt oavsett var och av vem uppgifterna hanteras. Därför bör det särskilt framhållas att myndigheters utkontraktering av informationshantering inte bara ska vara tillåten enligt sekretessregleringen. Den måste också i varje enskilt fall vara säker och i övrigt lämplig enligt regleringen om informationssäkerhet (se kapitel 9).

[108] Nils-Olof Berggren m.fl. Brottsbalken (10 november 2017, Zeteo), kommentaren till 2 kap. 3 § brottsbalken.

Med informationssäkerheten i åtanke krävs att myndigheten har ändamålsenliga och etablerade rutiner för ett systematiskt informationssäkerhetsarbete och skydd för personuppgifter. Information som utkontrakteras ska skyddas utefter vad dess känslighet kräver. En myndighet som har säkerhetsklassat sina informationstillgångar samt kontinuerligt genomfört riskanalyser har goda förutsättningar för att antingen kravställa lämplig nivå av teknisk och administrativ säkerhet vid upphandling av leverantör eller att fatta ett välgrundat beslut om att informationen inte är lämplig att utkontraktera.

Ett argument som ibland framhålls är att myndigheter bör vara försiktiga med att utkontraktera informationshantering till privata leverantörer, eftersom myndigheterna riskerar att förlora den absoluta kontrollen över sina informationstillgångar. En myndighet som bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete har emellertid goda förutsättningar att i upphandlingsunderlaget, och sedermera i form av avtalsvillkor, specificera såväl skyddskrav som krav på insyn, kontroll och uppföljning av leverantörens informationshantering.

Enligt vår bedömning kan utkontraktering i vissa fall också innebära att en myndighets informationstillgångar får ett bättre tekniskt och administrativt skydd än om myndigheten själv hade hanterat informationen, eftersom det i regel ingår i privata leverantörers affärsmodell att tillhandahålla hög kompetens inom säkerhetsområdet.

Vi bedömer sammanfattningsvis att det finns förutsättningar för myndigheter att med bibehållen god informationssäkerhet utkontraktera viss informationshantering till privata leverantörer, och att förutsättningarna därtill stärks av förslaget om en tystnadsplikt.

11 It-avtal

11.1 Avtal – en central komponent i den digitala förvaltningen

11.1.1 Kartläggningsresultatet och vårt uppdrag

Utkontraktering av it-drift och andra it-baserade funktioner har, som beskrivits i kapitel 10, kommit att bli allt mer centralt för en kostnadseffektiv och även i övrigt väl fungerande digital förvaltning. En konsekvens av detta är att avtal har blivit en allt mer väsentlig komponent i den offentliga förvaltningen.

Avtal med särskild relevans för den digitala utvecklingen inom offentlig förvaltning är de avtal som reglerar köp av it-drift eller andra it-baserade funktioner, dvs. it-avtal. Sådana avtal kan en myndighet ingå med företag i det privata näringslivet men också med en annan offentlig aktör.[1] Vid myndigheters köp av it[2] finns dessutom, under vissa förutsättningar, en laglig skyldighet att teckna personuppgiftsbiträdesavtal och säkerhetsskyddsavtal med den anlitade leverantören. Dessa typer av avtal möjliggör för en myndighet att efterleva gällande lagkrav även när viss verksamhet utkontrakteras (outsourcing). I förhållande till en utomstående aktör är alltså avtal den rättshandling som ska säkerställa att myndigheten fortsatt efterlever regelverket.

Både i vår kartläggning och genom vår samlade erfarenhet har det emellertid visat sig att ett antal myndigheter, i synnerhet små och medelstora, upplever uppenbara osäkerhetsfaktorer i sitt arbete med it-avtal. Bland annat har ett antal myndighetsrepresentanter betonat

[1] Statliga myndigheter träffar överenskommelser sinsemellan, snarare än avtal, se vidare kapitel 11.2.2.
[2] Med begreppet it avses här it-drift och andra it-baserade funktioner. Se närmare om begreppsanvändningen i kapitel 11.1.3.

komplexiteten i att dels omsätta de legala krav som åvilar myndigheten till juridiskt hållbara avtalsvillkor, dels att på ett övergripande plan teckna affärsmässigt gynnsamma it-avtal. Vid köp av it kan det röra sig om komplexa tjänster som är under snabb teknisk utveckling i kombination med svåröverblickbara affärsförhållanden hos leverantören. Detta kan sammantaget leda till att leverantören, som normalt har god kännedom om den tekniska utvecklingen och de tjänster marknaden erbjuder, har ett kunskapsövertag i förhållande till den upphandlande myndigheten.

Avtalshanteringen inom den offentliga förvaltningen är inte reglerad särskilt och vi har inte heller för avsikt att lämna författningsförslag på området. Författningsreglering riskerar att begränsa myndigheternas manöverutrymme i sitt avtalsarbete på ett sätt som inte är önskvärt. Genom kartläggningen har vi emellertid förstått att det finns ett angeläget behov, framför allt hos små och medelstora myndigheter (såväl statliga som kommunala) av utbyggt stöd i arbetet med it-avtal för att främja en trygg effektiv och innovativ utveckling av den digitala förvaltningen. Det stöd som efterfrågas omfattar vägledning kring *vad* som ska regleras i avtal och *hur* det ska regleras. Hjälp efterfrågas inte bara när det gäller generella it-avtal utan även, och kanske särskilt, när det är fråga om personuppgiftsbiträdesavtal. Därtill uppfattar vi att det finns en generell efterfrågan på kunskapshöjande åtgärder vid offentlig förvaltnings köp av it av privata leverantörer. De tjänstemän som deltar i eller ansvarar för en myndighets köp av it vill ha överblick av, och förståelse för, den privata marknadens utbud, affärsmodeller och -förhållanden för att bl.a. kunna förbättra sin förmåga att formulera juridiskt hållbara och affärsmässigt gynnsamma it-avtal.

I syfte att skapa bättre förutsättningar för att hantera rättsliga utmaningar med anledning av den fortsatta digitaliseringen av den offentliga förvaltningen är vår ansats i detta kapitel att på ett övergripande plan analysera myndigheters arbete med it-avtal och närliggande frågor. Vi kommer i det följande åskådliggöra vissa avtalsrelaterade frågor som har fångats upp i samband med vårt kartläggningsarbete och presentera den problematik som har beskrivits för oss. Därefter följer våra överväganden och förslag som vi ser har potential att skapa bättre förutsättningar för myndigheter att hantera dels rättsliga utmaningar i sitt avtalsarbete, dels utmaningar av mer metodmässig och administrativ karaktär.

11.1.2 Offentligt möter privat – upphandling och it-avtal

It-kostnader är i dag det andra största utgiftsslaget i den offentliga förvaltningens verksamhetskostnader. För statsförvaltningen beräknas it-kostnaderna uppgå till mellan 25 och 30 miljarder kronor per år. Omkring 14–16 procent av it-verksamheten är utkontrakterad, mätt i andel av de totala it-kostnaderna.[3] För kommuner och landsting saknas motsvarande uppgift om it-kostnadernas storlek och andel utkontrakterad verksamhet, men det har nämnts att statliga myndigheter, kommuner och landsting lägger sammanlagt 45 miljarder kronor på it varje år.[4]

Statliga myndigheter ska hushålla väl med statens medel[5] och kommuner, landsting och regioner ska ha en god ekonomisk hushållning i sin verksamhet.[6] I takt med den ökade digitaliseringen inom den offentliga förvaltningen kan myndigheters behov av att köpa in it från utomstående leverantörer förväntas öka och därmed också behovet av att teckna ändamålsenliga it-avtal. En del i att uppnå största möjliga kostnadseffektivitet i den digitala förvaltningen är därför att göra goda affärer genom att använda upphandling och avtal som verktyg för att öka effektivitet och kvalitet i den offentliga sektorn.

Ett framgångsrikt upphandlings- och avtalsarbete är med andra ord de nyckelfaktorer som ger förutsättningar för myndigheter att dels ta del av marknadens utbud av innovativa tjänster på ett kostnadseffektivt och juridiskt hållbart sätt, dels skapa goda förutsättningar för samverkan med myndighetens leverantörer. Med detta i beaktande blir myndigheternas it-avtal en allt mer central komponent för att säkerställa en stabil grund för den fortsatta utvecklingen mot en trygg, effektiv och innovativ digital förvaltning.

Upphandling är ett medel i den digitala omställningen som offentlig förvaltning i sin helhet står inför. Goda affärer i den offentliga förvaltningen vilar på god beställarkompetens i verksamheten.

---

[3] *Myndigheters strategiska it-projekt och it-kostnader, Delrapport it-användningsuppdraget*, Ekonomistyrningsverket, 21 december 2017, P-2017-77 och *Fördjupat it-kostnadsuppdrag, Delrapport 2: Kartläggning av it-kostnader*, Ekonomistyrningsverket, 23 oktober 2015, 2015:58.

[4] Se presentation på e-legitimationsdagen 2018 på https://www.elegnamnden.se/download/18.769a0b711614b669f29c3/1517927834469/Ardalan_Shekarabi-Digitalt_forst-nu_okar_vi_takten_i_det_offentliga_Sverige.pdf

[5] 1 kap. 3 § budgetlagen (2011:203) och 3 § myndighetsförordningen (2007:515).

[6] 11 kap. 1 § kommunallagen (2017:725).

Vid upphandling av komplexa it-tjänster omfattar beställarkompetensen en multikompetens som sällan besitts av en enskild person i verksamheten. Medarbetare med kunskap om inköpsprocesser och kunskap om it står för nyckelkompetens men det behövs även stöd från medarbetare med kunskap om juridik, informationssäkerhet och andra relevanta delar av verksamheten för att kunna genomföra en god behovs- och marknadsanalys och genomlysning av de rättsliga och säkerhetsmässiga kraven. Är myndighetens krav inte tydliga kan upphandlingsunderlaget komma att bli otydligt vilket i sin tur riskerar att återspeglas i avtalet mellan upphandlande myndighet och leverantör. En effekt av god beställarkompetens i en upphandlingsprocess är att myndigheten har goda förutsättningar att formulera och förhandla fram juridiskt hållbara och affärsmässigt gynnsamma avtalsvillkor.

Till skillnad från privaträttsliga aktörer är myndigheters avtalsfrihet till viss del begränsad, dels eftersom myndigheter i princip inte kan välja fritt vilken aktör de ska ingå affärsförbindelse med, dels eftersom avtalet behöver inkludera villkor som innebär att myndigheterna kan uppfylla gällande lagkrav. Avtalet är med andra ord det verktyg en myndighet har att i en affärsförbindelse med en utomstående leverantör specificera de krav leverantören måste uppfylla för att myndigheten i sin tur ska kunna efterleva det juridiska regelverket. De författningskrav som ställs på myndigheten behöver alltså formuleras som avtalsvillkor för att binda leverantören.

Å ena sidan kan ändamålsenligt utformade avtalsvillkor vid köp av it bidra till att en myndighet uppfyller kraven på bl.a. rättssäkerhet i verksamheten och samtidigt kan tillgodogöra sig kostnadseffektiva och innovativa lösningar i affärsmässigt gynnsamma relationer. Otydligt eller olämpligt formulerade avtalsvillkor, eller avsaknad av avtalsvillkor, kan å andra sidan resultera i bristande rättssäkerhet, inlåsningseffekter, oklara ansvarsförhållanden, kostnadsdrivande lösningar etc., vilket i sin tur kan leda till negativa konsekvenser för en myndighets förmåga att exempelvis bedriva ett effektivt digitaliseringsarbete.

11.1.3 Några begrepp

I detta kapitel ligger fokus främst på de olika typer av avtal, och i förekommande fall överenskommelser, som tecknas vid myndigheters köp av it. Dessa avtal benämner vi härefter it-avtal. Med it-avtal avser vi alla former av avtal som reglerar förhållandet mellan kund (här myndighet) och leverantör vid köp av it-drift eller andra it-baserade funktioner, t.ex. avtal om utveckling, införande, drift, förvaltning eller avveckling av it-system eller andra tjänster med it-baserade funktioner (se även kapitel 10.1.1 om terminologin). Begreppet it-avtal används med andra ord som ett samlande begrepp för bl.a. licensavtal, systemleveransavtal, supportavtal, driftsavtal, outsourcingavtal och molntjänstavtal. I det följande omfattar begreppet it-avtal, om inte annat anges, även överenskommelser mellan statliga myndigheter som rör köp av it-drift eller andra it-baserade funktioner. I kapitel 11.2.2 redogör vi närmare för skillnaden mellan civilrättsligt bindande avtal och överenskommelser.

För att beskriva kundens, dvs. myndighetens, direkta och indirekta avtalsparter använder vi begreppen (huvud)leverantör och underleverantör. Huvudleverantören är den leverantör varmed myndigheten har sitt huvudsakliga affärsförhållande. En underleverantör är en leverantör som anlitas av huvudleverantören och som har i uppdrag att bidra till att huvudleverantören uppfyller de förpliktelser som följer av it-avtalet.

I dataskyddsförordningen[7] används en parallell terminologi till begreppen huvudleverantör, underleverantör och kund (myndighet). Enligt dataskyddsförordningens reglering är en myndighet, som köper it-drift eller andra it-baserade funktioner av en (huvud)leverantör, att beteckna som personuppgiftsansvarig[8] om leverantören kommer att behandla personuppgifter på uppdrag av myndigheten. Huvudleverantören blir ett personuppgiftsbiträde[9] åt den personuppgiftsansvariga myndigheten. Om huvudleverantören anlitar underleverantörer, vars

[7] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.
[8] Personuppgiftsansvarig är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Artikel 4.7 dataskyddsförordningen.
[9] Personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning, artikel 4.8 dataskyddsförordningen.

uppdrag innefattar att behandla personuppgifter åt den personuppgiftsansvariga myndigheten, blir även dessa underleverantörer att beteckna som myndighetens personuppgiftsbiträden. Där vi behöver göra en tydlig åtskillnad mellan huvudleverantören och dess underleverantörer, som samtliga är personuppgiftsbiträden till den personuppgiftsansvariga myndigheten, använder vi begreppen (ursprungligt) personuppgiftsbiträde och underleverantör.

11.2 Avtal i den offentliga förvaltningen

11.2.1 Inledning

Avtalsrätten bygger på principerna om rätten för var och en att fritt ingå avtal (avtalsfrihet) och skyldigheten för avtalsparterna att infria avtalet (avtalsbundenhet). Avtalsfriheten innebär att individer själva ska kunna bestämma om de över huvud taget *vill* avtala, med *vem* avtalet ska ingås och *avtalsinnehållet.* Avtalsbundenheten innebär att en avtalspart är skyldig att uppfylla sina avtalslöften. Principen om avtalsbundenhet avser att tillförsäkra parterna de rättigheter som avtalen ger uttryck för.[10]

Principerna om avtalsfrihet och avtalsbundenhet gäller som utgångspunkt även när avtal tecknas av myndigheter. Men en myndighet måste parallellt förhålla sig till det offentligrättsliga regelverket som aktualiseras i dess särskilda verksamhet. Det innebär att avtalsinnehållet behöver anpassas för att säkerställa att myndigheten, när viss verksamhet t.ex. utkontrakteras, följer gällande regelverk. Till skillnad från det privata näringslivet kan en myndighet inte heller fritt välja med *vem* den vill ingå avtal. Vilken aktör som blir myndighetens avtalspart styrs i första hand av upphandlingsregelverket.

11.2.2 Statliga myndigheters avtal och andra överenskommelser

Statliga myndigheter utgör inte självständiga rättssubjekt utan är endast delar av rättssubjektet staten. I civilrättslig mening äger alltså myndigheterna inte några egna tillgångar eller något eget kapital. De

[10] Christina Ramberg och Jan Ramberg, *Avtalsrätten, En introduktion*, sjätte upplagan, 2017, Norstedts Juridik, s. 16.

förvaltar endast tillgångarna och kapitalet åt staten. En konsekvens av att myndigheterna inte utgör självständiga rättssubjekt utan endast är företrädare för staten är att de inte kan ingå civilrättsligt bindande avtal med varandra.

Ett avtal förutsätter att det sluts av två självständiga parter (rättssubjekt). Det är dock vanligt att statliga myndigheter sinsemellan i stället tecknar vad som brukar benämnas överenskommelser snarare än avtal. Det kan förutsättas att alla som berörs av en sådan överenskommelse utgår i från att den ska binda de myndigheter som träffat överenskommelsen på samma sätt som om det vore ett avtal i civilrättslig mening.[11] En viktig skillnad här är dock att statliga myndigheter inte kan lösa civilrättsliga tvister mellan sig genom att processa i allmän domstol. Staten kan så att säga inte stämma sig själv. I den händelse att myndigheter som ingått överenskommelser med varandra blir oense i frågor som träffas av överenskommelsen får sådana frågor i stället hänskjutas till regeringen eller regleras på annat sätt inom ramarna för respektive myndighets ansvar och behörighet.[12]

Utgångspunkten är således att en statlig myndighet kan ingå en överenskommelse med en eller flera andra statliga myndigheter. När det gäller en statlig myndighets köp av t.ex. it av privata leverantörer tecknas emellertid civilrättsligt bindande avtal. I det följande skiljer vi inte specifikt mellan avtal som statliga myndigheter tecknar med privata leverantörer och andra överenskommelser som ingås mellan statliga myndigheter. Utgångspunkten är i stället att även överenskommelser som myndigheter sluter sinsemellan omfattas av begreppet avtal, så som det används, i detta kapitel.

Det finns ingen särskild avtalsrätt när en statlig myndighet sluter avtal vare sig motparten är en annan myndighet eller en privat aktör. I princip aktualiseras samma avtalsrättsliga regler som vid avtal mellan enskilda. Situationen är dock speciell såtillvida att offentligrättsliga regler sätter gränsen för avtalskompetensen och även påverkar tolkningen av de avtal som myndigheten sluter. När myndigheter förfogar över ”sina” tillgångar och ”sitt” kapital genom att ingå avtal med ekonomiska förpliktelser för staten måste det ske inom ramen för det uppdrag som myndigheterna fått av företrädarna

[11] *Statliga myndigheters avtal,* (SOU 1994:136), s. 150 f.
[12] SOU 1994:136 s. 245 f. och Justitiekanslerns beslut den 13 maj 2008, dnr 8092-06-40.

för rättssubjektet staten, dvs. riksdagen och regeringen, och inom ramen för de statliga medel som är tillgängliga för myndigheterna.

Det finns inte något generellt regelverk som ger statliga myndigheter rätt att ingå avtal som innehåller ekonomiska förpliktelser för staten. Myndigheterna har dock bemyndigats att göra en rad åtaganden enligt 17 § anslagsförordningen (2011:223). En myndighet får bl.a. träffa avtal om anställning av personal, hyra av utrustning, leverans av tjänster och förbrukningsmaterial och liknande som medför utgifter under längre tid än tilldelat anslag avser, om detta är nödvändigt för att myndighetens löpande verksamhet ska fungera tillfredsställande. De åtaganden som kan göras avser framtida utgifter som är av karaktären driftkostnad.

11.2.3 Kommunala myndigheters avtal

Till skillnad från de statliga myndigheterna utgör kommuner, landsting och regioner offentliga rättssubjekt och kan således ingå civilrättsligt bindande avtal såväl över kommun- och landstingsgränserna som med myndigheter inom den statliga förvaltningen.

Det kommunala handlingsutrymmet begränsas emellertid, i viss utsträckning, av den s.k. lokaliseringsprincipen. Lokaliseringsprincipen innebär att kommuner och landsting själva får ha hand om angelägenheter av allmänt intresse som har anknytning till kommunens eller landstingets område eller dess medlemmar.[13] Utgångspunkten för kommuner och landsting är med andra ord att de ska utföra uppgifter inom den egna kommunen och för sina medlemmar.

Det är relativt vanligt att kommuner samverkar kring gemensam it-drift. Sådan samverkan kan ske t.ex. inom ramen för en gemensam nämnd eller ett kommunalförbund och är förenlig med lokaliseringsprincipen så länge samverkan avser de samverkande kommunernas uppgifter. Se även kapitel 11.3.4 om kommunutredningens förslag rörande kommunal avtalssamverkan.

[13] 2 kap. 1 § kommunallagen (2017:725).

11.3 Tidigare utredningsarbeten

11.3.1 Inledning

Den offentliga förvaltningens avtalshantering, i bemärkelsen att teckna ändamålsenliga, rättssäkra och i övrigt juridiskt hållbara och affärsmässiga avtal synes, enligt vad utredningen erfar, inte ha varit föremål för statligt utredningsarbete i någon större omfattning. Myndigheters avtalshantering förefaller traditionellt sett inom utredningsväsendet, snarast ha behandlats som ett inslag i andra bredare kontexter t.ex. i samband med utredning av upphandlingsfrågor.[14] Statliga myndigheters avtal gavs emellertid viss uppmärksamhet på 1990-talet, möjligen som en effekt av den reformerade budgetprocessen som bl.a. innebar en delegering från regeringen till myndigheterna att i allt större utsträckning fatta beslut om verksamhetens innehåll och användning av statens kapital.[15] Nedan redogörs kortfattat för huvuddragen i tre utredningsarbeten där myndigheters avtalsarbete utgjort ett större eller mindre fokus i utredningsuppdraget.

11.3.2 Utredningen om statliga myndigheters avtal

I april 1993 tillkallade regeringen en särskild utredare som bl.a. skulle överväga behovet av stöd till myndigheter i avtalsfrågor.[16] Inom ramen för utredningsarbetet genomfördes en allmän enkät om avtalsarbetet hos ett femtontal statliga myndigheter. I enkäten ställdes bl.a. frågor om vilka problem som fanns i fråga om de avtal som förekom hos myndigheten och om myndigheten behövde något stöd i avtalsfrågor. Resultatet av enkäten visade bl.a. följande.[17]

- Det kunde vara ett problem att få till stånd en rimlig kostnadsfördelning mellan myndigheten och dess motpart vid risk- och skadehantering.

[14] Se t.ex. Upphandlingsutredningens del- och slutbetänkande, *På jakt efter den goda affären – analys och erfarenheter av den offentliga upphandlingen,* (SOU 2011:73), och *Goda affärer – en strategi för hållbar offentlig upphandling,* (SOU 2013:12). Se även Upphandlingsstödsutredningens betänkande *Upphandlingsstödets framtid,* (SOU 2012:32).
[15] SOU 1994:136 s. 50.
[16] *Statliga myndigheters avtal*, (dir. 1993:60).
[17] SOU 1994:136 s. 128 f.

- Det förekom att avtal var alltför mångordiga och detaljerade samt slentrianmässigt influerade av gamla standardavtal.
- Nackdelen med standardavtal var att man inte satte sig in i villkoren och den speciella problematiken i det enskilda avtalet.

När det gällde frågan om myndigheters eventuella behov av stöd i avtalsfrågor framhöll Kammarkollegiet inom ramen för utredningen att det, enligt kollegiets uppfattning, fanns brister i kompetensen hos myndigheterna bl.a. i fråga om utformning av kravspecifikationer vid upphandling. I syfte att öka stödet för en riktig och effektiv handläggning av myndigheternas avtalsfrågor och ge myndigheterna klarare och lättare tillgängliga förhållningsregler föreslog utredningen att i en förordning om statliga myndigheters avtal samla vad som i allmänhet borde gälla om myndigheters avtalsverksamhet. Förordningsförslaget genomfördes emellertid inte.[18]

11.3.3 It-utredningen om elektronisk dokumenthantering

It-utredningen som tillsattes 1994 hade bl.a. i uppgift att utarbeta förslag till rättslig reglering som kunde behövas för användningen av elektroniska dokument inom förvaltningen och näringslivet. I utredningens betänkande behandlades frågor om hur den avtalsrättsliga regleringen kunde tillämpas i it-miljön främst vid handel inom det privata näringslivet.[19]

Utredarens utgångspunkt var att de rättsverkningar som parter avsåg att uppnå vid ingående av avtal borde kunna inträda också med användning av elektroniska rutiner. Även elektroniska förfaringssätt angavs ha till syfte att uppnå en bindande överenskommelse. Ett rättssubjekt som elektroniskt avger ett anbud eller accept borde därför bli bunden av anbudet eller svaret.[20] Utredaren menade att avtalslagen (1915:218) i huvudsak borde kunna tillämpas på de rättsfrågor som aktualiseras vid elektroniska förfaranden. Som exempel nämndes reglerna om avtals giltighet och tolkning som i princip inte är beroende av sättet för kommunikation. De moment av direkt

[18] SOU 1994:136 s. 231 f.
[19] *Elektronisk dokumenthantering,* (SOU 1996:40).
[20] SOU 1996:40 s. 121.

mänsklig vilja som i vissa fall saknas i anknytning till it synes i huvudsak inte utesluta en fungerande tillämpning av gällande rätt vid prövningen av avtals ingående och innebörd. Mot denna bakgrund menade utredaren att den avtalsrättsliga regleringen inte behövde bli föremål för några genomgripande ändringar. Sådana frågor som inte direkt föll in under någon gällande bestämmelse borde ändå kunna lösas i nära anslutning till de principer på vilka avtalslagen grundas. De omfattande regler som skulle bli följden av att detaljreglera rutiner för nya handelsmönster skulle med all säkerhet inte få den stabilitet och varaktighet som borde kännetecknа den centrala civilrätten.[21]

11.3.4 Kommunutredningen om kommunal avtalssamverkan

I oktober 2017 överlämnade Kommunutredningen sitt delbetänkande En generell rätt till kommunal avtalssamverkan.[22] Utredningens uppdrag i delbetänkandet var att utreda förutsättningarna för att ge kommunerna generella möjligheter till avtalssamverkan, dvs. möjlighet till samverkan som grundas på avtal mellan kommuner i stället för samverkan i ett kommunalförbund, i en gemensam nämnd eller i ett privaträttsligt subjekt.

Kommunutredningen konstaterade i sitt delbetänkande att det finns en utbredd efterfrågan av vidgade möjligheter till kommunal avtalssamverkan. Områden som uppmärksammats särskilt är bl.a. användning av it och digitalisering.[23][24] För att utöka möjligheterna till kommunal avtalssamverkan har Kommunutredningen föreslagit att det ska införas en generell möjlighet till sådan samverkan i kommunallagen (2017:725). Regeringen har, med anledning av utredningens förslag om kommunal avtalssamverkan, lämnat förslag på författningsändringar i kommunallagen.[25]

[21] SOU 1996:40 s. 122.
[22] *En generell rätt till kommunal avtalssamverkan,* (SOU 2017:77).
[23] SOU 2017:77 s. 18.
[24] Det saknas såvitt vi kan se generella definitioner av begreppen it och digitalisering. Med it förefaller ofta menas just informationsteknologin som sådan. Begreppet digitalisering synes däremot användas både i samband med införande av it eller informations- och kommunikationsteknik (IKT) och i samband med ändrade arbetsmetoder, organisationsprocesser, affärsmodeller och samhällsstrukturer i samband med detta införande.
[25] Lagrådsremissen, *En generell rätt till kommunal avtalssamverkan*, den 22 februari 2018.

I sitt betänkande har Kommunutredningen också övervägt om det bör införas särskilda regler om vad kommunala samverkansavtal bör innehålla. Utredningen har emellertid bedömt att övervägande skäl talar för att några sådana regler inte behövs eftersom en detaljreglering av avtalsinnehållet riskerar att minska en av de stora fördelarna med avtal som samverkansform, nämligen möjligheten att anpassa dessa till den aktuella verksamheten.[26] Däremot har utredningen framhållit att kommunala samverkansavtal åtminstone bör innehålla villkor om avtalets parter, vilka uppgifter eller tjänster som avtalet omfattar, omfattning av eventuell delegering av beslutanderätt som grundas på avtalet liksom krav på anmälan av beslut, avtalstiden och former för förlängning av denna, former för eventuella samråd och information, ordning för uppföljning av samverkansavtalet, ordning för lösandet av tvister mellan parterna, ekonomiska villkor och former för redovisning m.m. samt villkor för avtalets upphörande.[27]

Utredningen har samtidigt konstaterat att det behövs ett utvecklat stöd i upphandlingsjuridiska frågor och andra rättsliga frågor som påverkar möjligheterna till en ändamålsenlig kommunal avtalssamverkan. Mot denna bakgrund har utredningen föreslagit att Upphandlingsmyndigheten ska ges i uppdrag att, i samråd med Sveriges Kommuner och Landsting (SKL) och andra relevanta aktörer, lämna stöd till kommuner och landsting kring avtalssamverkan under åren 2018 och 2019. Det behov som utredningen har identifierat gäller avtalssamverkans förhållande till upphandlingsreglerna, men även andra rättsliga frågor som t.ex. förhållandet till kommunallagen och annan lagstiftning.[28]

11.4 Närmare om it-avtal

11.4.1 Inledning

Som framgått i kapitel 11.1.1 har vi funnit att vi bör göra analyser och lämna förslag på området som rör it-avtal i syfte att skapa bättre förutsättningar för hantering av rättsliga utmaningar med anledning av digitaliseringen av den offentliga förvaltningen. Som en bakgrund

[26] SOU 2017:77, s. 200 f.
[27] A.a. s. 22.
[28] A.a. s. 225.

till våra överväganden och förslag i kapitel 11.6, och också för att fördjupa diskussionen om vilka utmaningar myndigheter står inför vid köp av it, ser vi ett värde i att inledningsvis sätta it-avtalen i en kontext och bl.a. beskriva hur det går till när myndigheter gör köp av it. I det följande görs också några reflektioner från vår sida.

It-avtalets funktion är bl.a. att befästa den affärsmässiga relationen mellan myndigheten och leverantören, fördela ansvar och skyldigheter mellan parterna och fastställa krav på det upphandlade föremålets (tjänstens) funktion och kvalitet. I ett bredare perspektiv bör avtalet dessutom vara enkelt, begripligt och ha en ändamålsenlig struktur med väl balanserade avtalsvillkor. Avtalsvillkoren bör vara utformade på ett sätt som minimerar myndighetens beroende av leverantören.[29] Därtill bör avtalsvillkoren tillförsäkra myndigheten tillgång till effektiva uppföljningsverktyg som säkerställer nödvändig insyn och kontroll. Myndigheten behöver också ta ställning till om it-avtalet ska kompletteras med personuppgiftsbiträdesavtal och i förekommande fall säkerhetsskyddsavtal, och hur det avtalsmässiga innehållet ska formuleras för att uppfylla gällande lagkrav.

Avtalet är den avslutande länken i upphandlingskedjan som befäster det affärsmässiga förhållandet mellan upphandlande myndighet och vinnande leverantör. Besitter myndigheten god beställarkompetens och har gjort ett grundligt förarbete i form av säkerhets-, behovs- och marknadsanalys och utrett de rättsliga kraven finns goda förutsättningar att formulera juridiskt hållbara och affärsmässigt gynnsamma avtalsvillkor.

11.4.2 Avtals- och affärsförhållanden

En utgångspunkt vid köp av it är att de flesta privata leverantörer anlitar egna underleverantörer som har i uppdrag att bidra till att huvudleverantören uppfyller sina avtalsförpliktelser. Det innebär att en upphandlande myndighet måste förhålla sig inte bara till den upphandlade leverantören utan även till de underleverantörer som anlitas av huvudleverantören. Det gäller i synnerhet om underleverantörerna kommer att hantera myndighetens information i samband med utkontraktering. Myndigheten behöver ha kännedom om vilka underleverantörer som anlitas och var de är geografiskt

[29] Se om bl.a. immateriella rättigheter och inlåsningseffekter i kapitel 11.4.3.

belägna. Underleverantörerna behöver också bindas upp av samma avtalsvillkor som myndigheten har tecknat med huvudleverantören och som har i syfte att skydda informationen som hanteras och därtill säkerställer att myndigheten efterlever gällande författningskrav.

I praktiken kan det vara komplicerat att få en klar bild av en leverantörs affärsförhållanden, dvs. vilka underleverantörer som anlitas, vilka uppdrag de har och var de har sitt säte. Det gäller särskilt vid direktupphandling utan föregående avtalsförhandling eller vid användande av gratistjänster (se kapitel 11.4.4). Transparens i leverantörsledet är emellertid en nödvändighet för att myndigheten ska kunna göra en rimlig avvägning om det finns rättsliga förutsättningar för att ingå en affärsförbindelse med leverantören i fråga.

11.4.3 Vad ska it-avtalet reglera?

It-avtalet är en skriftlig dokumentation av den ingångna affären och ska utöver kraven på tjänstens kvalitet och funktion också reglera alla andra relevanta förhållanden mellan parterna. Avtalet är sällan en statisk produkt utan kan omförhandlas, inom de ramar som upphandlingslagstiftningen ger. Omförhandling kan t.ex. vara nödvändigt vid förändrade behov hos myndigheten eller om leverantören ändrar i den tillhandahållna tjänsten.

I vårt kartläggningsarbete har, som tidigare nämnts, vissa aktörer gett uttryck för att det kan vara komplicerat att formulera förutsebara, juridiskt hållbara och för myndigheten affärsmässigt gynnsamma avtalsvillkor i it-avtal. I vårt arbete har vi fångat vissa specifika områden som synes vara särskilt svåra att bemästra inom ramen för avtalsarbetet. Det rör sig bl.a. om att formulera avtalsvillkor som säkerställer att

- risker och ansvar fördelas på ett ändamålsenligt sätt mellan parterna,
- myndigheten kan tillgodogöra sig den tekniska utveckling som äger rum under avtalets löptid,
- myndigheten inte drabbas av framtida inlåsningseffekter, dvs. inte låses fast vid befintlig leverantör och dennes lösningar och system,

- nödvändiga avtalsuppföljningar kan genomföras,
- myndigheten kan återfå sin information i ett användbart format vid avtalets upphörande,
- leverantören förbinder sig att samarbeta vid ett framtida leverantörsbyte,
- sanktionsbestämmelser är ändamålsenligt utformade.

Även med beaktande av det förslag som vi lämnat i kapitel 10 om en författningsreglerad tystnadsplikt ser vi att behov kan kvarstå av att också i avtalsförhållandet reglera en tystnadsplikt för leverantören i förening med civilrättsliga sanktioner. Vi har också uppfattat en oro över att avtal som innehåller villkor som är ofördelaktiga för myndigheten förr eller senare kan ge ekonomiskt kännbara konsekvenser.

Nedan redogörs närmare för bl.a. upphovsrättsliga frågor och några av de ovan kort presenterade områdena som har koppling till s.k. inlåsningseffekter. Enligt vad vi erfar, kan dessa områden aktualisera särskilda utmaningar när det gäller att formulera ändamålsenliga avtalsvillkor som uppfyller en myndighets nuvarande och framtida behov.

Immateriella rättigheter m.m.

Den avtalsmässiga regleringen av immateriella rättigheter har olika stor betydelse beroende på vilket det aktuella avtalsobjektet är, t.ex. licenser vid avtal om it-drift eller rätten till resultatet av ett utvecklingsarbete. Enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk (upphovsrättslagen) har den som skapat ett datorprogram upphovsrätt till verket. Upphovsrätten omfattar även förberedande designmaterial för datorprogram, t.ex. flödesscheman, diagram eller annat material som nyttjats för utvecklandet av ett datorprogram.[30] Datorprogram har ett starkt upphovsrättsligt skydd, dels eftersom de anses vara speciellt känsliga för otillåtet

[30] 1 § första stycket 2 och tredje stycket upphovsrättslagen.

bruk, dels för att investeringskostnaderna för att utveckla nya datorprogram ofta är höga.[31] Det är programvaran[32] som innehåller den information som är föremål för upphovsrätt dvs. datorprogram. Programvaran består dock inte enbart av datorprogram utan även av teknisk information samt dokumentation som är nödvändig för att stödja och underhålla programvaran, teknisk know-how och eventuella databaser. Datorprogrammet i sig är text med programkoder som ger instruktioner till datorn, s.k. källkod. Källkoden är en central del av en programvara och det är i regel källkodens format och uttryck, dvs. kodens diverse former, som omfattas av det upphovsrättsliga skyddet. Däremot skyddas inte skärmbildsuttrycket dvs. källkodens funktion och bakomliggande idéer.[33]

Utöver skydd för datorprogram innehåller upphovsrättslagen även visst skydd för sammanställningar eller databaser, enligt det s.k. katalogskyddet (databasskydd).[34] För att skyddet ska realiseras krävs att databasen innehåller en sammanställning av ett stort antal uppgifter och att den är resultatet av en väsentlig investering. Det är databasens struktur som omfattas av det upphovsrättsliga skyddet och inte dess innehåll, dvs. inte uppgifterna i databasen.[35]

Vid köp av it kan parterna avtala om att upphovsrätten till en programvara ska övergå helt till beställaren, här myndigheten, eller att myndigheten ska få viss nyttjanderätt till programvaran. Det kan finnas anledning att lägga särskild vikt och noggrannhet kring utformningen av de avtalsvillkor som styr överlåtelse av upphovsrätt eller upplåtelse av nyttjanderätt. Enligt den praxis som utformats inom området tolkas alltför omfattande och otydliga eller ”tysta” avtal normalt sett restriktivt, till upphovsmannens fördel, enligt den s.k. specifikationsprincipen.[36]

Ofta är det emellertid tillräckligt att myndigheten i avtal får en långtgående nyttjanderätt till en programvara och att upphovsrätten ligger kvar hos leverantören. Men när en leverantör anlitas för ett

[31] *Upphandling av IT – inlåsningseffekter och möjligheter*, uppdragsforskningsrapport 2013:2, Konkurrensverket, s. 21.
[32] En samling datorprogram, eller datorprogram i allmänhet kallas ofta programvara eller mjukvara. Se https://sv.wikipedia.org/wiki/Datorprogram
[33] A.rapport s. 22.
[34] 49 § upphovsrättslagen.
[35] Se vidare om databasskyddet t.ex. Johan Axhamn, *Databasskydd*, Stockholms Universitet, 2016.
[36] Se genomgång av praxis i Upphovsrättsutredningens delbetänkande, *Avtalad upphovsrätt*, (SOU 2010:24), s. 94 f.

större utvecklingsarbete kan det vara nödvändigt att äganderätten till förberedande designdokument och till resultatet, t.ex. ett specialanpassat it-system,[37] övergår till myndigheten för att myndigheten själv ska kunna göra framtida ändringar eller vidareutveckla systemet (se även kapitel 7.4.2).

Vid köp av it, även utan inslag av utvecklingsarbete som leder till ett specifikt avtalat resultat, kan det också vara angeläget för myndigheten att avtala om överlåtelse av äganderätt till leverantörens dokumentation av systemet, s.k. driftdokumentation. Även driftdokumentation kan åtnjuta upphovsrättsligt skydd om den har tillräckligt hög grad av originalitet. Vanligen är denna typ av dokumentation så pass omfattande att den därigenom blir originell.[38]

Även av andra anledningar kan det vara angeläget att i avtal reglera att leverantörens upphovsrätt inte hindrar myndigheten från att få nödvändig insyn i de datorprogram som t.ex. ligger till grund för eller påverkar myndighetens automatiserade beslutsfattande. I kapitel 7 lämnar vi bl.a. förslag som innebär att en myndighet ska kunna ge information om hur myndigheten vid handläggning av mål eller ärenden använder algoritmer och datorprogram, som helt eller delvis påverkar utfallet eller beslutet vid automatiserade beslutsförfaranden (se kapitel 7.7.2). En förutsättning för att en myndighet ska kunna lämna sådan information, när en utomstående leverantör har utvecklat det datorprogram inkluderande algoritmer som används för beslutsfattandet, är att myndigheten får viss insyn eller i vart fall en övergripande förklaring från leverantören så att myndigheten å sin sida kan förklara för t.ex. tillsynsmyndigheter eller allmänheten hur dess verksamhet bedrivs.

Vid sidan av den traditionella upphovsrätten kan algoritmer och datorprogram som utvecklats av en privat leverantör också åtnjuta skydd enligt lagen (1990:409) om skydd för företagshemligheter. Med företagshemlighet avses sådan information om affärs- eller driftförhållanden i en näringsidkares rörelse som näringsidkaren håller hemlig och vars röjande är ägnat att medföra skada för honom

[37] Med it-system avses t.ex. ett system som används för att samla in, lagra, bearbeta och distribuera information med allmänt utformade eller specialanpassade datorprogram och/eller hårdvara.
[38] Agne Lindberg m.fl., *It-avtal – särskilt om outsourcing,* 2009, Norstedts Juridik, s. 144 med där införd hänvisning till Marianne Levin, *Lärobok i immaterialrätt,* 2007, Wolters Kluwer, s. 76 f. Se även Peter Adamsson m.fl., Lagarna inom immaterialrätten (1 december 2013, Zeteo) kommentaren till 1 § upphovsrättslagen.

i konkurrenshänseende. Med information förstås både sådana uppgifter som har dokumenterats i någon form, inbegripet ritningar, modeller och andra liknande tekniska förebilder, och enskilda personers kännedom om ett visst förhållande, även om det inte har dokumenterats på något särskilt sätt.[39] En myndighet behöver emellertid alltid kunna ta ansvar för sin verksamhet, t.ex. när det gäller automatiserat beslutsfattande, varför det måste finnas balans mellan parternas intressen (se vidare kapitel 7.7.1 och 7.7.2).

Inlåsningseffekter

Vid köp av it finns det alltid en risk att en myndighet fastnar i ett långvarigt beroendeförhållande till det företag som levererar tjänsten i fråga och att det då uppstår en s.k. inlåsningseffekt. En komplex teknisk lösning kan kräva att myndigheten behöver stadigvarande tillgång till leverantörens kunskap om systemet för att t.ex. komma i åtnjutande av underhåll och uppgradering. Myndighetens behov av underhåll och uppgradering kan leda till att avtalsförhållandet blir svårt att komma ur. Har en myndighet t.ex. inte avtalat om en vidsträckt förfoganderätt över en programvara som tillhandahålls av en leverantör, kan myndigheten vara förhindrad att anlita en annan leverantör eller att själv utföra support, underhåll och uppgradering. En teknisk inlåsning till en viss leverantör leder alltså inte sällan till ytterligare former av inlåsningar, t.ex. avtals- och kompetensmässig inlåsning.

Att en inlåsningseffekt uppstår kan bero på olika orsaker. I vissa fall rör det sig om att myndigheten har ställt krav på särskilda standarder, filformat eller programvaror som enbart kan tillhandahållas av en leverantör. I andra fall kan det bero på att det företag som levererar en specifik tjänst, t.ex. ett it-system, äger vissa immateriella rättigheter, t.ex. upphovsrätt, för den programvara som används av myndigheten. Om det it-system som är knutet till leverantörens immateriella rättigheter är av väsentlig betydelse för myndighetens verksamhet kan det vara kostsamt och förenat med stora svårigheter, eller till och med omöjligt, att byta leverantör.

[39] 1 § lagen (1990:409) om skydd för företagshemligheter. En ny lag om företagshemligheter har föreslagits träda i kraft den 9 juni 2018. Se lagrådsremissen *En ny lag om företagshemligheter*, den 8 februari 2018.

Att ta sig ur en inlåsning kan alltså vara både svårt och förenat med avsevärda kostnader men det finns olika sätt att minimera risken för att inlåsningseffekter uppstår. Redan i upphandlingens inledande fas kan myndigheten i sin kravspecifikation t.ex. precisera krav på programvara utan referens till specifika tekniker, leverantörer, varumärken eller slutna standarder som kontrolleras av enskilda företag. Därtill kan myndigheten formulera avtalsvillkor som innebär att leverantörens upphovsrätt inte begränsar myndighetens möjlighet att anlita andra leverantör för framtida support och utvecklingsarbeten. Myndigheten bör också i avtalet säkerställa att en upphandlad leverantör åtar sig att medverka vid ett framtida leverantörsbyte. Under de senaste åren har bl.a. flera forskningsrapporter förordat att myndigheter, i sina upphandlingar, bör ställa krav på öppna standarder och interoperabilitet för att motverka framtida inlåsningssituationer.[40]

11.4.4 Anskaffningsprocesser och it-avtal med privata leverantörer

Anskaffningsprocesser

För köp av it kan vi se fyra olika anskaffningsprocesser som leder fram till avtalsförhållanden med privata leverantörer nämligen:

1. avtal vid avrop från ramavtal,
2. avtal vid en annonserad upphandlingsprocess,[41]
3. avtal vid direktupphandling, och
4. avtal vid användande av kostnadsfri webbaserad tjänst.

Nedan redogörs för vart och ett av dessa områden med de anknytande frågeställningar som vi här finner relevanta. En skillnad mellan de olika anskaffningsförfarandena är att vid en annonserad upphandling

[40] Se t.ex. *It-standarder, inlåsning och konkurrens, En analys av policy och praktik inom svensk förvaltning*, uppdragsforskningsrapport 2016:2, Konkurrensverket, och *Upphandling av it – inlåsningseffekter och möjligheter*, uppdragsforsningsrapport 2013:2, Konkurrensverket.
[41] Här avses de upphandlingsformer som framgår av 6 kap. 1 § lagen (2016:1145) om offentlig upphandling. Vi har inte gjort någon åtskillnad mellan de olika upphandlingsförfarandena utan främst utgått i från processen med öppet förfarande (punkten 1 i nämnda paragraf).

sker en stor del av avtalsarbetet, såvitt gäller innehållet i avtalsvillkoren, när myndigheten tar fram sin kravspecifikation och övrigt upphandlingsunderlag. Vid direktupphandling kan två varianter förekomma beroende på typ av tjänst och leverantör som upphandlas. Antingen sker avtalsarbetet på det sätt som beskrivits ovan dvs. genom att myndigheten tar fram kravspecifikation och övrigt upphandlingsunderlag. Men vid direktupphandling, och även vid användning av gratistjänster, förekommer också att avtalsarbetet sker genom granskning och eventuell förhandling av villkoren i leverantörens standardavtal.

It-avtal vid avrop från ramavtal

Myndigheter kan upphandla ramavtal för sina egna behov eller göra en gemensam upphandling med andra myndigheter i syfte att teckna ramavtal som ska gälla gemensamt för de myndigheter som ingår i samarbetet. Ramavtal upphandlas också av s.k. inköpscentraler. Syftet med inköpscentraler är att effektivisera den offentliga sektorns upphandling av vissa varor och tjänster vilket ska leda till minskade administrationskostnader och bättre inköpsvillkor.[42]

Ramavtal är utformade efter de behov som har identifierats under upphandlingens förstudie, exempelvis vilka krav som ska ställas på leverantören och upphandlingsföremålet. Vid avrop från ramavtal görs i regel en förnyad konkurrensutsättning genom att avropande myndighet skickar ut en avropsförfrågan till ramavtalsleverantörerna att lämna anbud i enlighet med de villkor som angetts i ramavtalet. Myndigheten får i avropet precisera och komplettera villkor i enlighet med vad som framgår av ramavtalet.

En fördel med att avropa från ramavtal är att en avropande myndighet kan dra nytta av inköpscentralens upphandlarkompetens. Myndigheten behöver fortfarande besitta god beställarkompetens och utifrån behovsanalysen formulera sina krav. Men myndigheten behöver inte själv formulera affärsmässiga och juridiskt hållbara avtalsvillkor eftersom inköpscentralen, inom ramen för sin upphandling av ramavtalsleverantörerna, redan förhandlat fram ändamålsenliga avtal. Avtalen kan dock, i den mån det är tillåtet, behöva justeras utifrån omständigheterna i det enskilda fallet. Avtalspaketet

[42] 1 kap. 14 § lagen om offentlig upphandling.

kan också, i förekommande fall, behöva kompletteras med exempelvis informationssäkerhetsmässiga krav, personuppgiftsbiträdesavtal och säkerhetsskyddsavtal. Andra fördelar med att avropa från befintliga ramavtal är att avropande myndighet ofta har möjlighet att fråga inköpscentralen om råd under avropsprocessen och att upphandlingstiden kan förkortas.

It-avtal vid en annonserad upphandlingsprocess

Upphandling är ett strategiskt verktyg som rätt använt, bidrar till att öka effektivitet och kvalitet i den offentliga sektorn. En myndighet som avser att upphandla it måste kunna beskriva myndighetens krav på själva upphandlingsföremålet, t.ex. funktion och kvalitet, och vilka övriga krav som ställs på leverantören såväl i anbudsförfarandet som under avtalstiden (specifikation och kravställning).[43]

Vid köp av komplexa tjänster tenderar upphandlingsarbetet att bli tämligen komplicerat. Oavsett om den upphandlande myndigheten försöker hantera svårigheterna genom att vara mycket detaljerad i upphandlingen, eller genom att tillämpa mer öppna avtalsvillkor, finns det fallgropar. I det förstnämnda fallet krävs att myndigheten själv har en detaljerad kunskap om den tjänst, t.ex. it-drift eller andra it-baserade funktioner, som ska upphandlas. En alltför detaljerad kravspecifikation kan dock leda till att nya och effektiva tekniker utesluts. En mindre detaljerad styrning i kravspecifikationen kan i och för sig bidra till att nya och mer effektiva lösningar kan prövas, men det finns samtidigt en risk att leverantörens ökade frihet leder till oönskade resultat eller leveranser för myndigheten.

I upphandlingens avslutande skede ska de krav, öppna eller detaljerade, som myndigheten identifierat i sitt inledande arbete dokumenteras i avtalet. Kommer leverantören att hantera myndighetens information behöver avtalet innehålla villkor som speglar de rättsliga krav som ställs på myndighetens informationshantering. Det kan röra sig om krav som härrör från regleringen av informationssäkerhet, bevarande och gallring, sekretess, dataskydd etc. Utan villkor som säkerställer myndighetens regelefterlevnad kan

[43] Avser upphandlingen en tjänst som är av mer komplex natur kan myndigheten använda sig av någon av de mer flexibla upphandlingsformerna som konkurrenspräglad dialog, förhandlat förfarande eller innovationspartnerskap.

myndigheten inte, i ett senare skede, ställa krav på leverantören att vidta de åtgärder som krävs för att uppfylla gällande rätt.

I kartläggningsarbetet vittnar ett antal myndighetsrepresentanter dels om att det är svårt att lyckas med upphandlingar där den levererade tjänsten faktiskt motsvarar myndighetens krav, dels om att avtalshanteringen är komplicerad. Särskilt bland små och medelstora myndigheter framhålls att det råder en viss obalans i kunskapsnivån mellan beställande myndighet och de leverantörer som deltar i ett upphandlingsförfarande. Små och medelstora myndigheter har i regel svårt att hålla all den nödvändiga kompetens som behövs för att säkerställa att en upphandlingsprocess resulterar i affärsmässiga och juridiskt hållbara lösningar och en tjänst som motsvarar myndighetens krav.

För stöd i upphandlingsprocessen tillhandahåller Upphandlingsmyndigheten vägledning, metoder och verktyg med koppling till bl.a. lagen (2016:1145) om offentlig upphandling (se kapitel 11.5.1). Men det avtalsmässiga innehållet och formerna för avtalets ingående när själva upphandlingsprocessen är slutförd regleras inte av upphandlingsregelverket. I upphandlingsregelverket finns bestämmelser om när avtal får tecknas, men inte hur.[44] Generellt gäller att avtalsvillkoren ska baseras på annonsen, upphandlingsdokumenten, anbudet och resultatet av eventuell förhandling samt rättelse, förtydligande eller komplettering. Några övriga ändringar eller tillägg får i princip inte göras. Upphandlande myndighet behöver därför i sitt förberedande arbete ta ställning till inte bara vilka krav som ska ställas på själva tjänsteleveransen, utan också förutse informationssäkerhetmässiga krav och eventuellt behov av personuppgiftsbiträdesavtal etc. Det sagda pekar återigen på vikten av god beställarkompetens och att utföra ett grundligt förarbete i form av analyser, specifikation och kravställning innan en upphandling annonseras.

It-avtal vid direktupphandling

Webbaserade tjänster är i dag tillgängliga på ett sätt som, för många av oss, var helt otänkbart för 20 år sedan. Det är troligt att denna utveckling har lett till en ökad förekomst av direktupphandling av

[44] Se reglerna om avtalsspärr i 20 kap. 1–3 §§ lagen om offentlig upphandling.

digitala tjänster, ofta s.k. molntjänster,[45] som finns tillgängliga på internet. Vid direktupphandling av den här typen av tjänster förekommer inte alltid direktkontakt eller avtalsförhandling med leverantören i fråga. I stället utgår leverantören vanligen i från att dess kunder, offentlig förvaltning eller inte, accepterar leverantörens standardavtal vilket kan ske genom att kunden i helt webbaserat förfarande godkänner avtalsvillkoren. Denna typ av avtal kallas ibland klickavtal. Det är förstås inte uteslutet att avtalsförhandling sker mellan upphandlande myndighet och leverantören i fråga, men kartläggningsarbetet och utredningens samlade erfarenhet talar för att det ännu inte är särskilt vanligt med förhandling vid köp på internet av den här typen av tjänster.

Beroende på vilken tjänst och vilken leverantör det är fråga om kan standardavtalen vara mer eller mindre omfattande och svårtolkade. Det är inte ovanligt att standardavtalen är mer komplicerade än tjänsterna i fråga och det kan vara en grannlaga uppgift att granska samtliga avtalsdokument och kontrollera hur avtalsvillkoren förhåller sig dels till varandra, dels till det regelverk myndigheten har att efterleva. Inte desto mindre är avtalsgranskning och -förhandling av avgörande vikt för att säkerställa att en upphandlande myndighet inte accepterar villkor som står i strid med författningskrav eller som på annat sätt kan leda till kännbara framtida konsekvenser för myndigheten. Här bör myndigheten bl.a. uppmärksamma om avtalet innehåller olämpliga villkor om lagval och tvistelösning. Inte sällan hänvisas till amerikansk lag, om leverantören har sitt säte i USA, och att tvistelösning ska ske i amerikansk domstol eller skiljenämnd. Därtill kan avtalet innehålla villkor som ger främmande makts myndigheter, eller andra aktörer, omfattande möjligheter att ta del av den information som leverantören hanterar på uppdrag av myndigheten (se även kapitel 10.1.3). Vidare behöver myndigheten uppmärksamma villkor som ger leverantören möjlighet att ensidigt ändra avtalsvillkoren eller att självsvåldigt avgöra om det finns skäl att innehålla (suspendera) tjänsten eller avsluta avtalsförhållandet i förtid. Standardavtalen är därtill ofta avfattade på engelska och det kan vara påfallande komplicerat att tolka avtalsvillkoren i en svensk juridisk kontext.

[45] En molntjänst kan beskrivas som en tjänst som tillhandahålls med nätverksåtkomst och där resursdelning, skalbarhet, självbetjäning och betalning efter användning eller volym är några av de centrala kännetecknen. Se *Molntjänster i staten, en ny generation av outsourcing* Pensionsmyndigheten, januari 2016.

Vi har inte för avsikt att här gå igenom samtliga omständigheter en myndighet behöver vara uppmärksam på vid avtalsgranskningen, eftersom det givetvis beror på vilken typ av tjänst som upphandlas och i vilket syfte den ska användas. En aspekt som har lyfts fram vid ett par tillfällen i vårt arbete är dock frågan om transparens i leverantörsledet. Utan direktkontakt med leverantören kan det vara svårt, ibland omöjligt, för upphandlande myndighet att bilda sig en uppfattning om vilka eventuella underleverantörer som kan komma att hantera den information myndigheten registrerar i tjänsten och var dessa underleverantörer har sin hemvist. Detta försvårar för myndigheten att t.ex. göra rimliga juridiska bedömningar i sekretess- och dataskyddshänseende.

It-avtal vid kostnadsfri webbaserad tjänst

Tjänster som, i monetära termer, tillhandahålls gratis och där inga dolda ersättningar utgår till leverantören är undantagna från upphandlingsregelverket. Ett kännetecken för vad som kan betecknas som gratistjänster och som tillhandahålls på webben är att de är fritt tillgängliga för var och en att använda. Det innebär att vem som helst, när som helst, kan teckna ett konto, acceptera avtalsvillkoren och börja använda tjänsten. Här rör det sig i princip uteslutande om s.k. molntjänster och det är vanligt att avtal ingås med leverantören direkt på internet genom att kunden accepterar ett s.k. klickavtal. Enligt vad utredningen erfar är det relativt vanligt att myndigheter använder den här typen av tjänster för att t.ex. dela dokument digitalt. Antingen internt inom myndigheten eller externt med andra parter (se även kapitel 12.2.8).

Standardavtal som reglerar användning av kostnadsfria webbaserade tjänster tenderar att vara omfattande och kan därtill innehålla en mängd hänvisningar och webblänkar till andra dokument eller webbpublicerad information. Det leder sammantaget till att det kan vara besvärligt att få en klar överblick av hela avtalspaketet. Liksom har beskrivits ovan om it-avtal vid direktupphandling är det emellertid angeläget att en myndighet granskar och förhandlar om avtalsvillkor som inte kan accepteras. Att det rör sig om tjänster som tillhandahålls i ett standardutförande betyder inte att avtalsvillkor, som rör annat än själva tjänstebeskrivningen, behöver vara standardiserade.

Avtal som reglerar användningen av en kostnadsfri tjänst kan innehålla villkor som är fördelaktiga för leverantören men mindre förmånliga för användaren. Det kan röra sig om omfattande friskrivningsklausuler, reglering av tillämplig lag och jurisdiktion vid en eventuell tvist etc. Innan ett eventuellt avtal ingås behöver myndigheten därför kontrollera att myndigheten, genom avtalsvillkoren, ges förutsättningar att efterleva tillämplig lagstiftning. Det rör sig framför allt om dataskyddsregleringen men även arkiv- och sekretessregleringen kan aktualiseras liksom tryckfrihetsförordningens bestämmelser om allmänna handlingar.

11.4.5 Köp av it från annan statlig myndighet

Det är relativt vanligt förekommande att en statlig myndighet tillhandahåller it-drift eller andra it-baserade funktioner åt en eller flera andra myndigheter i statsförvaltningen. Vad vi här avser med köp av it från annan statlig myndighet är sådana situationer, där en myndighet, i stället för att vända sig till den privata marknaden, köper it av en annan myndighet.[46]

Vi har inte för avsikt att på ett djupare plan redogöra för eventuella avtalsmässiga utmaningar som följer av en statlig myndighets köp av it av en annan statlig myndighet. Vi kan dock kort konstatera, som tidigare framhållits i kapitel 11.2.2, att statliga myndigheter inte kan ingå civilrättsligt bindande avtal med varandra eftersom de inte är självständiga rättssubjekt utan delar av rättssubjektet staten. Statliga myndigheter ingår emellertid regelmässigt överenskommelser som till sin karaktär motsvarar innehållet i ett civilrättsligt avtal. Sådana överenskommelser som rör köp av it behöver naturligtvis, på samma sätt som vid köp från en privat leverantör, också uppfylla de legala krav och krav på säkerhet samt skydd för informationen etc. som den inköpande myndigheten har att efterleva.

11.4.6 Personuppgiftsbiträdesavtal

En myndighet som köper it av en leverantör, privat eller offentlig, behöver teckna ett personuppgiftsbiträdesavtal, eller motsvarande avtalsvillkor, med leverantören om denne kommer att behandla

[46] När det gäller gränsen mot det upphandlingspliktiga området se kapitel 9.6.2.

personuppgifter på uppdrag av myndigheten. Personuppgiftsbiträdesavtal behöver emellertid inte tecknas om personuppgiftsbiträdets hantering av personuppgifter är reglerad av en rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt (se vidare nedan under avsnittet om *Olika metoder att teckna personuppgiftsbiträdesavtal*).[47]

Syftet med personuppgiftsbiträdesavtal är bl.a. att säkerställa att de personuppgifter som behandlas av leverantören (personuppgiftsbiträdet) får samma skydd hos leverantören som om myndigheten (personuppgiftsansvarig) själv hade behandlat uppgifterna. Avtalet ska också garantera nödvändig insyn i, och kontroll av, personuppgiftsbiträdets behandling av personuppgifterna och borga för transparens mellan avtalsparterna. Avtalet kan sägas vara ett verktyg för myndigheten att uppfylla sina lagstadgade skyldigheter enligt dataskyddsregleringen.

De rättsliga kraven på personuppgiftsbiträden och nödvändigt avtalsinnehåll regleras av dataskyddsförordningen.[48] Regleringen är förhållandevis långtgående och detaljerade krav ställs på innehållet i personuppgiftsbiträdesavtal. Avtalet ska bl.a. föreskriva att personuppgiftsbiträdet

- enbart får behandla personuppgifter enligt dokumenterade instruktioner från den personuppgiftsansvarige,
- enbart får anlita en underleverantör[49] om den personuppgiftsansvarige gett sitt skriftliga tillstånd och om underleverantören åläggs samma skyldigheter i fråga om dataskydd som gäller för det ursprungliga personuppgiftsbiträdet,
- ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå,
- ska bistå den personuppgiftsansvarige att uppfylla sina skyldigheter i fråga om anmälan om personuppgiftsincident, information till den registrerade om incidenten m.m.,
- ska radera eller återlämna alla personuppgifter, inklusive kopior, till den personuppgiftsansvarige när personuppgiftsbiträdets uppdrag avslutas,

[47] Artikel 28.3 dataskyddsförordningen.
[48] Se bl.a. artikel 28 dataskyddsförordningen.
[49] För vår definition av begreppet underleverantör se kapitel 11.1.3.

- ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att skyldigheterna har fullgjorts samt möjliggöra och bidra till granskningar och inspektioner, som genomförs av den personuppgiftsansvarige eller av en revisor som utsetts av den personuppgiftsansvarige.

I dataskyddsförordningen har införts bestämmelser om att en tillsynsmyndighet får fastställa standardavtalsklausuler för personuppgiftsbiträdesavtal i enlighet med förordningens mekanism för enhetlighet.[50] Sådana standardavtalsklausuler kan bl.a. omfatta ovan uppräknade områden.

Utformning av avtalsvillkor

Av de aktörer som har bidragit i vårt kartläggningsarbete har flera framfört att det är besvärligt att ta fram personuppgiftsbiträdesavtal som innehållsmässigt uppfyller kraven i dataskyddsregleringen. Det rör sig inte i första hand om *vad* som ska regleras utan snarare *hur* avtalsvillkoren ska utformas för att uppfylla förordningens krav på insyn i, och kontroll av, leverantörens behandling av personuppgifter och nödvändig transparens i leverantörsledet. De områden som synes vara särskilt utmanande att omsätta till juridiskt hållbara och förutsebara avtalsvillkor har vi uppfattat vara bl.a. följande.

- Hur ett skriftligt förhandstillstånd för personuppgiftsbiträdet att anlita underleverantörer kan utformas. När och på vilket sätt den personuppgiftsansvarige ska informeras om personuppgiftsbiträdets planer på att anlita eller ersätta en underleverantör och under vilka rimliga förutsättningar den personuppgiftsansvarige kan motsätta sig att en viss underleverantör anlitas.
- Hur underleverantörer, som anlitas av personuppgiftsbiträdet, kan åläggas samma skyldigheter som personuppgiftsbiträdet har ålagts i personuppgiftsbiträdesavtalet.
- Hur den personuppgiftsansvarige kan säkerställa att personuppgiftsbiträdet, och eventuella underleverantörer, rapporterar samtliga relevanta personuppgiftsincidenter.[51]

[50] Artiklarna 28.8, 57.1 j, 58.3 g, 63 och 64.1 d dataskyddsförordningen.
[51] Se om personuppgiftsincidenter i artiklarna 4.12 och 33.2 dataskyddsförordningen.

- Hur den personuppgiftsansvarige kan genomföra effektiv och ändamålsenlig kontroll och uppföljning av att personuppgiftsbiträdet, inklusive underleverantörer, fullgör sina skyldigheter.
- På vilken detaljnivå de tekniska och organisatoriska säkerhetsåtgärderna som personuppgiftsbiträdet ska vidta, behöver formuleras i avtalet.

Ett par aktörer har vidare framhållit att avtalsarbetet i viss utsträckning borde gå att standardisera, i synnerhet när det rör sig om behandling av personuppgifter i tjänster som tillhandahålls i standardutförande.

Olika metoder att teckna personuppgiftsbiträdesavtal

Enligt dataskyddsförordningens reglering är det i huvudsak den personuppgiftsansvarige som ansvarar för att teckna personuppgiftsbiträdesavtal, eller motsvarande avtalsvillkor, med sitt eller sina personuppgiftsbiträden.[52] Dataskyddsförordningens bestämmelser om personuppgiftsbiträdesavtal synes bl.a. ha i syfte att i viss utsträckning underlätta avtalshanteringen för personuppgiftsansvariga. Så sker exempelvis genom att ett personuppgiftsbiträde som efter den personuppgiftsansvariges tillstånd anlitar en eller flera underleverantörer, ansvarar för att underleverantörerna binds av samma villkor för dataskydd som gäller för det ursprungliga biträdet. Någon motsvarande bestämmelse som i sin tur kan underlätta personuppgiftsbiträdens avtalshantering finns emellertid inte. Det innebär att personuppgiftsbiträden kan ha en utmanande uppgift att upprätta och förvalta personuppgiftsbiträdesavtal.

Kartläggningen har visat att formerna för att binda personuppgiftsansvariga och personuppgiftsbiträden, inklusive underleverantörer, vid avtalet i fråga kan vara förenat med avsevärda utmaningar. Flera representanter från både det offentliga och från det privata har påtalat för oss att det läggs ned oproportionerligt mycket tid och resurser på både utformning och förvaltning av personuppgiftsbiträdesavtal. För en personuppgiftsansvarig står i praktiken två olika förfaranden till buds för att binda ett personuppgiftsbiträde

[52] Artikel 28 dataskyddsförordningen.

och dess underleverantörer till avtalsvillkor som reglerar hur personuppgifterna får behandlas.

Den personuppgiftsansvarige kan välja att teckna separata personuppgiftsbiträdesavtal med varje underleverantör som agerar i rollen som personuppgiftsbiträde. Separata personuppgiftsbiträdesavtal med samtliga relevanta underleverantörer kan emellertid leda till en i det närmaste oöverskådlig mängd avtal för den personuppgiftsansvarige. Att förvalta en sådan mängd avtal är både tids- och resurskrävande.

Ett annat alternativ är att den personuppgiftsansvarige ger det ursprungliga personuppgiftsbiträdet i uppdrag att teckna personuppgiftsbiträdesavtal med samtliga relevanta underleverantörer. Ett personuppgiftsbiträde som fått i uppdrag att teckna personuppgiftsbiträdesavtal med sina underleverantörer ansvarar för att dessa åläggs samma skyldigheter i fråga om dataskydd som gäller för det ursprungliga personuppgiftsbiträdet. Därtill ansvarar personuppgiftsbiträdet, gentemot den personuppgiftsansvarige, för att underleverantörerna uppfyller sina skyldigheter enligt avtalsvillkoren.[53]

Som tidigare nämnts finns emellertid ingen särskild reglering i dataskyddsförordningen som underlättar avtalshanteringen för personuppgiftsbiträden. I den offentliga sektorn gör sig problemet särskilt gällande när en offentlig eller privat aktör, i rollen som personuppgiftsbiträde, tillhandahåller standardiserade tjänster till myndigheter i den offentliga förvaltningen. Som ett beskrivande exempel kan nämnas Inera AB[54] som på uppdrag av bl.a. landsting, regioner och kommuner har att utveckla och förvalta gemensamma digitala tjänster för vårdgivare. Inera AB, som agerar i rollen som personuppgiftsbiträde, tillhandahåller standardiserade tjänster med anslutande standardiserade personuppgiftsbiträdesavtal till ett stort antal personuppgiftsansvariga vårdgivare. Att personuppgiftsbiträdesavtalen kan standardiseras beror på att de personuppgiftsansvariga vårdgivarna behandlar samma typer av personuppgifter för samma eller liknande ändamål och omfattas av samma regelverk. Men trots att personuppgiftsbiträdesavtalens innehåll kan standardiseras saknas uttalade rättsliga förutsättningar som kan underlätta personuppgiftsbiträdets, här Inera AB:s, avtalshantering i den del som avser

[53] Artikel 28.4 dataskyddsförordningen.
[54] Inera AB är ett företag som ägs gemensamt av SKL Företag, landsting, regioner och kommuner.

avtals ingående och förvaltning. Det innebär, för ett personuppgiftsbiträde som tillhandahåller en standardiserad tjänst till ett stort antal personuppgiftsansvariga, en avtalsförvaltning som kan vara påtagligt resurs- och kostnadsdrivande. När separata personuppgiftsbiträdesavtal behöver tecknas med varje personuppgiftsansvarig kan det medföra att t.ex. generella avtalsjusteringar eller förlängning av kontraktstid behöver genomföras i hundratals separata men likalydande avtal.

Kravet på personuppgiftsbiträdesavtal är emellertid inte absolut. Ett alternativt förfarandesätt är att reglera personuppgiftsbiträdets behandling av personuppgifter i en EU-rättsakt eller i nationell författning.[55] I en departementspromemoria har exempelvis ett förslag lämnats som syftar till att ge Lantmäteriet rätt att meddela föreskrifter om personuppgiftsbiträdens behandling av personuppgifter i fastighetsregistret.[56] Lantmäteriet är personuppgiftsansvarig för fastighetsregistret och kommuner och kommunala lantmäterimyndigheter agerar i rollen som personuppgiftsbiträden när de för in uppgifter i registret. Vilka delar av fastighetsregistret som de kommunala lantmäterimyndigheterna och kommunerna får föra in och ta bort uppgifter i framgår redan av författning.[57] Enligt departementspromemorian framstår det som lämpligt att ytterligare krav på personuppgiftsbiträdenas behandling av personuppgifter i fastighetsregistret regleras i författning och inte i avtal.[58]

11.4.7 Säkerhetsskyddsavtal

Säkerhetsskyddsavtal är inte ett område som har lyfts fram särskilt i vårt kartläggningsarbete och vi avser inte att lägga fram några överväganden eller förslag i denna del. Vi vill ändå kortfattat belysa vikten av säkerhetsskyddsavtal och dess syfte att säkerställa att information, som omfattas av säkerhetsskyddslagen (1996:627) och som hanteras av en utomstående leverantör, får samma skydd hos leverantören som hos den utkontrakterande myndigheten. En grundtanke inom säkerhetsskyddslagstiftningen är att de intressen

[55] Artikel 28.3 dataskyddsförordningen.
[56] *Anpassningar av de fastighetsrättsliga, associationsrättsliga, transporträttsliga och immaterialrättsliga författningarna till dataskyddsförordningen*, (Ds 2017:19), kapitel 5.4.3.
[57] Se t.ex. 19 kap. 6 § fastighetsbildningslagen (1970:988).
[58] A.a. s. 129.

som lagstiftningen slår vakt om ska ha samma skydd oavsett om verksamheten bedrivs av det allmänna eller av enskilda. Enligt säkerhetsskyddslagen gäller att när staten avser att begära in anbud eller träffa avtal om upphandling där det förekommer uppgifter som med hänsyn till rikets säkerhet omfattas av sekretess, ska staten träffa ett skriftligt säkerhetsskyddsavtal med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet. Detsamma gäller för kommuner och landsting.[59] Ett säkerhetsskyddsavtal som träffats inför en anbudsinfordran ska revideras i erforderlig utsträckning när avtal träffas om upphandling.[60] Säkerhetsskyddsavtal ska träffas såväl med huvudleverantören som med dess eventuella underleverantörer.

Säkerhetsskyddslagen är för närvarande föremål för översyn och en ny säkerhetsskyddslag föreslås träda i kraft den 1 april 2019.[61] Regleringen av säkerhetsskyddsavtal i förslaget till ny säkerhetsskyddslag motsvarar till viss del nuvarande reglering men bestämmelsen har utvidgats.[62] En del i utvidgningen är att säkerhetsskyddsavtal ska ingås vid upphandling och efterföljande ingående av avtal om varor, tjänster eller byggentreprenader där det förekommer säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller över.[63] Säkerhetsskyddslagens krav på att teckna säkerhetsskyddsavtal gäller även för det fall leverantören har sin juridiska hemvist i ett annat land.

11.4.8 Förvaltning av it-avtal – uppföljning och kontroll

Avtalsförvaltning och avtalsuppföljning

Avtalsförvaltning är en central del av en upphandlande myndighets arbete med att uppnå en god affär. En aktiv avtalsförvaltning möjliggör avtalets fulla potential och kan bidra till kvalitets- och verksamhetsutveckling. Begreppet avtalsförvaltning omfattar bl.a. intern

[59] 8 § första stycket säkerhetsskyddslagen.
[60] 7 kap. 8 § Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd (PMFS 2015:3).
[61] *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag*, prop. 2017/18:89.
[62] Förslag till 2 kap. 6 § ny säkerhetsskyddslag.
[63] Prop. 2017/18:89 s. 105. Av förslag till 2 kap 2 § ny säkerhetsskyddslag följer att säkerhetsskyddsklassificerade uppgifter ska, utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet, delas in i säkerhetsskyddsklasserna kvalificerat hemlig, hemlig, konfidentiell och begränsat hemlig.

administration t.ex. att registrera avtalet i en intern avtalsdatabas och hantera eventuella förlängningar och prisjusteringar. Avtalsförvaltning innebär också att arbeta med avtalstrohet, dvs. att styra organisationens köp till den leverantör myndigheten har avtal med. Det kan exempelvis göras genom informationsinsatser om avtalet och genom att förenkla beställningsvägar.[64]

Avtalsförvaltning avser också avtalsuppföljning och begreppen används ibland synonymt. Med avtalsuppföljning menar vi här sådana aktiviteter som syftar till att säkerställa att leverantören uppfyller de krav som har ställts i förfrågningsunderlaget, och som sedermera har dokumenterats i avtalet, och att den upphandlande myndigheten får det som upphandlats. Men avtalsuppföljning är inte bara relevant för att myndigheten ska kunna försäkra sig om leverantörens avtalsefterlevnad. Betydelsen av avtalsuppföljning har även framhållits av företag i den mening att det, om uppföljning inte sker, finns risk för att mindre nogräknade företag anger att de uppfyller kraven i ett upphandlingsunderlag, trots att så inte är fallet.[65]

Uppföljning av it-avtal

Det finns ingen uttrycklig laglig skyldighet för en upphandlande myndighet att följa upp it-avtal under avtalens löptid (se dock nedan om uppföljning av personuppgiftsbiträdesavtal och säkerhetsskyddsavtal). Men en förutsättning för att säkerställa att en upphandlande myndighet bl.a. efterlever likabehandlingsprincipen och tillämpar ett öppet och objektivt förfarande är att myndigheten kontrollerar leverantörens möjlighet att uppfylla ställda upphandlingskriterier.[66] Avtalsuppföljningen bör inkludera krav på leverantören (dvs. kvalificeringskraven), krav på tjänsten, utvärderingskriterierna och övriga kontraktsvillkor.[67]

Upphandlingsutredningen, vars uppdrag bl.a. var att utvärdera upphandlingsregelverket ur ett ekonomiskt och samhällspolitiskt

[64] Se vidare om avtalsförvaltning i *Avtalsförvaltning, vägledning nr 2*, Upphandlingsmyndigheten, 2016.
[65] SOU 2012:32 s. 145 f.
[66] 4 kap. 1 § lagen om offentlig upphandling och EU-domstolens dom C-448/01 EVN och Wienstrom punkterna 50–52.
[67] Se Upphandlingsmyndighetens webbplats, http://www.upphandlingsmyndigheten.se/upphandla/Processen-for-LOU/avtalsforvaltning/genomfor-uppfoljningen/

perspektiv, framhöll i sitt delbetänkande att upphandlande myndigheters uppföljning av avtal var mycket bristfällig vilket gjorde att myndigheterna riskerade att inte få det de betalade för. Upphandlingsutredningen beskrev därtill att leverantörer och näringslivsorganisationer, under utredningsarbetet, framfört att kontrakt och genomförda upphandlingar alltför sällan följdes upp eller utvärderades av de upphandlande myndigheterna.[68]

Upphandlingsstödsutredningen, vars förslag låg till grund för Upphandlingsmyndigheten, framhöll att allt fler upphandlande myndigheter under senare år blivit medvetna om att de har bristfälliga system för avtalsuppföljning och att det finns ett ökande intresse att organisera avtalsuppföljning på ett adekvat sätt.[69]

I den Nationella upphandlingsstrategin betonar regeringen vikten av en väl fungerande avtalsuppföljning bl.a. för att visa anbudsgivare att avtal verkligen följs.[70] Om ingångna avtal inte följs upp riskerar de upphandlande myndigheterna att förlora i kvalitet och effektivitet samt i sin trovärdighet som avtalspartner. Samtidigt bidrar bristande avtalsuppföljning till att oseriösa leverantörer kan delta i konkurrensen om offentliga kontrakt.

Bilden av att det generellt sett finns utrymme att förbättra myndigheters rutiner för avtalsuppföljning har bekräftats inom ramen för vårt arbete. Av våra kontakter med privata leverantörer inom it-branschen har vi bl.a. förstått att det är ovanligt att myndigheter gör avtalsuppföljningar på plats hos leverantören. I de fall det sker förekommer det att uppföljningen, enligt leverantörernas mening, inte har ett tydligt fokus. Saknar myndigheten t.ex. en konkret revisionsplan blir målet med, och resultatet av, uppföljningen otydligt.

Uppföljning av personuppgiftsbiträdesavtal

Avtalsuppföljning enligt dataskyddsförordningen har givits en särställning i den bemärkelsen att personuppgiftsbiträdet är skyldigt att medverka till att sådan uppföljning kan ske.[71] Personuppgiftsbiträdet ska möjliggöra och bidra till granskningar och inspektioner

[68] SOU 2011:73 s. 18 och 147.
[69] SOU 2012:32 s. 145.
[70] Nationella upphandlingsstrategin
http://www.regeringen.se/globalassets/regeringen/dokument/finansdepartementet/pdf/2016/upphandlingsstrategin/nationella-upphandlingsstrategin.pdf.
[71] Artikel 28.3 h dataskyddsförordningen.

som genomförs av den personuppgiftsansvarige eller av en revisor utsedd av den personuppgiftsansvarige. I personuppgiftsbiträdesavtalet, eller motsvarande avtalsvillkor, som upprättas mellan den personuppgiftsansvarige och dennes personuppgiftsbiträde (och eventuella underleverantörer) ska anges att den personuppgiftsansvarige ska ges tillgång till all information som krävs för att visa att biträdet har fullgjort sina skyldigheter enligt avtalet och dataskyddsförordningen.

Uppföljning av säkerhetsskyddsavtal

I förslaget till ny säkerhetsskyddslag är det uttryckligen reglerat att verksamhetsutövaren är skyldig att kontrollera att leverantören följer säkerhetsskyddsavtalet.[72] Även om en myndighet redan i dag bör kontrollera säkerhetsskyddet hos en upphandlad leverantör har lagstiftaren, genom att reglera kravet på kontroll i lag, förtydligat vikten av att avtalsuppföljning sker. Kontrollskyldigheten innebär ett åliggande att se till att avtalsvillkoren följs.

11.5 Befintligt avtalsstöd

11.5.1 Upphandlingsmyndigheten

Upphandlingsmyndigheten har det samlade ansvaret för att utveckla, förvalta och stödja den upphandling som genomförs av upphandlande myndigheter och enheter. Myndigheten ska också ge stöd till leverantörer. Stödet ska bl.a. bidra till att upphandlingar hanteras strategiskt, genom metodutveckling eller på annat sätt och att upphandlingar planeras, genomförs, följs upp och utvärderas på ändamålsenligt sätt.[73] Upphandlingsmyndigheten tillhandahåller vägledningar om bl.a. offentlig avtalssamverkan, kontraktsuppföljning, ändringar av kontrakt och ramavtal, avtalsförvaltning m.m.[74] I Upphandlingsmyndighetens vägledningar *Avtalsförvaltning* och *Kontraktsuppföljning* ges bl.a. stöd och rekommendationer för hur avtalsuppföljning kan ske och vad som bör kontrolleras.

[72] Förslag till 2 kap. 6 § andra stycket ny säkerhetsskyddslag, prop. 2017/18:89.
[73] 1 och 2 §§ förordningen (2015:527) med instruktion för Upphandlingsmyndigheten.
[74] Se Upphandlingsmyndighetens webbplats under fliken publikationer.

11.5.2 Kammarkollegiet

Kammarkollegiet ansvarar för att upphandla samordnade ramavtal avsedda för andra statliga myndigheter. Inom området informationsteknik gäller ansvaret hela den offentliga förvaltningen, dvs. även kommuner, landsting och regioner. I uppgiften ingår att tillhandahålla stödverksamhet för inköp vid avrop från de samordnade ramavtal som myndigheten har upphandlat. Myndigheten ska vidare verka för att bästa möjliga villkor skapas för myndigheternas anskaffning av varor och tjänster.

Inom området informationsteknik ska Kammarkollegiet särskilt beakta förvaltningsgemensamma standarder samt intresset av innovationer och teknikneutrala lösningar.[75] Vid Kammarkollegiet är det Statens inköpscentral som har i uppdrag att ingå ramavtal för andra statliga myndigheter. Statens inköpscentral tillhandahåller stöd och vägledning till avropande myndigheter och leverantörer genom att erbjuda seminarier, webbinarier och nyhetsbrev. Det finns även möjlighet till personlig kontakt för att t.ex. ställa juridiska frågor om ramavtalen. Statens inköpscentral publicerar förfrågningsunderlag och befintliga ramavtal på webben (avropa.se). Myndigheter är fria att använda materialet som förlaga i egna upphandlingar vilket, enligt Kammarkollegiet, också sker i relativt stor utsträckning.

11.5.3 Datainspektionen

Datainspektionen[76] är tillsynsmyndighet enligt dataskyddsförordningen och i myndighetens uppdrag ingår bl.a. att övervaka och verkställa tillämpningen av dataskyddsförordningen.[77] Inom ramen för sitt uppdrag har Datainspektionen befogenhet att anta standardavtalsklausuler för personuppgiftsbiträdesavtal.[78] På Datainspektionens webbplats finns allmän information om kravet på innehåll i personuppgiftsbiträdesavtal och vad som gäller i fråga om underleverantörer och personuppgiftsbiträdesavtal. Datainspektionen har också tagit fram ett informationsmaterial, Molntjänster och personuppgiftslagen, vari redogörs för de grundläggande krav som ställs på

[75] 8 a § förordningen (2007:824) med instruktion för Kammarkollegiet.
[76] Datainspektionen kommer under år 2018 byta namn till Integritetsskyddsmyndigheten.
[77] Artikel 57.1 a dataskyddsförordningen.
[78] Artiklarna 28.8, 57.1 j, 58.3 g och 64.1 d dataskyddsförordningen.

innehållet i ett personuppgiftsbiträdesavtal som tecknas med en molntjänstleverantör.[79]

11.5.4 Säkerhetspolisen och Försvarsmakten

Säkerhetspolisen får enligt sin instruktion ge råd om säkerhetsskydd.[80] I Säkerhetspolisens föreskrifter och allmänna råd finns viss ledning om hanteringen av säkerhetsskyddsavtal i samband med säkerhetsskyddad upphandling.[81] Som ytterligare stöd för myndigheternas arbete har Säkerhetspolisen tagit fram en vägledning för säkerhetsskyddad upphandling, mallar för säkerhetsskyddsavtal och exempel på sekretessförbindelse.[82] Även Försvarsmakten, som är tillsynsmyndighet för vissa myndigheter enligt säkerhetsskyddsförordningen tillhandahåller en handbok om säkerhetsskyddad upphandling med säkerhetsskyddsavtal.[83]

11.5.5 Sveriges kommuner och landsting

Sveriges Kommuner och Landsting (SKL) ger rådgivning till kommuner, landsting och regioner inom upphandlingsområdet. Via SKL Kommentus[84] bedrivs dels en nationell inköpscentral som erbjuder en bred portfölj av ramavtal bl.a. inom områdena för inköp av it och andra tjänster som rör digitalisering, dels en konsultverksamhet som erbjuder kvalificerat stöd och utbildningar inom inköp och upphandlingsområdet. SKL Kommentus erbjuder personlig ramavtalsservice för bl.a. kommuner, landsting och regioner som vill ha stöd i den praktiska tillämpningen av ramavtalen. SKL har därtill tagit fram en mall för personuppgiftsbiträdesavtal och en checklista som t.ex. kan användas för att stämma av att ett befintligt personuppgiftsbiträdesavtal uppfyller de rättsliga kraven i dataskyddsförordningen.

---

[79] Se https://www.datainspektionen.se/Documents/faktablad-molntjanster.pdf Informationsbladet är senast reviderat i oktober 2016.
[80] 6 § förordningen (2014:1103) med instruktion för Säkerhetspolisen.
[81] 7 kap. 6 § Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd (PMFS 2015:3).
[82] Se Säkerhetspolisens webbplats, sakerhetspolisen.se.
[83] Se 39 § säkerhetsskyddsförordningen (1996:633) och *Säkerhetsskyddad upphandling med säkerhetsskyddsavtal* (M7739-352025).
[84] SKL Kommentus är ett bolag som ägs gemensamt av SKL (genom SKL Företag AB) och en majoritet av kommunerna.

Inom området för molntjänster, särskilt vid användning av sådana tjänster inom skolväsendet, har SKL tagit fram en vägledning som också inkluderar avtalshanteringen.[85]

11.6 Våra överväganden och förslag

11.6.1 Inledande överväganden

I det följande redogörs för några inledande överväganden inom ett par områden som rör avtal i den offentliga förvaltningen och som vi har uppmärksammat inom ramen för vårt arbete. Det rör för det första digital avtalshantering i bemärkelsen digitala metoder för avtals ingående och digitaliserad avtalsförvaltning i den del som främst avser avtal som digital originalhandling och påföljande ändringar och tillägg i sådana avtal. Det andra området vi har uppmärksammat är behovet av att följa upp ingångna avtal, dvs. nödvändigheten av att myndigheter följer upp it-avtal, personuppgiftsbiträdesavtal och säkerhetsskyddsavtal för att säkerställa att leverantören lever upp till de överenskomna villkoren.

Som vi tidigare har beskrivit är myndigheters avtalsförvaltning till stora delar oreglerad. Det saknas med andra ord rättsregler för hur myndigheter ska förvalta sina avtal. Även om vi inte har för avsikt att lämna specifika förslag kring hur myndigheter ska ingå och förvalta sina avtal vill vi ändå framhålla att det bör finnas stora vinster för myndigheter i den offentliga förvaltningen att övergå till digital avtalshantering. Det gäller förstås ur effektivitets- och kostnadsperspektiv men digitala avtal har också potential att säkra avtalets innehåll och således också den gemensamma partsviljan.

Digitalt avtalstecknande

It-utredningen framhöll för drygt 20 år sedan att de rättsverkningar som parter avser att uppnå genom att ingå avtal bör kunna inträda också med användning av elektroniska rutiner.[86] I dag är det knappast någon som ifrågasätter att avtalsbundenhet och rättsverkningar uppstår också när avtal ingås genom helt digitala förfaranden.

[85] Personuppgiftsbiträdesavtal, checklista och vägledning finns tillgängliga på skl.se.
[86] SOU 1996:40.

Trots det synes det traditionella sättet att ingå en avtalsförbindelse, dvs. genom underskrift med penna på papper, fortfarande vara det vanligaste tillvägagångssättet. Den ökande användningen av bl.a. molntjänster har dock fört med sig användning av andra former för avtals ingående. Det kan exempelvis vara fråga om att kunden, med ett enkelt klick i en ruta, bekräftar att avtalsvillkoren accepteras.

Dessa två varianter, penna på papper och s.k. klickavtal, kan betraktas som två ytterligheter där den förstnämnda normalt sett föregås av omfattande kontakt och avtalsförhandling mellan avtalsparterna innan avtalet bekräftas genom att en behörig företrädare signerar dokumenten i fråga. Ett klickavtal däremot, kan i regel ingås av vem som helst, när som helst. Den här formen av digitalt avtalstecknande, som främst används vid köp eller användande av molntjänster, kan vara förenat med vissa risker för kunden dvs. myndigheten. I kapitel 11.4.4 har vi redogjort för några områden som bör uppmärksammas särskilt när den här typen av avtal tecknas. En ytterligare aspekt som behöver beaktas vid ingående av klickavtal är att leverantören normalt sett har begränsade möjligheter att kontrollera att dennes avtalspart faktiskt har behörighet att företräda sin organisation att ingå avtal med leverantören i fråga.

Syftet med ett avtal är att ge uttryck för den gemensamma partsviljan. Genom att avtalsbundenhet uppstår är respektive part skyldig att uppfylla sina avtalslöften. Det finns inga legala formkrav för ingående av it-avtal. Enligt vad vi erfar är det dock, vid sidan av klickavtal, relativt ovanligt att myndigheter använder sig av digital teknik vid avtalstecknande. Det synes emellertid finnas stor utvecklingspotential inom detta område. Användning av den digitala tekniken bör t.ex. kunna säkerställa att endast en behörig företrädare har möjlighet att binda sin verksamhet vid ett visst avtal. Därtill ger tekniken bättre förutsättningar att kontrollera *vem* som tecknat avtal och *när* det har skett, t.ex. genom att kombinera en digital underskrift med någon form av identifiering exempelvis e-legitimation.[87]

[87] Utredningen om effektiv styrning av nationella digitala tjänster har analyserat behovet av elektroniska identitetshandlingar i tjänsten, *reboot – omstart för den digitala förvaltningen*, (SOU 2017:114), kapitel 15.

Digitala avtal

Avtal i den offentliga förvaltningen är som ovan beskrivits, i vart fall initialt, ofta pappersbaserade. Ett vanligt hjälpmedel vid förvaltningen av avtal är emellertid att registrera ingångna avtal i en särskild avtalsdatabas. En avtalsdatabas kan ge en myndighet bra överblick och struktur över de avtal myndigheten har ingått. Förutom att tillhandhålla verksamheten information om avtalen och dess innehåll kan en avtalsdatabas också ge stöd i uppföljningen genom att t.ex. bevaka giltighetstider, optioner, prisjusteringar och behovet av att genomföra generell uppföljning av avtalsvillkoren. Men oavsett om en avtalsdatabas används eller inte är det ofta otympligt att hantera t.ex. ändringar och tillägg i avtal som initialt har hanterats i pappersformat eftersom det inte går att ändra direkt i avtalstexten. I stället får ändringar och tillägg tillföras t.ex. i bilagor till avtalet. Avtal med lång löptid kan över tid innehålla en mängd ändringar och tillägg vilket bl.a. leder till att det blir svårt att överblicka avtalsinnehållet.

Enligt vad utredningen erfar har teknikutvecklingen med blockkedjor skapat nya möjligheter för digital avtalsförvaltning. Här synes finnas en ny potential att förenkla och effektivisera myndigheters avtalsarbete. Blockkedjetekniken kan t.ex. komma att användas för att verifiera att ett visst dokument utgör en digital avtalshandling i ursprungligt skick samtidigt som ändringar och kompletteringar i ursprungsfilen kan knytas till viss person och viss tidpunkt.[88] Möjligheten att spåra ändringar till person och tidpunkt kan vara av avgörande betydelse t.ex. om det uppstår en tvist om avtalsinnehållet mellan parterna.

Sammanfattande reflektioner – digitala avtal och avtalstecknande

I kartläggningen har det framkommit att det arbete som är förknippat med it-avtal och personuppgiftsbiträdesavtal kan kräva avsevärda personella och tidsmässiga resurser. Utgångspunkten är ofta att avtalen, i vart fall i det initiala skedet, hanteras i pappershandlingar. Ändringar och tillägg görs i regel genom att bilagor tillförs det ursprungliga avtalet.

[88] Se även kapitel 12.2.1 om originalinnehåll och originalexemplar.

Enligt vår uppfattning finns det inom ramen för digitaliseringens möjligheter flera potentiella lösningar för att reducera onödig resursåtgång vid avtalsförvaltning. Här kan i jämförande syfte nämnas det föreslagna kravet på elektroniska fakturor som utfärdas till följd av upphandling. Förslaget är ett steg i arbetet med att uppnå en papperslös offentlig förvaltning och förväntas leda till en samhällsekonomisk nytta om närmare 1,4 miljarder kronor under en sjuårsperiod.[89] Vi menar att det också finns stora effektivitetsvinster för den offentliga förvaltningen i att också övergå till digital avtalshantering.

Den digitala tekniken stödjer för det första möjligheten att ingå avtal genom digitala underskrifter. Det innebär t.ex. att flera avtalsparter över tid på ett enkelt sätt kan ansluta sig till ett och samma avtal. Detta kan i sin tur generera verksamhetsnytta för en aktör som t.ex. tillhandahåller en standardiserad tjänst med anslutande standardiserat personuppgiftsbiträdesavtal för en avgränsad sektor i den offentliga förvaltningen. På så sätt kan antalet avtal som ska förvaltas reduceras betydligt. En digital underskrift som därtill har kombinerats med digital identifiering, t.ex. e-legitimation, säkerställer dessutom vem som vid ett visst tillfälle har undertecknat avtalet i fråga.

För det andra kan den digitala tekniken, t.ex. med blockkedjor, komma att förenkla och effektivisera avtalsförvaltningen genom att spårbara ändringar och kompletteringar kan föras in i avtalet under dess löptid. Om ändringar kan göras direkt i avtalstexten leder det bl.a. till bättre överskådlighet av hela avtalet, särskilt när det löper under längre tid. Tekniken kan därtill komma att ge förutsättningar att säkerställa vem som har utfört ändringarna i ett avtalsdokument och när ändringarna i fråga har genomförts. Med stöd av tekniken kan alltså genomförandet av tillägg och ändringar i befintliga avtal påtagligt förenklas och effektiveras.

[89] Lagrådsremissen *Elektroniska fakturor till följd av offentlig upphandling*, den 1 februari 2018, som föreslår en ny lag om elektroniska fakturor till följd av offentlig upphandling. Den föreslagna lagen genomför Europaparlamentets och rådets direktiv 2014/55/EU av den 16 april 2014 om elektronisk fakturering vid offentlig upphandling.

Uppföljning av avtal

En systematisk avtalsuppföljning ger en myndighet förutsättningar att säkerställa att den får det som den betalar för. En sådan uppföljning skapar också tilltro till den offentliga upphandlingen och bidrar till leverantörers vilja att delta i konkurrensen. Upphandlingsmyndigheten har, i syfte att stödja myndigheters uppföljning och utvärdering av upphandling, publicerat lättillgänglig och konkret information om avtalsförvaltning i hela dess vidd dvs. inklusive avtalsuppföljning. En allmän reflektion från vår sida är också att myndigheter, som en effekt av den diskussion rörande säkerhetsskydd som tilltog under sommaren 2017,[90] har börjat höja ambitionsnivån när det gäller uppföljning av it-avtal. Det är positivt att frågan om avtalsuppföljning nu uppmärksammas i högre grad och vår bedömning är att den offentliga förvaltningen har goda förutsättningar att skapa rutiner för ändamålsenlig avtalsuppföljning med stöd av de vägledningar som redan finns tillgängliga.

Uppföljning av personuppgiftsbiträdesavtal och säkerhetsskyddsavtal är särskilt reglerat i dataskyddsförordningen respektive i förslaget till ny säkerhetsskyddslag. Enligt vår uppfattning bör en generellt förbättrad uppföljning av it-avtal även få effekter för uppföljningen av personuppgiftsbiträdesavtal och säkerhetsskyddsavtal. Avtalsuppföljning behöver ske med fokus på den upphandlande tjänsten och därför bör lämpligen all uppföljning i förhållande till en och samma leverantör kunna göras i ett sammanhang, oavsett typ av avtal.

Med beaktande av den beskrivna utveckling som nu äger rum vad gäller avtalsuppföljning ser vi inte anledning att lämna några särskilda förslag inom detta område.

[90] Se bl.a. Wikipedia, *Transportstyrelsen it-upphandling*, 11 januari 2018 och utskottsdokument 2016/17:dnr2581.

11.6.2 Utökat stöd för it-avtal

Utredningens bedömning: Myndigheterna i den offentliga förvaltningen bör tillhandahållas stöd i arbetet med att formulera juridiskt hållbara och affärsmässigt gynnsamma villkor i it-avtal.

Utredningens förslag: Myndigheten för digital förvaltning ska få i uppdrag att främja den offentliga förvaltningens digitala investeringar genom att stödja myndigheters inköps- och avtalsprocesser och bidra till spridning av goda exempel.

Skälen för utredningens bedömning och förslag

Allt mer komplexa it-avtal

Behovet av avtalsstöd utreddes för drygt 20 år sedan av Utredningen av statliga myndigheters avtal.[91] Vid det tillfället lades inget förslag fram om statligt organiserat avtalsstöd eftersom behovet ansågs tillgodosett bl.a. genom utredningens förslag till förordning om statliga myndigheters avtal.

Som tidigare nämnts realiserades aldrig utredningens författningsförslag. Under den tid som har förflutit sedan nämnda utredning lämnade sitt förslag har, enligt vår uppfattning, avtalsarbetet inom den offentliga förvaltningen ökat påtagligt. En orsak till detta är växande utkontraktering och inköp av it från utomstående leverantörer. Därtill har it-avtalen ändrat karaktär. Från att ha varit avtal med fokus på leverans av hårdvara har it-avtalen i dag främst fokus på tjänster och programvara. När avtalen tidigare beskrev den teknik som användes, är avtalen i dag inriktade på bl.a. funktioner och ansvar.[92] Denna förändring har bidragit till att de it-avtal som tecknas i dag är långt mer komplexa än de avtal som upprättades i början av 1990-talet. Utöver it-avtalens komplexitet medför den snabba teknikutvecklingen att det tenderar att råda en viss obalans i kunskapsnivån mellan avtalsparterna, dvs. myndigheten och leverantören. Leverantören har normalt sett god kännedom om den tekniska utvecklingen, om it-branschen i stort och om de tjänster

[91] SOU 1994:136.
[92] Agne Lindberg m.fl., s. 84.

marknaden erbjuder vilket kan leda till ett ojämlikt avtalsförhållande, till leverantörens fördel. Sammantaget ser vi en bild som visar att det kan vara påfallande svårt för en myndighet att teckna it-avtal som är både juridiskt hållbara och affärsmässigt gynnsamma. Mot denna bakgrund bedömer vi att myndigheters behov av avtalsstöd, som konstaterades redan för 20 år sedan, kvarstår och dessutom har ökat i omfattning, specifikt inom området för it-avtal.

Det avtalsmässiga innehållet

De avtalsvillkor som tecknas vid köp av it behöver å ena sidan vara tillräckligt flexibla för att ge parterna manöverutrymme om nya behov uppstår eller om ny teknik erbjuds som myndigheten vill tillgodogöra sig. Å andra sidan behöver avtalsvillkoren också vara tillräckligt tydliga och förutsebara för att skapa en tillitsfull och stabil affärsrelation mellan parterna.

Standardavtal har vissa fördelar genom att de regelmässigt innehåller reglering av relevanta områden mellan parterna. Men det finns också nackdelar med standardavtal om de hanteras alltför rutinmässigt. Även när en myndighet använder sina egna standardavtal är det viktigt att villkoren anpassas efter omständigheterna i det enskilda fallet. Grundar sig affärsförhållandet på leverantörens standardavtal är det än mer angeläget för myndigheten att noggrant ta del av samtliga villkor, tolka dem i förhållande till varandra, och förhandla om villkor som inte kan accepteras. Avtalsvillkoren behöver både vara juridiskt hållbara utifrån det regelverk myndigheten har att följa och affärsmässigt gynnsamma för att t.ex. bidra till kostnadseffektivitet i förvaltningen.

Nyckelkomponenter i ett framgångsrikt avtalsarbete kan sammanfattas i termer av att identifiera samtliga relevanta förhållanden som behöver regleras mellan parterna och att formulera ändamålsenliga och balanserade avtalsvillkor. Frågan är emellertid hur detta närmare ska gå till. Avtalstexten bör t.ex. inte innehålla villkor med oklar innebörd eller villkor med inbördes motstridigheter. Inom ramen för kartläggningsarbetet har vi identifierat ett antal områden myndigheterna pekat ut som särskilt komplicerade att formulera tydliga förutsebara avtalsvillkor kring (se kapitel 11.4.3). Det rör bl.a. villkor som fördelar risker och ansvar, villkor som säkerställer

myndighetens rätt till nödvändig insyn m.m. utan hinder av immateriella rättigheter eller bestämmelser om företagshemligheter och villkor som i övrigt säkerställer att myndigheten inte drabbas av framtida inlåsningseffekter.

I den offentliga förvaltningen finns ett visst stöd att få för myndigheterna i deras arbete med it-avtal (se kapitel 11.5). Det stöd som erbjuds är emellertid främst inriktat på generella vägledningar och omfattar inte i någon större utsträckning specifik vägledning i utformning av avtalsinnehållet. Det kan i och för sig argumenteras för att varje avtal är specifikt och måste anpassas efter den särskilda situationen som råder. Vi instämmer delvis i detta argument, men menar också att det finns vissa områden som är mer eller mindre allmänt förekommande i de flesta it-avtal och som bör kunna ta sin utgångspunkt i standardiserade formuleringar som kan anpassas utifrån varje enskild situation.

Myndigheter som behöver specifikt stöd eller vägledning i sitt arbete med formulera avtalsvillkor kan redan i dag ta hjälp av den privata marknaden. Utifrån vår kartläggning har vi emellertid uppfattat att det finns en efterfrågan på kunskapshöjande åtgärder inom området, oavsett om myndigheten själv står för avtalsarbetet eller anlitar extern hjälp. Det kan vara fråga om såväl komplexa tekniska tjänster och affärsförhållanden på leverantörens sida som komplicerade och omfattande avtal som ska tecknas. Det framstår med andra ord som önskvärt med förvaltningsgemensamma åtgärder för att stötta myndigheter med viss kunskap på området, oavsett om extern hjälp därtill anlitas vid tecknandet av specifika avtal.

Vår bedömning är därför att det befintliga stöd för it-avtal som i dagsläget tillhandahålls av bl.a. Upphandlingsmyndigheten och Kammarkollegiet skulle kunna kompletteras med t.ex. mer konkreta exempel och förslag kring identifiering och utformning av vissa avtalsvillkor vid myndigheters köp av it.

Stöd i myndigheters arbete med it-avtal

Som redogjorts för i kapitel 11.4.4 kan de anskaffningsprocesser som leder till avtalsbundenhet se ut på många olika sätt. I ena änden av spektrat finns den annonserade upphandlingen där avtalsarbetet ingår som en komponent i hela processen. I andra änden finns de s.k.

klickavtalen där avtalsbundenhet kan uppstå genom att kunden (myndigheten), utan föregående kontakt eller avtalsförhandling med leverantören, accepterar avtalsvillkoren direkt på webben. I det första fallet är det till största del myndighetens ansvar att formulera juridiskt hållbara och affärsmässigt gynnsamma avtalsvillkor. I det andra fallet handlar det snarare om att granska leverantörens avtal och identifiera eventuella avtalsvillkor som myndigheten inte kan acceptera och behöver förhandla om med leverantören för att avtal ska kunna ingås. Det avtalsstöd som här diskuteras bör kunna se till båda dessa situationer.

Myndigheters arbete med it-avtal är starkt sammanlänkat med upphandlingsprocessen och i synnerhet beställarkompetensen. Det är i den inledande fasen av upphandlingsarbetet som myndigheten t.ex. kan formulera en kravspecifikation som minimerar risken för framtida inlåsningseffekter. Men för att fullt ut undvika inlåsningseffekter till följd av leverantörens immateriella rättigheter behöver myndigheten dessutom formulera ändamålsenliga avtalsvillkor.

Det kan te sig besvärligt, och kanske inte heller lämpligt, att frigöra avtalsprocessen från upphandlingsprocessen i stort. Vi menar också att det inte går att lappa och laga i slutet av inköpsprocessen (avtalet) om orsaken till icke ändamålsenliga avtalsvillkor skulle bero på otillräckligt arbete i början av processen (behovs- och marknadsanalys, riskanalys och juridisk analys). En generell höjning av kompetensen kring it-avtal bör emellertid kunna bygga på ökad kunskap utifrån goda exempel. Genom att arbeta strategiskt och praktiskt stödjande genom hela inköpsprocessen där såväl verksamhetens som leverantörens behov beaktas liksom marknadens utbud, det juridiska regelverket och affärsmässighet kan förutsättningar ges för en långsiktig höjning av kompetensen kring it-avtal i den offentliga förvaltningen.

Vi föreslår mot den bakgrunden att en myndighet ska få i uppdrag att främja den offentliga förvaltningens digitala investeringar genom att stödja myndigheters inköps- och avtalsprocesser och bidra till spridning av goda exempel. Uppdraget skulle också kunna innefatta att utifrån goda exempel ta fram förslag på standardformuleringar av vissa avtalsvillkor som kan vara särskilt komplicerade att utforma t.ex. när det gäller att motverka inlåsningseffekter, möjliggöra nödvändig insyn utan hinder av immaterialrätt, avveckling av samarbete etc. Det föreslagna uppdraget kan också innefatta att ta fram en form

av checklista över avtalsvillkor som myndigheter generellt bör uppmärksamma vid avtalsgranskning.

Vem bör få uppdraget?

Det finns flera aktörer som framstår som lämpliga för det ovan skisserade uppdraget. En grundläggande förutsättning är dock att den aktör som får uppdraget har möjlighet att tillhandahålla avtalsstöd till hela den offentliga förvaltningen. Med denna begränsning anser vi att det finns tre aktörer som skulle kunna tillhandahålla det avtalsstöd som föreslås, nämligen Upphandlingsmyndigheten, Kammarkollegiet och den nya Myndigheten för digital förvaltning som inrättas den 1 september 2018.[93]

Upphandlingsmyndigheten har det samlade ansvaret för att utveckla, förvalta och stödja upphandling. I detta ansvar ingår bl.a. avtalsförvaltning i mening att administrera avtal och göra uppföljningar. Upphandlingsmyndighetens uppdrag är emellertid inriktat på stöd i upphandlingsprocesser ur ett mer övergripande perspektiv och inte med avseende på de närmare avtalen och konkreta situationer. För det skisserade uppdraget ser vi att det behövs särskild kunskap om komplexa it-tjänster och det avtalsmässiga innehållet. Därtill är inte Upphandlingsmyndighetens uppdrag specifikt inriktat på inköp av it utan omfattar upphandling i mer generella termer. Mot denna bakgrund bedömer vi att Upphandlingsmyndigheten inte ligger närmast till hands för det skisserade uppdraget.

Kammarkollegiet ansvarar för att upphandla samordnade ramavtal för hela den offentliga förvaltningen inom it-området. Kammarkollegiet har en lång erfarenhet av att förhandla avtal med privata leverantörer och formulera affärsmässiga och juridiskt hållbara avtalsvillkor. Statens inköpscentral hos Kammarkollegiet tillhandahåller redan i dag visst stöd och vägledning till avropande myndigheter. Stödet riktar sig emellertid enbart till avropande myndigheter och inte till myndigheter som driver egna upphandlingsarbeten. Mot denna bakgrund framstår Kammarkollegiets generella uppdrag som väl snävt i förhållande till det skisserade uppdraget om avtalsstöd.

[93] *Inrättande av en myndighet för digitalisering av den offentliga sektorn*, (dir. 2017:117).

Den nya Myndigheten för digital förvaltning ska verka för en ökad digitalisering av den offentliga sektorn. I myndighetens uppdrag ska bl.a. ingå att ge stöd till myndigheters digitala investeringar. Inom ramen för denna uppgift kommer myndigheten att överta ansvaret för Expertgruppen för digitala investeringars uppdrag.[94] Expertgruppens uppdrag är bl.a. att stödja myndigheter som avser att göra större strategiska verksamhetsinvesteringar i immateriella anläggningstillgångar med väsentliga inslag av it-användning och digitalisering. Expertgruppen har etablerat samarbete med ett tjugotal statliga myndigheter och målet är bl.a. att utifrån de projekt eller andra utvecklingsarbeten som har valts ut på respektive myndighet, ge råd kring digitala investeringar och bidra till kunskapsspridning mellan myndigheterna.

Det uppdrag rörande digitala investeringar som från den 1 september 2018 övertas av Myndigheten för digital förvaltning innebär att den myndigheten har möjlighet att i nära samarbete följa utvalda myndigheters utvecklingsarbeten som leder till digitala investeringar, t.ex. köp av it. Enligt vår uppfattning kan det föreslagna uppdraget att ge myndigheter stöd i sitt arbete med it-avtal lämpligen inkluderas i den nya myndighetens uppdrag att ge stöd till myndigheters digitala investeringar. Vi föreslår därför att den myndighetens uppdrag att ge stöd till myndigheter vid digitala investeringar också ska omfatta myndigheters inköps- och avtalsprocesser och bidra till spridning av goda exempel. Det kan också vara lämpligt att myndigheten i relevanta delar inhämtar synpunkter från det privata näringslivet.

11.6.3 Utökat stöd för personuppgiftsbiträdesavtal

Utredningens bedömning: Stödet för myndigheter att, i personuppgiftsbiträdesavtal, formulera juridiskt hållbara och förutsebara avtalsvillkor som uppfyller dataskyddsförordningens krav på transparens, insyn och kontroll bör utvecklas.

Utredningens förslag: Datainspektionen, Myndigheten för digital förvaltning och Myndigheten för samhällsskydd och beredskap ska få i särskilt uppdrag att gemensamt och i samråd med

[94] *En expertgrupp för digitala investeringar,* (dir. 2017:62). Se även tilläggsdirektiv (dir. 2017:118).

Sveriges kommuner och landsting, utforma standardavtalsklausuler för personuppgiftsbiträdesavtal som tecknas mellan en myndighet som personuppgiftsansvarig och en privat leverantör som personuppgiftsbiträde inom ramen för myndighetens köp av it-drift eller andra it-baserade funktioner.

Skälen för utredningens bedömning och förslag

Stöd i myndigheters arbete med personuppgiftsbiträdesavtal

Som vi har redogjort för i kapitel 11.1.1 bedömer vi att det inte är lämpligt att föreslå författningsreglering av myndigheters avtalsarbete eftersom det riskerar att begränsa myndigheternas manöverutrymme. När det gäller personuppgiftsbiträdesavtal finns emellertid redan delvis reglerat i dataskyddsförordningens artikel 28 vad som särskilt ska föreskrivas i ett sådant avtal, dvs. en slags miniminivå av det avtalsmässiga innehållet.

Ett övergripande syfte med personuppgiftsbiträdesavtal är att säkerställa att nödvändig transparens råder i avtalsförhållandet mellan den personuppgiftsansvarige och personuppgiftsbiträdet och dennes eventuella underleverantörer.[95] God transparens säkerställer att den personuppgiftsansvariges behov av insyn i, och kontroll av, biträdets och dess underleverantörers behandling av personuppgifter kan tillgodoses.

I vårt kartläggningsarbete har det påtalats att såväl myndigheter i egenskap av personuppgiftsansvariga som vissa till myndigheterna knutna personuppgiftsbiträden, anser sig lägga ned oproportionerligt mycket tid och resurser på att formulera avtalsvillkor som uppfyller regleringens krav på transparens, insyn och kontroll. Trots att mycket tid och resurser läggs in i avtalsarbetet kan en rättslig osäkerhet ändå kvarstå i fråga om avtalet uppfyller gällande lagkrav. Datainspektionen tillhandahåller visst stöd på sin webbplats om vilka områden som rent innehållsmässigt ska regleras i personuppgiftsbiträdesavtal. För kommuner, landsting och regioner har SKL tagit fram en avtalsmall, och en checklista som kan användas som stöd vid tecknande av personuppgiftsbiträdesavtal. SKL:s stödmaterial har en bred ansats och tanken är att avtalsmallen, efter

[95] För vår definition av begreppet underleverantör se kapitel 11.1.3.

anpassning, ska kunna användas i en mängd olika sammanhang där en kommunal myndighet är personuppgiftsansvarig och en annan, offentlig eller privat aktör, är personuppgiftsbiträde.

Resultatet av vår kartläggning har visat att det inte i första hand är *vad* som ska regleras i personuppgiftsbiträdesavtal som skapar osäkerhet utan snarare *hur* det ska regleras. Det avtalsstöd som i dag finns tillgängligt för offentliga myndigheter när det gäller tecknande av personuppgiftsbiträdesavtal bedömer vi inte uppfyller hela den offentliga förvaltningens behov. SKL:s avtalsmall riktar sig främst till kommuner, landsting och regioner och de verksamheter som bedrivs inom dessa sektorer. Det stöd som tillhandahålls på Datainspektionens webbplats är alltför generellt hållet för att ge vägledning i specifika situationer.

Vår bedömning är därför att stödet för myndigheter att i personuppgiftsbiträdesavtal formulera juridiskt hållbara och förutsebara avtalsvillkor som uppfyller dataskyddsförordningens krav på transparens, insyn och kontroll bör utvecklas ytterligare.

Standardavtalsklausuler för personuppgiftsbiträdesavtal

Ett konkret och användbart stöd som har potential att effektivisera avtalsarbetet inom den offentliga förvaltningen är att, i enlighet med regleringen i dataskyddsförordningen, utforma standardavtalsklausuler för personuppgiftsbiträdesavtal. Med hjälp av standardiserade avtalsklausuler kan en personuppgiftsansvarig ges bättre stöd i fråga om hur transparens i avtalsförhållandet kan etableras och därigenom uppnå god insyn i, och kontroll av, personuppgiftsbiträdets och eventuella underleverantörers behandling av personuppgifter.

Vår uppfattning är att önskemålet om exempel på standardiserade avtalsklausuler främst gör sig gällande i samband med en myndighets köp av it som innefattar utlämnande av personuppgifter till ett eller flera personuppgiftsbiträden (dvs. det ursprungliga personuppgiftsbiträdet och dennes underleverantörer). Men vi ser också att standardavtalsklausuler har en rationaliseringspotential för personuppgiftsbiträdesavtal som tecknas i samband med anslutning till myndighetsgemensamma digitala tjänster där personuppgifter behandlas. Det kan röra sig om tjänster där en myndighet agerar i rollen som personuppgiftsbiträde åt andra myndigheter eller där en privat leverantör,

som personuppgiftsbiträde, tillhandahåller en standardiserad tjänst åt ett stort antal personuppgiftsansvariga myndigheter.

Standardavtalsklausuler kan i praktiken användas på två sätt. En personuppgiftsansvarig kan välja att tillämpa klausulerna så som de är utformade, vilket bör borga för efterlevnad av dataskyddsförordningen i de delar som regleras av klausulerna. Men standardavtalsklausuler kan därtill används som en god förlaga för personuppgiftsansvariga som har behov av att ytterligare specificera kraven på personuppgiftsbiträdet och den behandling av personuppgifter som denne får i uppdrag att utföra. Även om standardavtalsklausulerna inte är direkt anpassade för andra situationer än där en myndighet anlitar en privat leverantör som personuppgiftsbiträde, bör de också kunna användas som förebild vid utformning av avtalsvillkor för dataskydd i andra sammanhang. Exempelvis där en myndighet agerar personuppgiftsbiträde åt andra myndigheter.

Vi föreslår mot den beskrivna bakgrunden att en eller flera myndigheter ska få i uppdrag att ta fram standardavtalsklausuler för personuppgiftsbiträdesavtal som tecknas mellan en myndighet som personuppgiftsansvarig och en privat leverantör som personuppgiftsbiträde inom ramen för myndighetens köp av it-drift eller andra it-baserade funktioner. Vilka villkor som bör formuleras i standardavtalsklausuler bör lämpligen avgöras av den eller de aktörer som får i uppdrag att ta fram standardavtalsklausuler.

Vem bör får uppdraget?

Ett uppdrag att ta fram standardavtalsklausuler för personuppgiftsbiträdesavtal bör utgå från en bred ansats i syfte att uppnå balanserade avtalsvillkor som kan accepteras såväl av den offentliga som av den privata sektorn. Mot denna bakgrund bedömer vi att det är lämpligt att uppdraget bör utföras gemensamt av ett antal aktörer. Frågan blir då vilka aktörer som är bäst lämpade att utföra detta uppdrag?

Datainspektionen, som är tillsynsmyndighet enligt dataskyddsförordningen,[96] har expertkunskaper i det dataskyddsrättsliga regelverket. Därtill är Datainspektionen den myndighet som, i enlighet

[96] Förslag till 3 § förordning med kompletterande bestämmelser till EU:s dataskyddsförordning, (SOU 2017:39).

med dataskyddsförordningen, har befogenhet att anta standardavtalsklausuler.[97] Av denna anledning är det naturligt att Datainspektionen behöver vara en av aktörerna som får i uppdrag att medverka vid framtagande av standardavtalsklausuler.

Datainspektionens uppgifter framgår av regleringen i dataskyddsförordningen.[98] I dataskyddsförordningen stadgas också att myndigheten ska vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med förordningen.[99] Förordningens krav på oberoende har tolkats som att utrymmet för regeringen att styra Datainspektionen genom regleringar i myndighetsinstruktionen generellt är begränsat.[100] Enligt vår uppfattning torde detta ställningstagande dock inte påverka regeringens befogenhet att ge Datainspektionen ett särskilt regeringsuppdrag som är begränsat i tid, även om uppdraget innefattar genomförandet av en sådan uppgift som redan framgår av dataskyddsförordningens reglering att Datainspektionen har att utföra.

I kapitel 11.6.2 har vi föreslagit att den nya Myndigheten för digital förvaltning ska få i uppdrag att främja den offentliga förvaltningens digitala investeringar genom att stödja myndigheters inköps- och avtalsprocesser. Genom detta uppdrag, och myndighetens föreslagna verksamhet i övrigt med fokus på digitalisering, ser vi att den myndigheten bör kunna bidra med särskilda kunskaper såväl när det gäller myndigheters krav på avtalsvillkoren som privata leverantörers behov.

Eftersom dataskyddsförordningens bestämmelser om säkerhet för personuppgifter i stor utsträckning tangerar informationssäkerhetsfrågor bör även en aktör med särskilda kunskaper inom detta område medverka i uppdraget. Myndigheten för samhällsskydd och beredskap (MSB) förefaller vara bäst lämpad i denna del.

Vårt förslag är således att regeringen ska ge Datainspektionen, Myndigheten för digital förvaltning och MSB i särskilt uppdrag att ta fram standardavtalsklausuler för personuppgiftsbiträdesavtal. För att även kommunala myndigheters eventuellt specifika behov ska bli omhändertagna, bör det föreslagna uppdraget genomföras i samråd

[97] Artiklarna 28.8, 57.1 j, 58.3 g, 63 och 64.1 d dataskyddsförordningen.
[98] Artikel 57 dataskyddsförordningen.
[99] Artikel 52.1 dataskyddsförordningen.
[100] *Ett samlat ansvar för tillsyn över den personliga integriteten,* (SOU 2016:65), s. 160.

med SKL. I syfte att balansera avtalsvillkoren mot privata leverantörers behov bör det också vara lämpligt att i relevanta delar inhämta synpunkter från det privata näringslivet.

11.6.4 Konsekvenser av förslagen

I takt med den ökade digitaliseringen och utkontrakteringen i den offentliga förvaltningen har it-avtal och personuppgiftsbiträdesavtal kommit att bli allt mer centrala komponenter i myndigheternas verksamhet. Teknikutvecklingen har emellertid också bidragit till att it-avtal har blivit allt mer komplicerade och omfattande och i ett avtalsförhållande mellan en myndighet och en privat leverantör tenderar det att råda en viss obalans i styrkeförhållandet, till leverantörens fördel. Det har också visat sig att myndigheterna i den offentliga förvaltningen anser sig lägga ned oproportionerligt mycket tid och resurser på att teckna juridiskt hållbara personuppgiftsbiträdesavtal.

Förslagen om att utöka det förvaltningsgemensamma stödet för it-avtal och personuppgiftsbiträdesavtal har potential att bidra till en kunskapshöjning i den offentliga förvaltningen kring avtalens utformning och innehåll. Därtill kan rättssäkerheten förväntas öka eftersom ändamålsenligt utformade avtalsvillkor bl.a. kan säkerställa myndigheternas rätt till insyn och kontroll av leverantörens hantering av myndighetens information. Vidare kan en viss kostnadsbesparing och effektivitetshöjning förutses eftersom avtalsarbetet kan bedrivas med färre personella resurser.

Förslagen innebär att den nya Myndigheten för digital förvaltning får extra kostnader för de resurser som kommer att behövas för att utföra uppdragen i fråga. Myndigheten är för närvarande under bildande och arbete pågår med att tilldela myndigheten resurser. Mot denna bakgrund är det svårt att beräkna vilka ytterligare resurser som krävs med anledning av just dessa förslag i förhållande till myndighetens sammantagna uppdrag. Vi kan därför inte beräkna särskild resursåtgång för den myndigheten.

Datainspektionen kommer att behöva ha en nyckelroll i uppdraget att ta fram standardavtalsklausuler för personuppgiftsbiträdesavtal. Datainspektionen befinner sig för närvarande i ett

omfattande reformarbete bl.a. med anledning av dataskyddsförordningens ikraftträdande. Regeringen har tillfört Datainspektionen extra medel för att stärka arbetet med den personliga integriteten vilket bl.a. ska ske genom att inspektionens stödjande och rådgivande roll ska bli tydligare. Förslaget att ta fram standardavtalsklausuler menar vi kan innefattas i Datainspektionens stödjande och rådgivande roll och bör rymmas inom det finanseringstillskott som regeringen redan har aviserat.[101]

MSB kan förväntas behöva avsätta färre personella resurser än övriga deltagande myndigheter. Den myndighetens bidrag avser främst att säkerställa att informationssäkerhetsfrågorna omhändertas. Förväntad resursåtgång bör därför kunna rymmas inom det befintliga anslaget.

Förslagen om utökat stöd för it-avtal och personuppgiftsbiträdesavtal skulle kunna ge effekten att myndigheters köp av konsulthjälp för sådant avtalstecknande minskar. Med hänsyn tagen till den allt växande komplexiteten inom området och bl.a. dataskyddsförordningens ikraftträdande ser vi emellertid inte att förslagen kommer att leda till intäktsbortfall för den privata marknaden inom dessa områden. För generella konsekvenser av våra förslag hänvisas till kapitel 14.2.

[101] Se regeringens pressmeddelande *Datainspektionen blir Integritetsskyddsmyndigheten*, den 15 december 2017.

12 Rättsutveckling för den digitala förvaltningen

12.1 Hur ska det fortsatta arbetet bedrivas?

12.1.1 Juridik som stöd för förvaltningens digitalisering

I de föregående kapitel 7–11 har vi presenterat några prioriterade förslag till författningsändringar och andra åtgärder för bättre förutsättningar att hantera rättsliga utmaningar med anledning av förvaltningens fortsatta digitalisering.

Vi har bl.a. lämnat förslag till ändringar i 4 kap. offentlighets- och sekretesslagen (2009:400) som syftar till att förenkla för myndigheter att upprätthålla en god offentlighetsstruktur vid vissa automatiserade förfaranden, samtidigt som offentlighetsprincipen säkerställs och rättssäkerheten stärks. Det gäller för det första säkerställande av förmågan att kunna ge insyn i vissa automatiserade förfaranden när algoritmer eller datorprogram används i samband med urval eller beslutsfattande (se kapitel 7.7.2). För det andra lämnas förslag som främjar inhämtande av beslutsunderlag på annat sätt än direkt från enskilda samtidigt som förvaltningen säkerställer ordning och reda på beslutsunderlag (se kapitel 7.7.3). I kapitel 7 ges också förslag till fortsatt organiserat arbete för att säkerställa rättssäkra förfaranden när förvaltningen använder AI-system med maskininlärda algoritmer samtidigt som både innovation och samverkan främjas (se kapitel 7.8.2).

I kapitel 8 har vi föreslagit ny och anpassad reglering i förvaltningslagen (2017:900) om digital kommunikation. Syftet är att stärka kraven på att förvaltningen ska vara digitalt tillgänglig på det sätt som allmänheten förväntar sig, samtidigt som tilliten till digitala förfaranden stärks med klara regler om hur kommunikationen förväntas gå till. Förslagen innehåller en ny huvudregel om att myndigheter ska

vara skyldiga att tillhandahålla, och på lämpligt sätt anvisa, en eller flera digitala mottagningsfunktioner dit handlingar kan förmedlas. För att säkerställa en god balans mellan intressen av bl.a. effektivitet och säkerhet föreslås att huvudregeln inte tillämpas om det är olämpligt av säkerhetsskäl eller av andra skäl. Ytterligare anpassningar i fråga om förvaltningens kommunikation föreslås också för att skapa tillit till förvaltningens digitala förfaranden (se kapitel 8.3.4 vad gäller anpassning av reglering om ankomstdag för handlingar som sänds digitalt till förvaltningen och kapitel 8.3.5 om underrättelser). Vi har vidare föreslagit en ny huvudregel om att förvaltningens kommunikation till enskilda ska vara digital (se kapitel 8.3.6). För att stärka de rättsliga förutsättningarna för tillhandahållande av digitala tjänster där ärenden kan inledas har vi föreslagit att en myndighet bör ges i uppdrag att ta fram allmänna råd eller annat stödmaterial som avser utformningen av sådana tjänster (se kapitel 8.4.5).

En digital förvaltning ska vara en rättssäker och även i övrigt säker förvaltning. Utöver de ovan redovisade förslagen har vi därför lämnat några förslag som syftar till att skapa en stabil rättslig bas för fortsatt utveckling i en digital förvaltning som samverkar såväl internt som i förhållande till privata aktörer. Vi har föreslagit att regeringen fortsatt ska låta utreda behov av att komplettera regleringen om informationssäkerhet för hela den offentliga förvaltningen (se kapitel 9.7.2). Vi har också föreslagit bl.a. en ny lag om tystnadsplikt vid utkontraktering till privata leverantörer som behandlar myndigheters uppgifter för teknisk bearbetning eller lagring (se kapitel 10). Slutligen har vi föreslagit att förutsättningarna för hantering av rättsliga utmaningar med anledning av digitaliseringen ska stärkas genom att regeringen uppdrar åt vissa myndigheter att ge utökat stöd i myndigheters it-avtalsprocesser och vad gäller personuppgiftsbiträdesavtal (se kapitel 11.6.2 och 11.6.3).

Åtgärder och ställningstaganden från såväl riksdag som regering pekar mot att förvaltningens digitaliseringsarbete nu ska genomdrivas med ökat fokus. Vi är väl medvetna om att de förslag till författningsändringar och andra åtgärder som vi nu lämnat för att ge en stabil och förvaltningsgemensam bas där juridiken stödjer fortsatt digitalisering inte kommer att vara tillräckliga för att möta de kommande årens behov av förändringar i lagstiftningen. Såväl våra tidigare erfarenheter som vår kartläggning ger för handen att det finns ett väsentligt större förändringsbehov än det som vi inom

ramen för denna utredning har haft i uppdrag att ta omhand, inte minst eftersom våra direktiv bl.a. har varit att undvika förslag avseende lagstiftning som enbart påverkar enstaka verksamhetsområden inom den offentliga förvaltningen.

12.1.2 Behovet av rättsutveckling som stöd för en digital förvaltning

I kapitel 5 har vi presenterat en sammanfattning av vårt kartläggningsresultat. Där framgår att myndighetsrepresentanter och andra aktörer som vi träffat under utredningen har framfört behov av rättsutveckling på en rad områden för att stödja framväxten av den digitalt samverkande förvaltningen. Återkommande har också efterfrågats mer juridiskt stöd i centrala rättskällor (författning, förarbeten, praxis eller doktrin) för förvaltningens digitalisering.

Ett exempel på område där myndighetsrepresentanter fört fram behov av författningsändringar avser området för formkrav t.ex. på underskrifter och krav på viss form vid informationshantering i myndigheternas ärendeprocesser (se kapitel 5.3.4 och 5.6.1). Inom detta område ser även vi att det de närmaste åren, när satsningar på att digitalisera förvaltningen intensifieras, i ett lagstiftningsperspektiv kommer att behöva avsättas resurser för att genomföra anpassningar i gällande rätt i takt med önskemål om att förvaltningen digitaliserar t.ex. ansökningsförfaranden och hela eller delar av ärendeprocesserna. Det gäller även frågor som belysts i kapitel 5.5.7 om vilka slags uppgifter det egentligen är som kommer att vara av betydelse för mer effektiva och rättssäkra förfaranden i den digitala förvaltningen.

Ett annat område där det mot bakgrund av såväl kartläggningsresultatet som våra tidigare samlade erfarenheter finns behov av att anpassa gällande rätt rör informationsutbyten mellan myndigheter. Inom detta område har särskilt dataskyddsregleringen, men även sekretessregleringen, lyfts fram som onödigt hindrande eller hämmande i samband med digitaliseringsåtgärder. (Se kapitel 5.5. Se även kapitel 6.2 för en inledande analys.) Digitalisering av informationsutbyten mellan myndigheter är av påtaglig betydelse inte bara för de effektivitetsvinster som den digitala formen för sådana utbyten i sig för med sig, utan även för fortsatt automation av myndigheters

ärendeprocesser med de fördelar ur såväl rättssäkerhets- som effektivitetssynpunkt som sådan automation kan föra med sig (se kapitel 7). Att förbättra de rättsliga förutsättningarna för just digitala informationsutbyten ser vi, i linje med vad som också framgår av våra direktiv, som fortsatt angeläget. Även digital kommunikation med enskilda kan hindras eller hämmas av denna typ av reglering, dvs. registerförfattningar och sekretessreglering, (se kapitel 5.2).

Digitala informationsutbyten mellan myndigheter kan beskrivas vara en särskild form för informationsförsörjning inom förvaltningen, när utbytena t.ex. följer av en viss ärendeprocess eller av uppgiftsskyldigheter. Det finns emellertid också myndigheter som har ett särskilt utpekat registeransvar eller som har i uppdrag att försörja inte bara förvaltningen utan samhället i stort med viss information, i form av grunddata. Även inom detta, tredje, område har vi under kartläggningen fångat behov av författningsändringar (se kapitel 5.4).

Ett fjärde område för överväganden om rättsutveckling gäller öppenhet i den digitala förvaltningen genom tillhandahållande av öppna data eller elektroniskt utlämnande av allmänna handlingar (se kapitel 5.8). Övergången till en allt mer datadriven förvaltning där underlag för ärendehantering i högre utsträckning hämtas från databaser eller andra digitala källor, i stället för genom blanketter etc. som fylls i av enskilda, medför att handlingar som hanteras i förvaltningen i lägre utsträckning kommer att vara s.k. färdiga elektroniska handlingar. Vi ser bl.a. därför, utöver de förslag som lämnats i kapitel 7, behov av att fortsatt belysa hur rättsutvecklingen kan möta teknikutvecklingen för att säkerställa insynen i den digitala förvaltningen.

Alla de hittills beskrivna områdena kan också sägas ha bäring på de tankar som presenterats i kapitel 5.9 om att framgent överväga reglering i en sammanhållen författning av karaktären att styra just informationshanteringen i den digitala förvaltningen, snarare än lagstiftning om arkivering av informationen.

Ett ytterligare, femte, område för behov av rättsutveckling, är nära sammanlänkat med de behov av närmast infrastrukturliknande karaktär som också har lyfts fram. Det gäller identiteter och annan koppling till fysisk eller juridisk person (behöriga företrädare, fullmakter och frågor som rör delgivning, se kapitel 5.3). Vi ser också att det de närmaste åren kommer att finnas behov av resurser för att, parallellt med att nya tekniska lösningar tas fram, också

bedriva lagstiftningsarbete inom detta område med syfte att anpassa gällande rätt eller ta fram författningar till stöd för nya lösningar. Det kan t.ex. gälla att ta till vara på digitaliseringens möjligheter till effektiva och rättssäkra delgivningsförfaranden. Vi har inom ramen för denna utredning dock inte gått närmare in på dessa frågor, särskilt med beaktande av att andra utredningar har eller nyligen har haft i uppdrag att utreda den typen av frågeställningar.[1]

Ett antal ytterligare frågor har som framgått också lyfts fram i kapitel 5, bl.a. när det gäller tryckfrihetsförordningen och samverkan mellan myndigheter respektive språklagstiftningen.

Vi har i kapitel 7 även uppmärksammat vissa andra behov av att vara vaksam på för framtida lagstiftningsarbete vad gäller bl.a. digitalisering och automation på områden för faktiskt handlande inom förvaltningen. I kapitel 7 ges också förslag på ett uppdrag för samverkan kring rättssäkra AI-förfaranden som kan föranleda att behov av anpassning eller komplettering av gällande rätt lyfts fram.

Om politiska ställningstaganden görs att det t.ex. ska skapas en gemensam plattform för att på en plats tillhandahålla förvaltningens digitala tjänster för enskilda kan, utöver de förslag som lämnats i kapitel 8, ytterligare författningsåtgärder behövas.

Här finns också anledning att påminna om vårt förslag i kapitel 9 om att utreda frågan om en mer generell informationssäkerhetslagstiftning.

I det följande (se kapitel 12.2.1) belyses också att t.ex. blockkedjetekniken kan få inverkan på bl.a. rättsområden som panträtten, utsökningsrätten, fastighetsrätten och bokföringsrätten.

Samtidigt som det ovan beskrivna behovet av att lägga resurser på att överväga eller genomföra författningsändringar för att möjliggöra eller stödja digitaliseringen av förvaltningen, såväl som samhället i stort, förefaller vara omfattande kommer juristresurserna för att bedriva sådant arbete att vara begränsade. Prioriteringar och avvägningar hur de resurserna används på bästa sätt kommer att behöva göras för att så resurseffektivt som möjligt åstadkomma den rättsutveckling som önskas.

[1] Se bl.a. *reboot – omstart för den digitala förvaltningen* (SOU 2017:114) och Åtgärder för att minska bedrägeribrottsligheten – skärpta krav och rutiner för svenska identitetshandlingar (dir. 2017:90).

12.1.3 Organisation för beredning av författningsförslag

Utredningens bedömning: Formerna för samordning av arbetet med författningsändringar kan förbättras så att sådana ändringar kan åstadkommas i rätt tid och i lämplig omfattning för att inte hindra eller hämma önskad digital utveckling i förvaltningen.

Utredningens förslag: Regeringen ska tillsätta ett rättsligt beredningsorgan i form av en kommitté eller särskild utredare som under de närmast kommande åren får i uppdrag att löpande ta fram beredningsunderlag för anpassning av gällande rätt vid digitalisering av ärendehandläggning i förvaltningen, som stöds av digital informationsförsörjning.

Skälen för utredningens bedömning och förslag

Vårt uppdrag

Det ingår i vårt uppdrag att analysera och lämna förslag till hur den offentliga förvaltningen som helhet kan samverka kring behovet av ny eller ändrad lagstiftning för att främja digitaliseringen av förvaltningen. I våra direktiv beskrivs också att samverkan redan i dag sker inom den offentliga förvaltningen för att identifiera behov av ny eller ändrad lagstiftning på området för digitalisering av den offentliga förvaltningen. Förutsättningarna beskrivs dock kunna utvecklas, bl.a. för att säkerställa att mer fullständiga underlag tas fram som väger in samtliga relevanta intressen och för att involvera fler delar av förvaltningen i arbetet.

Kartläggningsresultatet

Under vår kartläggning har vi fått bilden av att myndigheter i allt högre grad samverkar med varandra och t.ex. gemensamt hemställer om de författningsändringar som behövs för ett digitalt utvecklingsarbete som exempelvis involverar informationsutbyte mellan flera myndigheter. Från myndighetshåll efterfrågas emellertid effektivare och smidigare processer för att kunna föra fram behov av ny eller förändrad reglering till lagstiftaren, där t.ex. återkoppling ges om det

behövs förtydliganden eller tillägg i de analyser som gjorts inför hemställan om författningsändringar. Det har också beskrivits vara viktigt att lagstiftningsprocessen till stöd för digitaliseringen av förvaltningen hålls igång löpande. Myndigheter efterfrågar dessutom en samordning eller gemensam kontaktpunkt för frågor som rör författningsändringar, för att möjliggöra sådana ändringar i den tid och omfattning som behövs för pågående eller planerade utvecklingsarbeten. I önskemålen om samordning ligger även frågan om gemensamma prioriteringar mellan departement när myndigheter under olika departement samverkar i dessa utvecklingsarbeten.

Våra överväganden

Inriktningen i vårt uppdrag sammanfaller enligt vår bedömning väl med de önskemål som även från myndighetsrepresentanter förts fram under vår kartläggning. Därtill kommer att det nu sker en fokusering på att förvaltningen de närmaste åren ska ta ytterligare kliv framåt mot att bli än mer digital.[2] För att detta ska vara möjligt krävs förutsättningar för att i tid åstadkomma beredningsunderlag så att behov av författningsändringar kan omhändertas i den tid och i den omfattning som är lämpligt för att stödja och främja den önskade digitaliseringen.

Frågan är emellertid på vilket sätt det kan vara möjligt att åstadkomma goda förutsättningar för att kunna bedriva rättsutveckling i takt med den digitala utvecklingen.

Flera av dem vi talat med under kartläggningen har, som framgått ovan, beskrivit för oss att en förändring under senare tid ägt rum såtillvida att myndigheter i ökad grad samverkar med varandra för att ta fram gemensamma hemställningar om författningsändringar som behövs för myndighetsgemensamma utvecklingsarbeten. Ett alternativ vi har övervägt är därför att stanna vid att bejaka den utvecklingen, som vi ser som positiv. Det har emellertid också framkommit att det ändå kan vara svårt att få dessa hemställningar om författningsändringar prioriterade bland annat behov av lagstiftningsarbete och att det tar lång tid att åstadkomma förändringar. Vi bedömer därför att formerna för samordning fortfarande kan förbättras i riktning

[2] Se även SOU 2017:114 och vad som där beskrivs vara en omstart för den digitala förvaltningen.

mot att författningsändringar kan åstadkommas i lämplig tid och omfattning för att inte hindra eller hämma önskad digital utveckling i förvaltningen.

Det som i dagsläget synes saknas är enligt vår bedömning en förvaltningsgemensam länk mellan å ena sidan myndigheter, där bl.a. tillämpande jurister gör rättsliga bedömningar om behov av författningsändringar när digitala utvecklingsarbeten planeras, och å andra sidan Regeringskansliet och departementen där jurister som arbetar med lagstiftning tar vid efter de prioriteringar som den politiska ledningen gör.

Ett alternativ som vi har övervägt, för att skapa denna länk, är om den nya Myndigheten för digital förvaltning får eller borde få en särskild roll i att t.ex. samla myndigheternas behov av författningsändringar på digitaliseringsområdet och bistå regeringen med prioriteringar i fråga om vilket lagstiftningsarbete som ska bedrivas. I de skrivningar som framgått i direktiven för organisationskommittén har myndigheten emellertid inte givits någon sådan framträdande rättslig roll.[3] Med beaktande av att varje förvaltningsmyndighet är fristående är det också svårt att se att en viss förvaltningsmyndighet ska ha i uppdrag att för andra myndigheter, även kommunala och landstingskommunala, samordna och prioritera bland behov av författningsändringar. Frågan är dessutom om ett sådant förfarande i någon större utsträckning skulle snabba på processerna med att t.ex. ta fram mer fullständiga beredningsunderlag än dem varje myndighet själv kan utforma.

Det finns enligt oss anledning att lägga särskild vikt vid behovet att just de närmaste åren genomföra de författningsändringar som kommer att behövas när en ökad fokusering på den digitala förvaltningen görs. Ett särskilt beredningsorgan med uppdrag att den närmaste tiden löpande ta fram beredningsunderlag i form av förslag på författningsändringar för förvaltningens digitalisering skulle kunna fungera som en sådan länk som efterfrågas.

En väl beprövad form för att ta fram beredningsunderlag där samtliga relevanta intressen vägs in är kommittéformen (inklusive formen särskild utredare). En kommitté eller särskild utredare skulle under några års tid kunna ges i uppdrag att, t.ex. i delbetänkanden, löpande ta fram beredningsunderlag för författningsändringar som

[3] *Inrättande av en myndighet för digitalisering av den offentliga sektorn* (dir. 2017:117).

bedöms nödvändiga för förvaltningens, under samma period, planerade digitaliseringsåtgärder. Vi förutsätter också att resultatet från ett sådant beredningsorgans arbete kan tas omhand på ett samordnat sätt i Regeringskansliet mellan departementen.

För att nå framgång med att ta fram fullständiga beredningsunderlag behövs enligt oss såväl kunskap om lagstiftningsarbete som kunskap om de faktiska och praktiska förutsättningarna för de digitaliseringsåtgärder som övervägs. En rättslig beredning i kommittéform ger möjlighet att samla experter med olika slags kompetens från myndigheter och kompetens från bl.a. departementen kring lagstiftningsteknik. Att samordna teoretisk och praktisk kunskap kommer, såvitt vi kan se, vara nödvändigt för att nå hela vägen fram till genomförande av författningsändringar. Prioriteringar avseende vilka författningsförslag som ska lämnas och när behöver också göras i samråd med de aktörer som tar ställning till vilket utvecklingsarbete som ska bedrivas under kommande år.

De områden som enligt vår uppfattning borde prioriteras inom ramen för en sådan rättslig beredning som här skisseras är området för formkrav t.ex. på underskrifter och krav på viss form vid informationshantering i myndigheternas ärendeprocesser.[4] För att åstadkomma digitalisering av ärendeprocesser krävs också ändringar på området för informationsutbyten mellan myndigheter, särskilt vad avser reglering i registerförfattningar och sekretessreglering, och sannolikt också inom området för reglering med utpekande av särskilt ansvar för informationsförsörjning genom vissa register.

Det bör nämnas att vi har övervägt att nu föreslå större grepp i fråga om vilka ändringsbehov som finns i gällande rätt för att stödja och främja en digital förvaltning. Erfarenhetsmässigt har dock försök till större reformer på de aktuella rättsområdena varit svåra att genomföra på kort tid. Med tanke på behovet av att i närtid bl.a. undanröja rättsliga hinder mot digitala informationsutbyten ser vi i den närmaste framtiden i stället framför oss ett metodiskt och förvaltningsgemensamt arbete med anpassningar av gällande rätt. Ett sådant anpassningsarbete bör kunna sträva mot att på sikt och sammantaget kunna leda till större förändringar. Inledningsvis kan dock stegvisa författningsändringar genomföras på kortare tid.

[4] Se vidare kapitel 12.2.1 om att här avses just formkrav i gällande rätt och inte e-legitimation eller e-underskrift i mer tekniskt hänseende.

Det finns anledning att också framhålla att ett sådant beredningsorgan som här skisseras inte alls utesluter att initiativ till författningsändringar också tas på andra sätt, genom sedvanliga hemställningar från myndigheter till ansvarigt departement eller andra politiska initiativ inom det breda området för förvaltningens digitalisering.

För det fortsatta arbetet med rättsutveckling för en digital förvaltning finns redan en hel del underlag, bl.a. i form av E-delegationens tidigare betänkanden och det material som myndigheter delat med sig av till oss under kartläggningen. Vi har också i flera avseenden genomfört analyser av kartläggningsresultatet som kan vara till nytta i det fortsatta arbetet. De analyserna och våra bedömningar redovisas därför i det följande.

Här följer också vissa analyser på områden som kanske inte närmast hör hemma i den typ av rättslig beredning som ovan skisserats utan kan förtjäna att övervägas i särskild ordning, däribland frågor om öppenhet i den digitala förvaltningen som kan tangera överväganden om behov av grundlagsändringar.

Sammanfattningsvis föreslår vi att regeringen tillsätter ett beredningsorgan som under de kommande åren får i uppdrag att utgöra en rättslig beredning för löpande anpassning av gällande rätt vid digitalisering av ärendehandläggning i förvaltningen, som stöds av digitalt informationsutbyte och andra former för digital informationsförsörjning. För det skisserade beredningsorganet kan inte gälla de begränsningar som vi haft i förevarande utredning i fråga om att sektorsspecifik lagstiftning inte ska prioriteras, eller att förslag på författningsändringar inte får lämnas på t.ex. personuppgiftsområdet.

Konsekvenser av förslaget

Syftet med förslaget är att så resurseffektivt som möjligt åstadkomma den rättsutveckling som önskas. Genom förslaget förutses bättre förutsättningar för att åstadkomma författningsändringar i rätt tid och i lämplig omfattning för att inte hindra eller hämma önskad digital utveckling i förvaltningen. Förslaget innebär att beredningsorganisationen ges formen av en kommitté eller särskild utredare. Den formen är väl känd och det förutses därför inte följa

några särskilda konsekvenser av förslaget. Se även kapitel 14.2 vad gäller generella konsekvenser av våra förslag.

12.1.4 Ytterligare insatser för att möta behov av rättsutveckling

Utredningens bedömning: För att rättsutvecklingen ska kunna möta teknik- och samhällsutvecklingen ser vi behov av ett kompetenscenter för juridiska frågor inom digitaliseringsområdet. Regeringen bör överväga att inrätta en funktion med juridisk expertis i den nya Myndigheten för digital förvaltning.

Skälen för utredningens bedömning: Som angetts i kapitel 12.1.2 finns ett flertal områden där olika former av rättsliga överväganden och ställningstaganden kommer att behöva göras för att möjliggöra eller stödja digitaliseringen av förvaltningen, samtidigt som teknikutvecklingen går fort framåt. Prioriteringar och avvägningar av hur de rättsliga resurserna används på bästa sätt kommer att behöva göras för att så resurseffektivt som möjligt åstadkomma den rättsutveckling som önskas. Vi har också i det föregående belyst vissa områden där vi lämnar förslag till åtgärder för ökat stöd i rättstillämpningen (se kapitel 8.4 om digitala tjänster med eget utrymme och kapitel 11.6 om it-avtal). Vid sidan av det beredningsorgan som här ovan har skisserats har vi också i kapitel 7.8.2 föreslagit ett särskilt uppdrag med sikte på rättssäkra förfaranden när förvaltningen använder AI-system med maskininlärda algoritmer.

Det av oss föreslagna särskilda uppdraget som avser rättssäkra förfaranden vid användning av AI-system med maskininlärda algoritmer kan emellertid inte bli annat än tidsbegränsat. Det beredningsorgan som ovan skisserats ser vi också framför oss ska vara operativt under de närmaste åren, och inte en permanent organisation. I förlängningen ser vi därför behov av ytterligare insatser för att säkerställa att Sverige kan ligga i framkant vad gäller rättsliga förutsättningar för digitalisering. Det gäller både i fråga om att proaktivt uppmärksamma regeringen på behov av anpassning av lagstiftningen för att kunna stödja utvecklingen när den äger rum, och i fråga om att uppmärksamma behov av ökat stöd i rättstillämpningen.

För att möta teknik- och samhällsutvecklingen med analyser avseende behov av rättsutveckling ser vi mot den bakgrunden att det även framgent kommer att behövas någon form av kompetenscenter för juridiska frågor inom digitaliseringsområdet. Det är tveksamt, och i alla fall på längre sikt inte sannolikt, att det av oss föreslagna beredningsorganet ensamt kan ta hand om detta behov. Snarare ser vi framför oss att kompetens, bl.a. i det skisserade beredningsorganet men även på andra håll i förvaltningen, nu upparbetas. Den typen av spjutspetskompetens inom digitaliseringsområdet bör även på längre sikt komma till nytta för en större del av förvaltningen. Här kan den nya Myndigheten för digital förvaltning få en roll att spela. Där inrättas nu en funktion med expertis på området för digitala investeringar. Någon motsvarande funktion med expertis på det rättsliga området har dock hittills inte föreslagits. Vi lämnar i denna del inte något särskilt förslag, med anledning av att myndigheten är under bildande i denna stund, men bedömer att regeringen i linje med det sagda fortsatt bör överväga att i den nya myndigheten också inrätta en funktion med juridisk expertis.

12.2 Analys av vissa frågor från kartläggningen

12.2.1 Underskrifter och ärendeprocesser

Utredningens bedömning: I det fortsatta arbetet är det angeläget att vidta åtgärder för att anpassa gällande rätt med krav på underskrift, undertecknande eller namnteckning till digitala förfaranden.

Det bör också prioriteras att, i takt med att det bedöms nödvändigt när digitala ärendeprocesser införs i förvaltningen, anpassa andra typer av regler i gällande rätt där pappersform för informationshantering antingen krävs eller förutsätts.

Skälen för utredningens bedömning

Kartläggningsresultatet

Som framgått i kapitel 6.8 har regeringen högt ställda mål för digitaliseringen av offentlig förvaltning. I kapitel 8 har även strävan mot en papperslös offentlig förvaltning beskrivits. Den politiska

viljan att undanröja rättsliga hinder mot digital kommunikation eller digital ärendehandläggning har också manifesterats på olika sätt under relativt lång tid. Redan år 2002 och 2003 utförde Regeringskansliet på regeringens uppdrag en departementsvis översyn av gällande formkrav i lagar och förordningar och övervägde behoven av förändringar i syfte att undanröja onödiga hinder för elektronisk[5] kommunikation och elektronisk dokument- och ärendehantering. För att samordna arbetet inrättades inom Regeringskansliet en arbetsgrupp, den s.k. Formel-gruppen.[6]

Med formkrav avses krav på att ett dokument eller meddelande ska ha viss form eller tillkomma på visst sätt för att ha en viss rättsverkan. Formel-gruppens genomgång av gällande rätt med formkrav omfattade sammantaget omkring 2 000 författningsställen. Genomgången visade att formkrav kunde betecknas på många olika sätt. Formel-gruppen framhöll att sådana krav kan hindra digital kommunikation eller dokumentation genom att uttryckligen utesluta digitala rutiner eller genom att det råder osäkerhet om hur kraven ska tillämpas på digitala rutiner. Det framkom också att formkravens innebörd inte sällan var oklar och att även likalydande formkrav kunde ha olika innebörd. Det visade sig även att formkraven kunde ha olika syften och bevekelsegrunder. Ofta var det dessutom svårt att reda ut vilket syfte som låg bakom enskilda formkrav. Bland de formkrav som enligt Formel-gruppens analys och bedömningar hindrade elektroniska rutiner återfanns bl.a. krav på underskrift, namnteckning och undertecknande. Det fanns andra typer av termer som inte alls borde uppfattas som formkrav, t.ex. anmälan, ansökan, underrättelse. Det fanns också exempel på termer eller krav som normalt inte borde hindra elektroniska rutiner, t.ex. handling respektive beslut, eller krav på skriftlighet eller att uppgifter ska lämnas enligt ett visst formulär.[7]

Med den tid och de resurser som står till vår utrednings förfogande har det inte funnits möjlighet att på nytt göra en genomgång av förekomsten av formkrav som hindrar digitala rutiner i alla gällande författningar. Mot bakgrund av den genomlysning som

[5] Tidigare användes genomgående begreppet ”elektronisk” förvaltning. Utvecklingen har gått mot att nu allt mer tala om en ”digital” förvaltning och digitala rutiner etc.
[6] *Formel Formkrav och elektronisk kommunikation* (Ds 2003:29).
[7] Se sammanfattningen i Ds 2003:29 s. 12 f.

Formel-gruppens arbete innebar, och det resultat som dokumenterades, kan det också ifrågasättas om det finns någon anledning att göra om den genomgången igen.

Vår kartläggning har dock visat att det, i linje med vad Formelgruppen tidigare fann, på flera rättsområden fortfarande finns behov av att ändra författningar som innehåller formkrav för att förvaltningen helt ska kunna ersätta pappersförfaranden med digitala förfaranden (se kapitel 5.3.4). Begrepp i lagstiftningen som underskrift, undertecknande och namnteckning kommer alltjämt i ljuset när myndigheter nu undersöker möjligheter att t.ex. anordna digitala tjänster för att inleda ärenden. Frågor om rättsliga krav på formerna för att verifiera en utställare bakom en handling är alltså fortfarande högst aktuella. I anslutning till frågor om formkrav för utställarverifiering har under kartläggningen också vissa frågor om digitala originalhandlingar aktualiserats, inte minst med beaktande av den tekniska utveckling som nu äger rum. Bland annat undersöker någon myndighet möjligheterna att säkerställa dokuments originalinnehåll med hjälp av blockkedjeteknik. Även privata aktörer har för utredningen framhållit vikten av att den offentliga förvaltningen deltar i arbetet med att möjliggöra sådan ny och innovativ teknik.

Kartläggningsresultatet visar emellertid också på ett bredare behov av att anpassa rättsregler som styr formerna för informationshantering under ärendeprocesser (se kapitel 5.6.1). Med andra ord är det inte enbart formkrav av innebörden krav på att ett dokument eller meddelande ska ha viss form eller tillkomma på visst sätt för att ha en viss rättsverkan som kan utgöra hinder i digitaliseringsarbeten. Det kan i stället röra sig om att regleringen av processen för hur information ska hanteras hindrar fullt tillvaratagande av digitaliseringens möjligheter. Som exempel kan nämnas regler om att en viss handling ska översändas till en viss mottagare, eller att en anmälan ska föregå en viss ansökan. Sådana regler behöver i och för sig inte alltid utesluta digital form för överföring av informationen. Däremot kan det finnas lämpligare sätt att anordna informationshanteringen. Informationen kanske inte alls behöver eller bör översändas eller hanteras i två steg genom både anmälan och ansökan.

Att det i vissa fall snarare är regleringen av en process för informationshantering än ett formkrav på t.ex. underskrift som kan utgöra rättsligt hinder mot att effektivt utnyttja digitaliseringens

möjligheter att förbättra informationshanteringen i förvaltningen omnämndes också av den tidigare Formel-gruppen.[8] Den typen av hinder kan, såvitt vi kan se, ha ökat i betydelse. I flera fall synes pågående eller önskat utvecklingsarbete, som företrädare för myndigheter nu börjar undersöka, innefatta helt andra processer för informationshantering än en digital motsvarighet till pappershantering. Digitalisering av ärendeprocesser handlar med andra ord inte om att förmedla färdiga pdf-dokument eller andra färdiga elektroniska handlingar på ett sätt som motsvarar tidigare pappershantering. Också detta kan medföra behov av ändringar i författningar som reglerar ärendeprocesser i förvaltningen.

I detta kapitel belyser vi närmare de analyser vi gjort inom det ovan presenterade området, särskilt vad gäller behov av anpassning av gällande rätt i fråga om formkrav på underskrifter etc. Vi går däremot inte närmare in på frågor av infrastrukturkaraktär avseende e-legitimering eller e-underskrifter.[9]

Formel-utredningen om digitala underskrifter

Krav i lagstiftningen på underskrift, namnteckning eller undertecknande kunde enligt Formel-gruppens mening inte uppfyllas med elektroniska rutiner. I de fall där sådana formkrav skulle anpassas för elektroniska rutiner borde de i stället ersättas med andra krav på utställarverifiering.[10] Formel-gruppen undersökte frågan om hur generell man borde göra en reglering som tillåter elektroniska rutiner på områden som omfattas av formkrav. Gruppen fann att den ena extrempunkten utgjordes av att ändra varje bestämmelse som innehåller formkrav för att det tydliggöra att elektroniska rutiner kan användas och vilka krav dessa måste uppfylla. Det motsatta angreppssättet skulle enligt Formel-gruppen innebära att man införde en generell bestämmelse som skulle föreskriva att samtliga formkrav av en viss typ, t.ex. namnunderskrift, skulle anses uppfyllda med vissa elektroniska rutiner, t.ex. elektronisk signatur. Exempel på det sistnämnda angreppssättet finns i den finska lagen (13/2003) om elektronisk kommunikation i myndigheternas verksamhet, i vars 9 § sägs:

[8] A.a. s. 44.
[9] Se i stället bl.a. SOU 2017:114.
[10] Ds 2003:29 s. 87 f.

> Vid anhängiggörande och behandling av ärenden uppfyller också elektroniska dokument som sänts till en myndighet kravet på skriftlig form. Om det vid anhängiggörande eller behandling av ett ärende krävs en undertecknad handling, uppfylls kravet på underskrift också genom en sådan elektronisk signatur som avses i 18 § lagen om elektroniska signaturer.

Den finska lagstiftningen utgör ett exempel på föreskrift om att alla formkrav av en viss typ får fullgöras med en viss typ av elektroniska rutiner vid all kommunikation med förvaltningen. Man kunde enligt Formel-gruppen också tänka sig en regel som vore än mer vidsyftande än den finska, nämligen en som inte är begränsad till förvaltningen utan omfattar all kommunikation och dokumentation i samhället. Mellan de båda extrempunkterna fann gruppen olika möjliga varianter. Man kunde exempelvis tänka sig regler med generell verkan inom ett begränsat område, t.ex. en viss myndighet eller en viss typ av ärenden.

En generell regel som jämställer elektroniska signaturer med vissa traditionella formkrav hade dock avvisats redan innan gruppen inledde sitt arbete.[11] Eftersom detta ställningstagande inte hade föregåtts av någon generell översyn av formkrav fann gruppen emellertid sig föranledd att än en gång ta ställning till denna fråga.

Sammantaget var det enligt Formel-gruppen dock inte lämpligt att införa en regel som generellt föreskriver att exempelvis krav på underskrift får fullgöras på visst sätt med elektroniska rutiner. Gruppen ansåg inte heller att det var lämpligt att införa en regel som föreskrev detta för förvaltningen. Däremot uteslöt de inte att det kunde finnas skäl att på vissa områden införa regler som föreskrev att formkrav kunde fullgöras på visst sätt eller att samtliga kommunikationer skulle ha viss form. Avslutningsvis påpekade gruppen att valet av regleringstekniskt angreppssätt också hängde samman med vilken ansats som valdes i processuellt hänseende.

Nya formkrav, som skulle tillåta elektroniska rutiner, måste därmed enligt gruppen utformas utifrån förutsättningarna på varje enskilt område. Gruppen föreslog alltså inga generella standardlösningar för hur formkrav borde anpassas.

Formel-gruppen noterade också två tänkbara lösningar när det gäller förhållandet mellan traditionella formkrav och elektronisk kommunikation eller dokumentation. Det finska exemplet ovan

[11] *Digitala signaturer – en teknisk och juridisk översikt* (Ds 1998:14), s. 183 f.

bygger på att de traditionella formkraven i annan lagstiftning finns kvar, men anses uppfyllda på ett visst nytt sätt. Det andra alternativet angavs vara att föreskriva nya formkrav som hänför sig enbart till den elektroniska miljön och föreskriva särskilda elektroniska formkrav. Då är det alltså inte fråga om att fullgöra traditionella formkrav med nya medel, utan ett krav på t.ex. elektronisk signatur är ett alternativt formkrav. Båda förhållningssätten ansågs förenliga med strävan efter teknikneutralitet.[12]

eIDAS-förordningen

Europaparlamentet och rådet har antagit den s.k. eIDAS-förordningen.[13] Förordningen syftar till att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att skapa en gemensam grund för ett säkert elektroniskt samspel mellan företag, medborgare och offentliga myndigheter inom unionen. Förordningen innehåller bestämmelser om (1) krav på ömsesidigt erkännande av anmälda e-legitimationer och (2) krav på tillhandahållande av betrodda tjänster och en rättslig ram för sådana tjänster. Här är främst den andra delen av intresse. Som betrodd tjänst definieras bl.a. skapande, kontroll och validering av elektroniska underskrifter.[14] Förordningens materiella delar började tillämpas den 1 juli 2016. Från och med den 29 september 2018 krävs också att svenska myndigheter erkänner utländska e-legitimationer i svenska tjänster.

Regleringen av elektroniska underskrifter i förordningen skiljer sig inte i någon större utsträckning från den tidigare regleringen i det upphävda signaturdirektivet.[15] Förordningen behåller uppdelningen i avancerade och kvalificerade elektroniska underskrifter, och kraven för respektive nivå är snarlik den som gällt enligt äldre regler. Den

[12] A.a. s. 50 f.

[13] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

[14] Artikel 3 eIDAS-förordningen. För det som numera benämns elektronisk underskrift användes tidigare termen elektronisk signatur. I det allmänna språkbruket har den termen med tiden kommit att ersättas med termen elektronisk underskrift, men termerna har samma innebörd.

[15] Förordningen upphäver det tidigare signaturdirektivet (1993/93/EG) som implementerats i Sverige genom lagen (2000:832) om kvalificerade elektroniska signaturer (signaturlagen). Genom lagen (2016:561) om kompletterande bestämmelser till EU:s förordning om elektronisk identifiering upphävs den svenska signaturlagen.

nya regleringen i förordningen gäller emellertid direkt utan implementering. Dessutom omfattar eIDAS-förordningen en bredare kategori av s.k. betrodda tjänster än signaturdirektivet.

Det finns inga krav på medlemsstaterna att använda sig av kvalificerade elektroniska underskrifter. Sådana krav kan dock i högre grad komma att ställas genom olika former av gränsöverskridande tjänster eller samarbeten. De svenska elektroniska underskrifter som används i dag anses generellt sett uppfylla kraven för avancerade elektroniska underskrifter.[16]

Kvalificerade elektroniska underskrifter ska enligt eIDAS-förordningen ha samma rättsliga verkan som en handskriven underskrift.[17] Detta hindrar inte att en nationell rättsordning kan ge även andra former av elektroniska underskrifter, t.ex. avancerade elektroniska underskrifter, samma rättsliga verkan som en handskriven underskrift.

Det finns också ett undantag i eIDAS-förordningen, som anger att förordningen inte påverkar regler i nationell rätt som avser rättsliga eller förfarandemässiga skyldigheter avseende formkrav.[18] I de fall ett nationellt formkrav anses innebära ett krav på fysiskt undertecknande har ett sådant alltså företräde framför eIDAS-förordningens reglering av rättslig verkan för elektroniska underskrifter. Tillämpningsområdet för detta undantag är emellertid inte helt tydligt och praxis saknas ännu.

Det finns även ett generellt undantag för betrodda tjänster som till följd av nationell rätt eller avtal mellan en avgränsad uppsättning deltagare endast används inom slutna system.[19] Detta innebär exempelvis att ett helt myndighetsinternt system för elektroniska underskrifter av medarbetare sannolikt faller utanför förordningens krav på betrodda tjänster.

Att eIDAS-förordningen innebär, delvis utmanande, krav på myndigheter att bl.a. acceptera och hantera utländska elektroniska identitetshandlingar står klart. Inom ramen för denna utredning har vi

[16] Svenska elektroniska underskrifter tillhandahålls i dagsläget främst via e-legitimationer som t.ex. BankID som utfärdas av banker eller Telias e-legitimation, se dock dir. 2017:90. Se även bl.a. *Skuldsanering – förbättrade möjligheter för överskuldsatta att starta om på nytt*, prop. 2015/16:125, s. 209.
[17] Artikel 25.
[18] Artikel 2.
[19] Artikel 2.

emellertid inte sett anledning att närmare analysera dessa frågor, främst mot bakgrund av andra utredningars uppdrag inom området.[20]

Originalinnehåll och originalexemplar

Pappersbaserade handlingar kan sägas bestå av tre delar med varsin urskiljbar funktion vilka tillsammans utgör en helhet:

- bäraren (papperet),
- texten (uppgifterna), och
- utställarangivelsen (t.ex. en underskrift).

Sambandet mellan bärare, text och utställarangivelse framstår i pappersmiljön som så självklar att endast bäraren (papperet) anges, t.ex. en faktura.[21] Även i den elektroniska miljön har man talat om *originalinnehåll* under förutsättning att ett visst informationsinnehåll t.ex. har skrivskyddats eller försetts med en elektronisk signatur så att det kan återskapas gång på gång utan risk för att det förvanskas.[22] Det har emellertid också hävdats att det inte på traditionellt sätt går att skilja ett *originalexemplar* från en kopia när data förs över från en databärare till en annan eftersom informationen endast förekommer som ett originalinnehåll.[23] Det förekommer också förarbetsuttalanden där ett elektroniskt original jämställs med en bestyrkt papperskopia.[24]

Informationshantering i digital miljö har länge byggt på kopiering av digitala data. Nya exemplar har därför normalt blivit att anse som identiska med sina förlagor. Om en elektroniskt underskriven handling kopieras så att alla data överförs utan ändringar har med andra ord flera ”original” uppstått. Originalet har därmed inte ansetts knutet till en unik bärare på samma sätt som text och underskrift varit knutna till ett pappersark. Förenklat har detta hittills sammanfattats som att det i elektronisk miljö funnits ett originalinnehåll men inte något originalexemplar.[25]

---

[20] Se bl.a. SOU 2017:114.
[21] *Ny bokföringslag m.m.*, prop. 1998/99:130, s. 245. Se också E-delegationens vägledning *Elektroniska original, kopior och avskrifter*, 7 juni 2012.
[22] *Offentlighetsprincipen och informationstekniken*, prop. 2001/02:70, s. 14. f.
[23] *Lag om kvalificerade elektroniska signaturer, m.m.*, prop. 1999/2000:117, s. 19.
[24] *Elektronisk ingivning till Bolagsverket*, prop. 2005/06:135, s. 63.
[25] Se bl.a. i not 16 angiven vägledning s. 12.

De tidigare ställningstagandena kan möjligen nu behöva revideras med anledning av framväxten av blockkedjetekniken och dess potential vad gäller att bl.a. säkerställa att ett dokument inte förvanskats (se kapitel 7.3.4 och 11.6.1).

Digitala tjänster och parallell pappershantering

Under kartläggningen har flera aktörer beskrivit för oss att ett enstaka formkrav, t.ex. ett krav på undertecknande av ett visst dokument, i och för sig inte hindrar framtagande av en digital tjänst. Den digitala tjänsten blir dock inte optimal eftersom det digitala förfarandet behöver kompletteras med en pappershantering där originalexemplaret med underskrift på papper måste tas om hand. Ibland behöver pappersexemplaret bevaras medan det i andra fall har beskrivits finnas förutsättningar för att skanna in dokumentet, gallra pappersexemplaret och fortsätta handläggningen digitalt.[26] Oavsett förutsättningarna innebär momentet för pappershantering en resursåtgång som förefaller onödig när en digital tjänst tillhandahålls och den enskilde använder den som kanal för kommunikation. Som beskrivits i kapitel 8 kan det förhållandet att en del av ärendehandläggningen görs digital samtidigt som pappersbaserade inslag behålls också försvåra insynen i såväl det enskilda ärendet som i verksamheten i stort.

Mot den beskrivna bakgrunden har vi sett ett särskilt behov av att fördjupa oss i frågan om anpassning av lagstiftning som kräver underskrift, undertecknande eller namnteckning – dvs. de formkrav som hittills, i vart fall i viss lagstiftning, har bedömts hindra digitala rutiner.

Frånvaro av författningskrav på underskrift

En av frågorna att ta ställning till för den som står i begrepp att utforma och tillhandahålla en digital tjänst är om det finns något formkrav som kräver underskrift på ansökningshandlingar och liknande skrifter till en myndighet. Regler om att handlingar ska skrivas under finns i vissa författningar (se vidare under följande rubrik),

[26] Riksarkivet kan i sina myndighetsspecifika föreskrifter (RA-MS) reglera statliga myndigheters möjligheter att gallra en fysisk handling som har skannats in.

men det finns inte något generellt formkrav av innebörd att framställningar till förvaltningen ska vara underskrivna. I förvaltningslagen finns däremot en bestämmelse om att en handling ska bekräftas av avsändaren om myndigheten anser att det behövs. Myndigheten kan alltså begära att en handling bekräftas av avsändaren genom t.ex. ett egenhändigt undertecknande om myndigheten anser att det är lämpligt. Formerna för hur bekräftelsen ska göras regleras dock inte i lagen.[27]

Det är inte enbart formkrav i gällande rätt utan i viss mån även frånvaron av såväl reglering som uttalanden i förarbeten om digitala underskrifter som har uppmärksammats för oss under kartläggningen. Vi har bl.a. fått frågor om vilka överväganden en myndighet ska göra när det gäller att säkerställa att uppgifter kan lämnas digitalt från en enskild ”på heder och samvete”, utan att de digitala tjänster som tas fram blir för krångliga att använda eller kostsamma att införa. Behövs en digital legitimering eller underskrift, även om det inte finns något lagkrav som särskilt reglerar detta? En reflektion från vår sida är att närmast rutinmässiga krav på undertecknande vid pappersförfaranden i vissa fall synes ha uppställts av myndigheter utan att det funnits krav i lag eller förordning som anger att det behövs.

Enligt vår bedömning är det inte möjligt att ge ett generellt svar på den ovan ställda frågan om det finns skäl för myndigheter att kräva legitimering eller underskrift i en digital tjänst även när det saknas lagkrav som anger det. Frågan behöver belysas utifrån förutsättningarna i det enskilda fallet. Vilket ärendeslag är det frågan om? Vilket beslutsunderlag i övrigt har myndigheten? Hur stor är risken för eventuellt missbruk i just den typ av ärenden som är aktuella? Vilka straffrättsliga bestämmelser kan aktualiseras även utan krav på legitimering eller underskrift i den digitala tjänsten? Kan eventuellt felaktigt utbetalda förmåner krävas åter? Bland annat dessa typer av frågeställningar bör en myndighet ta i beaktande vid utformningen av den digitala tjänsten, och om t.ex. service via telefon eller personligt möte är ett alternativ för dem som inte kan eller vill använda den digitala tjänst som tillhandahålls.[28]

[27] 21 § förvaltningslagen och *En modern och rättssäker förvaltning – ny förvaltningslag,* prop. 2016/17:180, s. 306 f.
[28] Se för närmare belysning av dessa frågor även *Juridisk vägledning för införande av e-legitimering och e-underskrifter*, eSam, februari 2017.

Författningskrav på underskrift

Författningskrav på underskrift kan betecknas med ett antal olika termer, varav underskriven, undertecknad och namnteckning är några. Ibland kompletteras de olika termerna med ordet ”egenhändig”. Exakt vad dessa krav innebär är emellertid inte helt klart.[29] Det finns ingen bestämmelse som anger hur kravet ska fullgöras och några vägledande förarbetsuttalanden är svåra att finna, såväl i fråga om hur kravet kan fullgöras som för vilka syften det finns. Att underskriften på något sätt och i någon form ska ange en utställare torde dock vara självklart. Ibland ger underskriften uttryck för en vilja. Den som skriver under något får anledning att överväga innebörden och vikten av det som undertecknats. I andra fall kan huvudsyftet med underskriften vara att koppla handlingen till en utställare och därmed garantera att viljeyttringen härrör från honom eller henne. I båda fallen är det utställarverifikationen som är det väsentliga. En underskrift har vidare ofta säkerhetsrelaterade funktioner genom att den utgör underlag för äkthetsprövning, bevissäkring och originalkvalitet. Syftet med dessa funktioner är att ge skydd mot förfalskning och förnekande.

De olika formuleringarna är knappast avsedda att ha olika innebörd. Någon sådan skillnad har inte heller framkommit vid den inventering av formkrav som Formel-gruppen tidigare genomförde.[30]

Termen undertecknad har på senare år fått en teknikoberoende betydelse i ett par författningar.[31] Kravet kan enligt dessa författningar alltså uppfyllas både genom undertecknande på papper eller med elektroniska medel. Beträffande flertalet författningar har emellertid samma begrepp, även under senare tid, bedömts endast kunna uppfyllas genom namnteckning med penna på papper.[32] Det finns alltså fortfarande skillnader i hur ett likalydande formkrav kan uppfyllas i olika författningar.

När krav på undertecknande under senare år har anpassats till digitala rutiner har olika lagtekniska konstruktioner valts. I några enstaka fall vid införande av ny reglering har, som anges ovan,

[29] Se även *Elektroniska underskrifter av domstolsavgöranden och vissa andra handlingar*, Justitiedepartementet, den 30 juni 2017, Ju2017/05823/KRIM.
[30] Ds 2003:29 s. 88.
[31] *Skatteförfarandet*, prop. 2010/11:165, s. 346 och *Skatteförslag med anledning av energiöverenskommelsen*, prop. 2016/17:142, s. 41 och 61.
[32] *Elektronisk stämningsansökan i brottmål*, prop. 2011/12:126 och *Elektronisk ansökan om lantmäteriförrättning*, prop. 2013/14:236.

begreppet undertecknande ansetts vara teknikoberoende. I många fall har emellertid begreppet undertecknande fått behålla sin ursprungliga innebörd, nämligen att det endast kan uppfyllas genom namnteckning med penna på papper. Kravet har då kompletterats med en möjlighet till elektronisk underskrift, ofta med angivande av att den elektroniska underskriften ska vara av viss kvalitet. Kvalitetskraven har vanligen inte konkretiserats i bestämmelserna utan hänvisning har skett till den numera upphävda lagen (2000:832) om kvalificerade elektroniska signaturer. Hänvisning sker nu i stället till eIDAS-förordningen i den ursprungliga lydelsen. Denna lagstiftningsteknik har använts i ett relativt stort antal författningar och nyligen lämnade förslag fortsätter att utgå från den tekniken.[33] En variant av denna lagtekniska konstruktion har varit att komplettera ett krav på undertecknande med en möjlighet att skriva under elektroniskt men utan angivande av vilken kvalitet som ska gälla för den elektroniska underskriften. Kvalitetskraven har då i stället reglerats på lägre normgivningsnivå, t.ex. i förordning eller myndighetsföreskrifter.[34]

Våra överväganden

Allt fler myndigheter och andra aktörer inom offentlig sektor står i begrepp att eller har redan börjat erbjuda tjänster som bygger på digitala funktioner för legitimering eller underskrifter.[35] Vi har därför sett det som särskilt angeläget att undersöka om vi inom ramen för denna utredning skulle kunna nå fram till en generell författningsändring i syfte att åstadkomma en förvaltningsgemensam reglering där digitala förfaranden för underskrifter så långt som möjligt likställs med pappersförfaranden. En sådan generell reglering på formkravsområdet vore särskilt önskvärd mot bakgrund av vad som ovan beskrivits om att samma termer i olika lagstiftning för närvarande ges olika innebörd. Sådana olikheter försvårar samverkan i en digital

[33] Se t.ex. 45 kap. 4 § rättegångsbalken, 11 § skuldsaneringslagen (2016:675), 111 kap. 5 § socialförsäkringsbalken, 2 kap. 7 § årsredovisningslagen (1995:1554) och 9 kap. 3 § lagen (2007:1091) om offentlig upphandling.
[34] Se t.ex. prop. 2013/14:236 s. 14 f.
[35] Se *Juridisk vägledning för införande av e-legitimering och e-underskrifter*, eSam, februari 2017 s. 3.

förvaltning, där utrymmet för att tolkning och tillämpning av rättsregler ska kunna skilja sig åt mellan myndigheter eller verksamheter är mer begränsat än i den analoga miljön (se kapitel 6.2).

Frågan om det i svensk rättsordning är möjligt eller lämpligt att införa en generell bestämmelse som skulle föreskriva att samtliga formkrav av en viss typ, t.ex. underskrift, skulle anses uppfyllda med vissa elektroniska rutiner har emellertid bedömts två gånger tidigare, med resultat att någon sådan generell bestämmelse i vart fall inte då bedömts vara lämplig.[36] I tiden därefter har lagstiftaren, om än inte helt enhetligt så ändå systematiskt, valt lagstiftningstekniken att ändra varje bestämmelse som innehåller formkrav så att det tydliggörs att elektroniska rutiner kan användas och vilka krav dessa måste uppfylla. Regeringen har nyligen lämnat en lagrådsremiss om elektroniska underskrifter av domstolsavgöranden och vissa andra handlingar.[37] Även där anges att någon generell slutsats innebärande att begreppet undertecknad numera skulle ha en annan innebörd än tidigare inte låter sig göras med ledning av endast ett fåtal bestämmelser. Innebörden av formkravet bör enligt regeringen i stället lämpligen bedömas för varje enskild bestämmelse med beaktande av den rättsliga miljö som aktuell bestämmelse finns i och hur kravet tidigare har bedömts.[38] I Regeringskansliets riktlinjer för författningsskrivning anges också att vid varje reform som berör ett flertal författningar ska man ändra i varje författning som berörs av reformen.[39]

Även med beaktande av att eIDAS-förordningen tillkommit och att det ligger i linje med den nya EU-rätten att jämställa digitala underskrifter med namnteckningar på papper, också när det gäller nationella formkrav, ser vi det som svårt att nu gå fram med ett förslag till en generell författningsbestämmelse som likställer digitala förfaranden med pappersförfaranden när det gäller vad som betecknas underskrift, undertecknande eller namnteckning.

Därtill kommer det förhållandet att teknikutvecklingen med bl.a. blockkedjeteknikens möjligheter att säkerställa digitala ursprungs-

[36] *Digitala signaturer - en teknisk och juridisk översikt* (Ds 1998:14) och Ds 2003:29. Jfr också IT-utredningens förslag i *Elektronisk dokumenthantering* (SOU 1996:40).
[37] *Digital hantering av domstolsavgörande, strafföreläggande och ordningsbot,* lagrådsremiss av den 25 januari 2018.
[38] A.a. s. 22.
[39] *Gröna boken – riktlinjer för författningsskrivning* (Ds 2014:1), s. 111.

filer synes gå fort framåt. Därmed kan tidigare gjorda ställningstaganden behöva omvärderas vad avser innehållet i digitala handlingar som verifieras av en utställare genom en underskrift. Det kan i sin tur påverka hur det lagtekniskt är önskvärt att utforma vissa författningskrav inom vissa rättsområden, t.ex. panträtten, utsökningsrätten, fastighetsrätten och bokföringsrätten. Mot bakgrund av detta och tidsramarna för vår utredning har vi sett svårigheter med att här göra välavvägda bedömningar om hur ett eventuellt generellt författningskrav skulle kunna utformas. Mot den beskrivna bakgrunden ser vi nu inte förutsättningar att nå framgång med ett förslag till generell reglering. Vi lämnar därför inte något författningsförslag i denna del.

Vår bedömning

Trots slutsatsen att vi inom ramen för denna utredning inte kan lämna ett generellt författningsförslag ser vi fortsatt att frågan om undanröjande av formkrav på underskrift, namnteckning eller undertecknande som kräver pappershantering bör vara högt prioriterad. Det finns enligt vår bedömning flera underlag att utgå från för fortsatt arbete med att anpassa formkrav i gällande rätt, inte minst den utredning som gjordes av Formel-gruppen, underlag från E-delegationen och det underlag som vi tagit del av under kartläggningen.

Det fortsatta lagstiftningsarbetet för att undanröja onödiga formkrav bör enligt vår uppfattning gagnas av den slags samordning som skisserats i kapitel 12.1.3. En sådan samordning skulle bl.a. ge goda förutsättningar för att fortsatt åstadkomma lagstiftning där t.ex. samma termer inte ges olika innebörd i olika författningar.

Här har närmast analyserats de frågor som gällt underskrifter och motsvarande krav i gällande rätt. Som framgått i kartläggningen (se kapitel 5.6.1) har vi emellertid fått flera exempel på när andra typer av bestämmelser i gällande rätt avseende förvaltningens ärendeprocesser reglerar krav på viss form för informationshanteringen. Det gäller t.ex. specifika krav på att vissa handlingar ska förmedlas med post eller att processteg som utgår från analoga förfaranden inte längre behövs vid en digital informationshantering. Även den typen

av formkrav bör enligt oss anpassas, i den takt och omfattning som bedöms nödvändig när myndigheter digitaliserar ärendeprocesser.

12.2.2 Registerförfattningar och informationsutbyten

Utredningens bedömning: Det bör prioriteras att, på ett samordnat sätt, metodiskt ta om hand de förändringar som behövs avseende registerförfattningarna för att inte i onödan hindra eller hämma det digitaliseringsarbete som bedöms vara önskvärt de kommande åren, särskilt med avseende på informationsutbyten mellan myndigheter.

Skälen för utredningens bedömning

Informationshanteringsutredningens överväganden och förslag

Att registerförfattningar kan hindra eller hämma digitala informationsutbyten har sedan länge uppmärksammats i olika sammanhang.[40] I oktober 2011 gav regeringen en särskild utredare i uppdrag att se över registerlagstiftningen och vissa därmed sammanhängande frågor i syfte att skapa rättsliga förutsättningar för en mer effektiv e-förvaltning, där såväl den enskildes rätt till personlig integritet som allmänhetens berättigade anspråk på insyn i den offentliga verksamheten tillgodoses.[41] Utredningen tog namnet Informationshanteringsutredningen. Utredningens uppdrag hade sin bakgrund i att det i olika sammanhang framförts kritik mot registerlagstiftningen för att vara ett svåröverblickbart och fragmenterat rättsområde med bristande enhetlighet i struktur och normtekniska lösningar samt med, i en del fall, otillräcklig anpassning till annan lagstiftning av central betydelse för myndigheternas informationshantering såsom tryckfrihetsförordningens bestämmelser om allmänna handlingar och offentlighets- och sekretesslagen (2009:400). Utredningen delade i stort den problembilden och kunde konstatera att problemen skapar osäkerhet i tillämpningen, vilket bl.a. gör uppgiftsutbyte och annat samarbete mellan myndigheter onödigt komplicerat. Utredningen fann att regelverkens struktur försvårade för enskilda registrerade

[40] Se t.ex. *It-stödet i rättskedjan*, Riksrevisionen, 30 september 2011, RiR 2011:25, s. 97.
[41] *Integritet, effektivitet och öppenhet i en modern e-förvaltning* (dir. 2011:86).

och allmänheten att förstå vad som egentligen gäller för myndigheters informationshantering. Vidare angavs det vara ett problem i sig att registerlagar ofta behöver ändras till följd av att myndigheterna får nya uppgifter.

Mot bakgrund av bl.a. den identifierade problembilden, och ytterligare svårigheter,[42] fann utredningen ett angeläget behov av förändringar i den reglering som rör personuppgiftsbehandling inom den offentliga sektorn. En samlad reglering i en lag om myndigheters behandling av personuppgifter bedömdes göra det möjligt att åstadkomma ett tydligt regelverk som är lättare att tillämpa och bättre anpassat till övrig reglering av myndigheters informationshantering. En sammanhållen lag skulle också ge bättre förutsättningar för allmänhetens insyn och för enskilda registrerades möjligheter att göra gällande sina rättigheter enligt det dataskyddsrättsliga regelverket. Ytterligare en aspekt var att en samlad reglering vore mer ändamålsenlig för att möta den vid det tillfället ännu inte beslutade dataskyddsreformen inom EU.

Givet beskrivningen ovan föreslog utredningen en ny lag, myndighetsdatalagen, som skulle likna de befintliga registerförfattningarna men innehålla generellt tillämpliga bestämmelser omfattande alla statliga och kommunala myndigheters personuppgiftsbehandling (bortsett från den brottsbekämpande sektorn). Regleringen borde enligt utredningen bl.a. utformas som en renodlad persondataskyddsreglering som bara tog sikte på frågor om skydd för personuppgifter som uppstår i myndigheternas elektroniska informationshantering. Bestämmelserna i den nya lagen skulle alltså inte i något avseende syfta till att reglera en myndighets sakverksamhet. Renodlade registerförfattningar om inrättandet och förandet av vissa specifika register bedömdes utgöra en slags verksamhetsreglering som även i fortsättningen borde regleras i särskild ordning (jfr kapitel 12.2.4 om grunddata och informationsförsörjning).

Till den nya lagen skulle det kunna finnas bilagor och en anslutande förordning. Efter hand som behov av sektors- eller myndighetsspecifika särregler uppstod kunde sådana tas in i en systematiskt ordnad reglering som skulle komplettera den nya lagen. På så sätt skulle ett sammanhållet ramverk med enhetligt utformad reglering kunna uppnås, både vad avser förhållanden som kunde regleras generellt och förhållanden där fortsatta särregler – utifrån närmare

[42] *Myndighetsdatalag* (SOU 2015:39), s. 22.

avvägningar mellan integritetsintressen och t.ex. effektivitetshänsyn på området i fråga – behövdes. Utredningen bedömde emellertid att behovet av fortsatt särreglering skulle komma att minska betydligt, och oftast kunna ges i förordning vilket skulle förenkla regelgivningen och underlätta nödvändiga förändringar. Den nya lagen skulle inte heller utesluta att det även fortsättningsvis för vissa myndigheter eller verksamheter skulle komma att bedömas mera lämpligt med särreglering i separat författning som skulle gälla utöver den nya lagen.[43]

EU:s dataskyddsreform

Den 27 april 2016 antogs den nya dataskyddsförordningen.[44] Dataskyddsförordningen utgör en ny generell reglering för personuppgiftsbehandling inom EU och kommer att ersätta dataskyddsdirektivet från år 1995. Förordningen börjar tillämpas den 25 maj 2018. Det huvudsakliga syftet med förordningen är att ytterligare harmonisera och effektivisera skyddet för personuppgifter för att förbättra den digitala inre marknadens funktion och öka enskildas kontroll över sina personuppgifter.

Från dataskyddsförordningens tillämpningsområde undantas bl.a. personuppgiftsbehandling som utförs av behöriga myndigheter i syfte att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straff, inkluderande skydd mot, samt förebyggande av, hot mot den allmänna säkerheten. Den personuppgiftsbehandling som görs för dessa syften faller i stället under det nya dataskyddsdirektivets tillämpningsområde.[45] Direktivet ska dels skydda fysiska personers grundläggande fri- och rättigheter, särskilt deras rätt till skydd av personuppgifter, dels underlätta det informationsutbyte mellan behöriga myndigheter som är nödvändigt enligt unionsrätt eller nationell rätt.

[43] A.a. s. 22 f.
[44] Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[45] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

Från både dataskyddsförordningens och det nya dataskyddsdirektivets tillämpningsområden undantas personuppgiftsbehandling i verksamhet som inte omfattas av unionsrätten, däribland området nationell säkerhet.

EU:s dataskyddsreform har lett till en bred översyn av svenska författningar om personuppgiftsbehandling. Här finns inte möjlighet att gå igenom allt det lagstiftningsarbete som i anledning av EU:s dataskyddsreform alltjämt pågår på registerförfattningarnas område. Det bör dock nämnas att regeringen bl.a. lagt förslag till ny lag med kompletterande bestämmelser till EU:s dataskyddsförordning.[46] På det brottsbekämpande området har Utredningen om 2016 års dataskyddsdirektiv lämnat förslag till dels en sammanhållen ramlag, brottsdatalagen, dels anpassningar i de registerförfattningar som ska tillämpas inom detta område.[47]

Kartläggningsresultatet

Den problembild med avseende på registerförfattningar och digitala informationsutbyten som länge varit känd har bekräftats i vårt kartläggningsarbete. Myndighetsrepresentanter har bl.a. varit relativt samstämmiga i uppfattningen att dataskyddsregleringen är svåröverskådlig, komplex, fragmenterad och onödigt detaljerad. Det har beskrivits att detaljregleringen avseende informationsutbyten på vissa håll lett till att regelverket över tid har blivit något av ett lappverk efter ett antal författningsändringar. I olika registerförfattningar har det också utvecklats olika begreppsanvändning. Några av dem vi mött har också framfört att det vore önskvärt att författningsreglera digitala informationsutbyten på mer principiell nivå, eventuellt inom ramen för en generell myndighetsdatalag efter den omarbetning av registerförfattningarna som EU:s numera beslutade dataskyddsreform lett till.

[46] *Ny dataskyddslag*, prop. 2017/18:105.
[47] Utredningen om 2016 års dataskyddsdirektivs delbetänkande *Brottsdatalag* (SOU 2017:19) och slutbetänkande *Brottsdatalag – kompletterande lagstiftning* (SOU 2017:74). Se även lagrådsremissen *Brottsdatalag*, den 1 mars 2018.

Våra överväganden

I vart fall inom vissa delar av förvaltningen kvarstår, och kommer det att kvarstå även efter anpassningen av svensk rätt till EU:s dataskyddsreform, fortsatta behov av att anpassa registerförfattningar för att dessa inte, på ett sätt som kan anses vara onödigt, ska hindra eller hämma förvaltningens digitalisering. Det gäller främst med avseende på informationsutbyten mellan myndigheter men i vissa avseenden även digital kommunikation med enskilda. I kapitel 5.5.2 har beskrivits att bl.a. regleringen om direktåtkomst respektive utlämnande på medium för automatiserad behandling fortfarande orsakar svårigheter, inte minst när det gäller en på vissa håll detaljerad reglering om direktåtkomst. Andra områden som beskrivits kunna utgöra onödigt hindrande eller hämmande reglering i registerförfattningar rör snävt formulerade ändamålsbestämmelser respektive sökbegränsningar (se även vad som beskrivits i kapitel 6.2).

Området för registerförfattningarna är talande för de slutsatser vi dragit om att det erfarenhetsmässigt är svårt att genom stora grepp genomföra förändringar i den lagstiftning som kringgärdar förvaltningens informationshantering. Förvaltningen är dessutom nu i ett läge där förväntningar finns på ökad digitalisering de närmaste åren. Vi menar därför att det inte vore lämpligt att helt avvakta genomförandet av ytterligare, efter dataskyddsreformen, större grepp avseende registerförfattningarna. Det bör i stället kunna prioriteras att inom ramen för ett sådant beredningsorgan som skisserats i kapitel 12.1.3 metodiskt ta om hand vissa av de förändringsbehov på området för registerförfattningarna som är nödvändiga för det digitaliseringsarbete som bedöms vara önskvärt de kommande åren. I det arbetet kan också strävan vara att åstadkomma förändringar som på sikt är förenliga med en mer generell reglering för myndigheter på dataskyddsförordningens område, i linje med såväl den föreslagna myndighetsdatalagen som den föreslagna ramlagen på det brottsbekämpande området.

12.2.3 Sekretessreglering och informationsutbyten

Utredningens bedömning: Det förslag som Utredningen om rätt information i vård och omsorg har lämnat om att en sekretessbrytande bestämmelse ska införas i offentlighets- och sekretesslagen och som innebär att socialtjänstsekretess inte ska hindra att uppgift lämnas från en myndighet som bedriver verksamhet inom socialtjänsten i en kommun till en annan sådan myndighet i samma kommun, bör övervägas i Regeringskansliet.

Skälen för utredningens bedömning

Kartläggningsresultatet

I kapitel 6.2 har vi anfört att digital informationshantering, exempelvis digitala informationsutbyten mellan myndigheter, vanligen ställer krav på en väsentligt större exakthet än vad som har behövts i en manuell eller analog miljö, där rutiner och andra förfaranden har kunnat bestämmas och anpassas efter hand. Kravet på exakthet innebär att en myndighet på förhand, dvs. innan ett digitalt informationsutbyte sker, behöver ha vetskap om exakt vilka uppgifter som ska överföras. Behovet av vetskap på förhand gör sig också gällande i fråga om sekretessgränser mellan myndigheter eller verksamhetsgrenar inom en organisation. Sådana sekretessgränser kan få till följd att det i den digitala miljön inte går att följa en hel ärendeprocess på det sätt som i övrigt, särskilt av rättssäkerhetsskäl och insynsskäl, är önskvärt. I den digitala miljön ställs alltså rättsfrågor på sin spets som behöver lösas på förhand, till skillnad från tidigare när pappershandlingar, pärmar och underlag har kunnat hanterats på ett pragmatiskt sätt. Det har beskrivits för oss att bl.a. dessa aspekter leder till osäkerheter vad gäller diarieföring och ärendeprocesser i den digitala miljön. Det har också beskrivits för oss att detta medför att myndigheter fortsätter med pappershanteringen.

Sekretessregleringen kommer även i andra avseenden i ljuset i samband med förvaltningens digitalisering, se t.ex. vad som i kapitel 5.2.3 har anförts om hur enstaka uppgifter skulle kunna generera nytta i förvalslistor. Även snävt formulerade uppgiftsskyldigheter har anförts utgöra ett område där behov av författningsändringar i samband med utvecklingsarbeten inte alltid har

prioriterats, med följd att de tjänster som tas fram inte når den fulla potentialen.

Med beaktande av att vi haft att prioritera förvaltningsgemensamma frågor har vi inte kunnat fördjupa oss i flertalet av de specifika sekretessfrågor som framkommit i vår kartläggning. Vi har dock sett anledning att närmare analysera en särskild fråga om sekretessgränser inom kommunal verksamhet, eftersom frågan rör en betydande del av förvaltningen.

Sekretessgränser inom kommunal verksamhet

Tidigare fanns det i princip en kommunal nämnd för varje verksamhetsområde. Införandet av den fria kommunala nämndorganisationen på 1990-talet har inneburit att en kommun har möjlighet att dela upp en verksamhet, t.ex. socialtjänsten, på flera sektorer som organisatoriskt hör till olika nämnder. Det förekommer exempelvis en geografisk uppdelning på kommundelsnämnder, men det kan även vara en uppdelning på olika kompetensområden eller utifrån ett beställar- och utförarperspektiv. Av 8 kap. 1 § offentlighets- och sekretesslagen framgår att sekretess gäller mellan myndigheter. Eftersom varje nämnd är att anse som en egen myndighet i offentlighets- och sekretesslagens mening gäller sekretess mellan olika nämnder inom samma kommun. Utbyte av uppgifter kan således inte göras mellan nämnderna utan en föregående sekretessprövning.

Sekretess kan i vissa fall enligt 8 kap. 2 § offentlighets- och sekretesslagen även gälla inom en och samma nämnd, nämligen om det inom nämnden finns verksamhetsgrenar som är att betrakta som självständiga i förhållande till varandra. En självständig verksamhetsgren i förhållande till en annan verksamhet inom en myndighet uppstår om det är fråga om olika verksamhetsgrenar och dessa är självständiga i förhållande till varandra. Om olika delar av myndighetens verksamhet ska tillämpa helt olika uppsättningar av sekretessbestämmelser kan det vara fråga om olika verksamhetsgrenar. Ifall verksamheterna bedöms vara olika verksamhetsgrenar måste man också bedöma om de har organiserats på ett sådant sätt att de förhåller sig självständiga till varandra. Om dessa både kriterier är uppfyllda finns en sekretessgräns inom myndigheten. Omständigheter av betydelse för bedömningen av självständigheten kan vara att

organet självständigt förvaltar viss egendom, har viss handlingsfrihet inom en angiven ekonomisk ram eller i övrigt kan vidta vissa faktiska åtgärder självständigt och på eget ansvar. Andra omständigheter som påverkar bedömningen kan vara att man i vissa frågor beslutar självständigt och i eget namn.

Sekretess inom socialtjänsten

Sekretess gäller enligt 26 kap. 1 § offentlighets- och sekretesslagen inom den offentligt utförda socialtjänsten för uppgift om enskilds personliga förhållanden om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående lider men. Med socialtjänst avses enligt nämnda bestämmelse huvudsakligen verksamhet enligt lagstiftningen om socialtjänst och den särskilda lagstiftningen om vård av unga och av missbrukare utan samtycke samt verksamhet som i annat fall enligt lag bedrivs av socialnämnd eller av Statens institutionsstyrelse.

Behov av en sekretessbrytande bestämmelse för socialtjänstsekretess

Under kartläggningen har det framkommit att uppgifter hänförliga till verksamhet främst inom socialtjänsten på grund av sekretess inte kan lämnas från en kommunal nämnd till en annan sådan nämnd i samma kommun. Sådana sekretessgränser mellan olika verksamheter i samma kommun skapar problem för verksamheten genom att hindra nödvändiga och ändamålsenliga digitala informationsutbyten mellan verksamheterna. Det har från flera håll ifrågasatts om kommunernas val av organisation ska medföra sekretessgränser som inte är sakligt motiverade och om det är rimligt att kommuner ska välja en organisationsform endast utifrån sekretessöverväganden.

På socialtjänstens område finns inte någon sekretessbrytande bestämmelse motsvarande den som gäller för hälso- och sjukvårdsområdet och som innebär att sekretess inte hindrar att uppgift lämnas från en myndighet som bedriver hälso- och sjukvård i en kommun till en annan sådan myndighet i samma kommun.[48] Bestämmelsen infördes i samband med införandet av patientdatalagen (2008:355).[49]

[48] 25 kap. 11 § offentlighets- och sekretesslagen.
[49] *Patientdatalag m.m.*, prop. 2007/08:126, s. 164 f.

Förslaget från Utredningen om rätt information i vård och omsorg

Utredningen om rätt information i vård och omsorg lämnade i slutbetänkandet *Rätt information på rätt plats i rätt tid* förslag till en mer ändamålsenlig sekretessreglering i socialtjänsten. Utredningen föreslog att en sekretessbrytande bestämmelse skulle införas i 26 kap. 8 § offentlighets- och sekretesslagen enligt nedan.

> Sekretessen enligt 1 § hindrar inte att uppgift lämnas […] från en myndighet som bedriver verksamhet som avses i 1 § i en kommun till en annan sådan myndighet i samma kommun […].

Förslaget innebar att en uppgift kan lämnas, utan hinder av socialtjänstsekretess, från en myndighet som bedriver verksamhet inom socialtjänsten till en annan sådan verksamhet i samma kommun.[50] Förslaget bereds i Regeringskansliet.

Datainspektionen avstyrkte förslaget i betänkandet som helhet. Vad avser den nu diskuterade delen menade Datainspektionen att förslag[51] som innebär en sådan förändring i åtkomsten till ytterst integritetskänsliga personuppgifter kräver en mer grundlig utredning och analys över de konsekvenser behandlingen kan komma att få för de enskildas personliga integritet.[52]

Riksdagens ombudsmän (JO) var emellertid positiv till förslaget. JO anförde att det inte fanns någon anledning till att den kommun som väljer att organisera socialtjänsten inom olika nämnder ska ha svårare att utbyta information och samverka än en kommun som valt att behålla socialtjänsten inom en och samma nämnd.[53]

Även Göteborgs kommun och Sandvikens kommun ställde sig positiva till förslaget eftersom det innebär att kommunens organisationsfrihet inte kommer att inverka på möjligheten att bedriva socialtjänstverksamhet på ett effektivt sätt och utifrån den enskilda kommunens bästa. Göteborgs universitet, Sahlgrenska akademin ansåg att förslaget att låta dokumentationen följa patienten och inte organisationen i princip var bra, i synnerhet för personer med mer

[50] SOU 2014:23 s. 604 f., 1074 och 1216.
[51] Det kan påpekas att Datainspektionen yttrade sig på samma gång över utredningens förslag om att en socialnämnd ska ha möjlighet till direktåtkomst till personuppgifter som behandlas hos en annan sådan nämnd i samma kommun.
[52] Datainspektionens yttrande över SOU 2014:23 Rätt information på rätt plats i rätt tid, den 8 december 2014, dnr 1568-2014.
[53] JO:s yttrande över betänkandet Rätt information på rätt plats i rätt tid (SOU 2014:23), den 7 november 2014, dnr R 54-2014.

omfattande social problematik, men menade att förslagets fördelar bör vägas mot integritets- och förtroendeproblematiken.[54]

Våra överväganden

Införandet av den fria kommunala nämndorganisationen har medfört att nya sekretessgränser kan uppstå beroende på hur en kommun väljer att organisera sin verksamhet, även om de överväganden som ligger till grund för vald organisationsform inte har någon relevans för sekretessfrågan. Detta har enligt oss lett till att lagstiftningen försvårar en digital informationshantering som inte kan motiveras av sekretesskäl.

Förslaget från Utredningen om rätt information i vård och omsorg om ett sekretessbrytande undantag från socialtjänstsekretess för uppgiftslämnande inom samma kommun, skulle innebära att kommuner får ökade möjligheter att organisera sin verksamhet inom socialtjänsten utifrån lokala behov och förutsättningar utan att omotiverade sekretessgränser uppstår. Med hänsyn till att antalet aktörer som bedriver socialtjänst har ökat väsentligt och att det skett en strukturförändring på socialtjänstens område[55] är det angeläget att socialtjänsten har en informationshantering som är ändamålsenlig och sammanhållen. Förslaget bidrar därmed till en mer effektiv och ändamålsenlig förvaltning. För den enskilde möjliggörs i större utsträckning en informationshantering utifrån hans eller hennes behov av stöd, service, vård och behandling, vilket stärker förutsättningarna för en god och effektiv socialtjänst av hög kvalitet. Förutsättningarna för att bedriva socialtjänst blir lika över landet och är inte beroende av hur enskilda kommuner valt att organisera sin verksamhet inom socialtjänsten.

Förslaget innebär inte någon generell lättnad av socialtjänstsekretessen. Enskildas behov av skydd för integritetskänsliga uppgifter på området tillgodoses fortfarande. Det bör betonas att för en kommun som väljer att organisera sin verksamhet så att all socialtjänst lyder under samma nämnd uppkommer inte några sekretess-

[54] Remissammanställning över betänkandet Rätt information på rätt plats i rätt tid (SOU 2014:23), S 2014700112/FS, s. 205 f.
[55] Se om socialtjänstens utveckling i SOU 2014:23 s. 560 f.

gränser mellan de verksamheter som faller under området socialtjänst. Vi menar därför att förslaget inte innebär någon försämring av den enskildas personliga integritet.

Även om det inte gäller någon sekretess mellan socialtjänstmyndigheter i samma kommun bör en klients uttryckliga önskemål om att hans eller hennes uppgifter inte ska lämnas till en annan socialtjänstmyndighet i kommunen normalt respekteras. Det får anses följa av bestämmelserna i 1 kap. 1 § socialtjänstlagen (2001:453) och 6 § lagen (1993:387) om stöd och service till vissa funktionshindrade (LSS) om att verksamheten ska bygga på respekt för den enskildes självbestämmanderätt och integritet. I linje med detta bör en enskilds önskemål om att uppgifterna om honom eller henne inte ska lämnas från en socialtjänstmyndighet till en annan sådan myndighet inom kommunen normalt sett respekteras.

Generalklausulen i 10 kap. 27 § offentlighets- och sekretesslagen, som innebär att sekretessbelagda uppgifter får lämnas till en myndighet om det är uppenbart att intresset av att uppgifterna lämnas har företräde framför det intresse som sekretessen ska skydda, är inte tillämplig för några få sekretessområden, bl.a. hälso- och sjukvårdssekretessen och socialtjänstsekretessen. Det innebär att de sekretessgränser som kan uppstå mot bakgrund av den fria kommunala nämndorganisationen har skapat särskilda problem inom bl.a. områdena hälso- och sjukvård och socialtjänst. Med hänsyn till hur nämnderna var organiserade innan den fria kommunala nämndorganisationen infördes innebär förslaget från sekretessynpunkt i praktiken en återgång till den tidigare gällande ordningen. Motsvarande argument anfördes i det lagstiftningsärende som ledde till att en sekretessbrytande bestämmelse infördes på hälso- och sjukvårdsområdet för att möjliggöra informationsutbyte inom samma kommun.[56] Vi anser att socialtjänsten inom en kommun bör ha motsvarande möjlighet som hälso- och sjukvården har att utbyta uppgifter.

Mot denna bakgrund ansluter vi oss till förslaget från Utredningen om rätt information i vård och omsorg om en sekretessbrytande bestämmelse som innebär att socialtjänstsekretess inte hindrar att en uppgift lämnas från en myndighet inom socialtjänsten i en kommun till en annan sådan myndighet i samma kommun. Vi

[56] Prop. 2007/08:126 s. 164 f.

anser att förslaget bör tas upp för övervägande i Regeringskansliet, särskilt med den pågående digitaliseringen i förvaltningen i åtanke.

Vi har övervägt om problemet med sekretessgränser finns inom fler områden i förvaltningen än inom socialtjänsten och om det kan finnas behov av en generell reglering i frågan i syfte att främja pågående digitalisering. Som nyss nämnts finns det en sekretessbrytande bestämmelse inom hälso- och sjukvård som motsvarar den som Utredningen om rätt information i vård och omsorg har föreslagit för socialtjänstområdet. Eftersom generalklausulen är tillämplig på de flesta andra sekretessområden innebär det att en verksamhet som delas upp på flera myndigheter i de flesta fall har goda möjligheter att med stöd av den bestämmelsen utbyta uppgifter om det behövs.[57] Vi har därför inte nu kunnat se att det finns behov av en generell sekretessbrytande bestämmelse som möjliggör digitalt informationsutbyte mellan myndigheter som bedriver verksamhet inom samma verksamhetsområde i samma kommun.

12.2.4 Grunddata och informationsförsörjning

Utredningens bedömning: Parallellt med att nya former för att anordna förvaltningens informationsförsörjning övervägs, exempelvis hur grunddata ska tillhandahållas, bör författningsändringar i vissa registerförfattningar övervägas.

Skälen för utredningens bedömning

Kartläggningsresultatet

I kapitel 4 har vi redogjort för att den offentliga förvaltningen har en central roll i att förse samhället i stort med information. Myndigheterna står för en stor del av produktionen av den datamängd som det digitala samhället bygger på. Den information som samlas in, produceras och lagras inom förvaltningen har både ekonomiska och samhällsnyttiga värden. Att ta tillvara på dessa värden bidrar till att öka tillväxten i samhället. Innovationer som bygger på myndigheters informationsmängder kan också i förlängningen användas av det

[57] A. prop. s. 165.

offentliga och i sin tur bidra till en än mer effektiv och rättssäker förvaltning. Öppenhet i den digitala förvaltningen är också centralt för den demokratiska förankringen av förvaltningens verksamhet.

Det finns emellertid, som också kartläggningen visar, ett antal frågeställningar med anknytning till myndigheters roll att försörja samhället med information. Det gäller bl.a. regleringen av ansvar för vissa myndigheter att särskilt svara för viss informationsförsörjning samt frågor som rör elektroniskt utlämnande av allmänna handlingar i förhållande till tillhandahållande av information som öppna data (se vidare i kapitel 12.5–12.7). Frågor om finansieringsmöjligheter har i dessa avseenden också nära samband med de rättsliga frågeställningarna.

Rättsregler om ansvar för information

Rättsregler som avser myndigheters ansvar för information finns i olika typer av författningar. Viss reglering som avser ansvar för information utgår från att skydda eller tillvarata särskilda intressen som informationssäkerhet,[58] skydd för personuppgifter,[59] god offentlighetsstruktur[60] eller arkiv.[61] Annan typ av reglering kan snarare innebära att en viss myndighet pekas ut som ansvarig för informationens innehåll, lagring och utlämnande av information. Ofta stöds sådan verksamhet av särskilda register som är reglerade i särskilda författningar.[62] Det förekommer emellertid också reglering som ålägger myndigheter ansvar för att tillgängliggöra information reglerat ur ett mer processuellt perspektiv och som inte förutsätter ett särskilt register eller något annat särskilt medel för tillgängliggörandet.[63]

[58] Se t.ex. förslag till 2 kap. 2 § ny säkerhetsskyddslag i prop. 2017/18:89, 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1)
[59] Se t.ex. dataskyddsförordningen.
[60] Se t.ex. 4 kap. offentlighets- och sekretesslagen.
[61] Se t.ex. arkivlagen (1990:782).
[62] Se t.ex. lag (1998:620) om belastningsregister och lag (2000:224) om fastighetsregister.
[63] Se t.ex., vad gäller information om avgöranden i domstols dom eller beslut, bl.a. 26–31 §§ förordningen (1996:271) om mål och ärenden i allmän domstol med hänvisning till förordningen (2003:234) om tiden för tillhandahållande av domar och beslut, m.m. jämförd med förordningen (1970:517) om rättsväsendets informationssystem.

Under kartläggningsarbetet har vi i olika sammanhang uppmärksammats på frågor som gällt behov av att peka ut ”ägarskap” av information. Begreppet ”ägarskap” av information i relation till förvaltningens åtgärder med uppgifter är emellertid problematiskt ur ett rättsligt perspektiv mot bakgrund av vad som ovan beskrivits om reglering som med hänsyn till olika intressen definierar ansvar för informationen. Vi väljer därför att inte använda termen ägarskap i detta sammanhang. Det är inte heller givet att det rättsligt utpekade ansvaret för en viss informationsmängd vid varje tillfälle och ur alla de perspektiv som ovan har nämnts i dag är placerat hos en och samma aktör, även om detta är en naturlig utgångspunkt. I regleringen om ansvar för arkivbildning finns exempelvis vissa bestämmelser om ansvarsfördelning, som inte omedelbart speglas i t.ex. regleringen som avser ansvar för att skydda informationens säkerhet.[64] Frågor om vilket ansvar för, eller vilken rådighet över, uppgifter som myndigheter bör ha behöver mot den beskrivna bakgrunden belysas mer detaljerat och med alla de beskrivna rättsområdena i åtanke, beroende på vilken förändring som är önskvärd i samband med att nya former för t.ex. informationsförsörjning övervägs.

Förutom de beskrivna typerna av reglering bör även sekretessregleringen nämnas här som ytterligare ett rättsområde att beakta i samband med att nya former för informationsförsörjning övervägs, om de nya formerna medför en spridning av information som inte existerar i den analoga miljön.

[64] Se 3 § första stycket andra meningen arkivlagen, där ansvaret för arkivbildningen avgränsas till den myndighet som svarar för huvuddelen av upptagningen, och komplettering i 4 § arkivförordningen där Riksarkivet bemyndigas att föreskriva om en sådan avgränsning om flera myndigheter svarar för ungefär lika stora delar av upptagningen. Jfr t.ex. med 19 § förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, i vilken varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt.

Centraliserade eller decentraliserade system

Datoriserade register eller system för att tillhandahålla information åt andra aktörer inom den offentliga förvaltningen eller åt samhället i stort har funnits sedan 1960-talet.[65] Nya möjligheter med anledning av känd och kommande digital informations- och kommunikationsteknologi föranleder emellertid löpande att sätten för att lagra och tillgängliggöra information ses över.

I syfte att nu skapa bättre förutsättningar för en mer ändamålsenlig och effektiv informationsförsörjning pågår bl.a. arbete inom ramen för eSamverkansprogrammet.[66] Inom vissa områden har det också tagits fram digitala tjänster för tillgängliggörande av information.[67] På andra områden övervägs det för närvarande om en central registerhantering eventuellt inte längre är den tryggaste och mest effektiva lösningen för att tillhandahålla vissa grundläggande uppgifter som efterfrågas ofta och därför är av stor betydelse för det allmänna. Säkrare och mer effektiva lösningar där korrekt och aktuell information hämtas från andra digitala källor inom förvaltningen, där data först samlas in eller produceras, kan vara ett bättre alternativ.

I utredningens kartläggning har det framkommit att det även ur ett rättsligt perspektiv finns problem förknippade med att hålla centrala register för tillhandahållande av grundläggande information. Det har bl.a. framförts att en sådan informationshantering kan leda till att uppgifter lagras i kopior på flera håll inom förvaltningen. Dels behöver den registeransvariga myndigheten ofta samla in uppgifterna från en annan myndighet, där de först samlats in eller producerats och lagras. Dels förekommer det att andra aktörer (både myndigheter och privata) hämtar sådan registerinformation vid mer enstaka tillfällen för att därefter själv lagra en kopia av registret. Lagring av samma uppgifter på flera håll inom förvaltningen medför problem att på varje ställe hålla uppgifterna korrekta och aktuella,

[65] År 1966 inleddes t.ex. arbetet med att bygga upp rättsväsendets informationssystem (RI). År 1968 fattade riksdagen principbeslut om uppbyggnaden av ett centralt ADB-baserat fastighetsregister och året därpå om inrättandet av ett ADB-baserat fordonsregister gemensamt för hela landet. (Se Datasamordningskommitténs betänkande *ADB och samordning* (SOU 1976:58), s. 72 f.)

[66] *Rapport – En effektiv informationsförsörjning,* eSam, 29 maj2017.

[67] Bland annat finns den sammansatta bastjänsten SSBTEK. Genom tjänsten kan handläggare inom socialtjänstens verksamhetsområde ekonomiskt bistånd få utlämnat information från a-kassorna, Arbetsförmedlingen, CSN, Försäkringskassan, Pensionsmyndigheten och Skatteverket. Se kapitel 5.11.5 för en närmare beskrivning av tjänsten.

vilket i sin tur leder till såväl verksamhetsmässiga nackdelar som brister i fråga om hanteringen av personuppgifter. Som exempel på den sistnämnda typen av brister kan nämnas risk för att uppgifter i en dubbellagrad kopia inte uppdateras efter att en person erhållit skyddad identitet, med följd att det kanske inte finns praktiska förutsättningar att förhindra att sådana känsliga uppgifter röjs på ett otillbörligt sätt.

Problemen med inaktuella uppgifter i kopior av register förstärks när de myndigheter som ansvarar för att tillhandahålla information förutsätts ta ut avgifter för utlämnandet, eftersom avgifterna sänker incitamenten för mottagaren att löpande inhämta uppdateringar.

Vad som tidigare talat emot mer decentraliserade system är bl.a. tekniska svårigheter att åstadkomma sökmöjligheter för att finna efterfrågade uppgifter och att decentraliserade system sammantaget skulle vara mer kostsamma. Det har emellertid redan tidigare framförts att det ur ansvarssynpunkt finns fördelar med decentraliserade system, där den myndighet som först samlat in eller producerat uppgifter också tar ansvar för både innehåll och spridning.[68] Samtidigt finns det enligt vår bedömning områden där det fortfarande, av olika skäl, inte är lämpligt eller möjligt att anordna informationsförsörjningen på något annat sätt än genom ett centralt register.[69]

Våra överväganden

I takt med att de tekniska förutsättningarna förändras behöver även de finansiella och de rättsliga förutsättningarna anpassas så att förvaltningen och samhället i övrigt ges de bästa förutsättningarna för en god informationsförsörjning. Vi kan konstatera ett kommande behov av att se över särskilt de äldre formerna av registerförfattningar som bl.a. förutsätter att centrala register förs för insamling, lagring och tillgängliggörande av information. Det finns emellertid inte förutsättningar att inom ramen för denna utredning göra de överväganden eller lämna de förslag till författningsändringar som kommer att behövas för de olika registren. Behovet av författningsändringar bör i stället övervägas parallellt med att nya former för att tekniskt anordna informationsförsörjningen övervägs, t.ex.

[68] Se bl.a. *Den fortsatta utvecklingen av rättsinformationssystemet* regeringens skrivelse 2003/04:168, s. 26 f.
[69] Se t.ex. *Nationell läkemedelslista* (Ds 2016:44).

vad gäller sätten för att tillhandahålla grunddata. Med beaktande av det pågående förändringsarbetet, bl.a. med avseende på den nya Myndigheten för digital förvaltnings kommande roll, kan vi inte nu komma med detaljerade förslag som rör det här beskrivna behovet av författningsöversyn.

Vi vill emellertid särskilt peka på att även frågor om skyldigheter för myndigheter att hämta uppgifterna från viss digital källa i stället för att efterfråga dem hos enskilda bör övervägas i det ovan beskrivna sammanhanget. En sådan regleringsansats skulle väsentligt främja principen om att uppgifter, så långt det är möjligt, endast ska lämnas en gång till förvaltningen (The Once-Only Principle, TOOP).

Om det regleras att uppgifter ska hämtas från en utpekad digital källa bör det vidare finnas eller ges förutsättningar som innebär att dessa uppgifter inte alltid behöver kommuniceras med enskilda i varje enskilt ärende enligt 25 § förvaltningslagen, i de fall de utgör beslutsunderlag. Det bör enligt vår bedömning kunna vara tillräckligt att enskilda har möjlighet att kontrollera och t.ex. begära rättelse av uppgifterna vid källan med beaktande av att dataskyddsregleringen också uppställer krav på information till den enskilde.[70] Ett sådant förfarande kan underlätta förvaltningens effektivitet samtidigt som det besparar enskilda onödigt arbete med att ta emot underrättelser och granska beslutsunderlag som är gemensamt för förvaltningens olika behov (se även kapitel 8.3.7).

Viktiga aspekter i samband med ett förändringsarbete avseende informationsförsörjning är om avgifter ska tas ut för den information som tillhandahålls och om det ska gälla särskilda krav avseende i vilket format informationen ska tillhandahållas. Det är positivt, även ur ett rättsligt perspektiv, att regeringen genomfört förändringar som innebär att grundläggande information ska kunna utbytas mellan statliga myndigheter utan krav på avgifter. Det återstår emellertid vissa frågor om i vilken utsträckning och på vilket sätt som förvaltningen ska svara för avgiftsfri informationsförsörjning för samhället i stort i form av öppna data. Dessa belyser vi närmare i det följande.

[70] Se t.ex. artikel 13.1e och 13.2e dataskyddsförordningen.

12.2.5 Gällande rätt om att ta del av information i visst format

Allmänna handlingar och utskriftsundantaget i tryckfrihetsförordningen

I tryckfrihetsförordningen regleras rätten att ta del av allmänna handlingar. Som framgått i kapitel 4 syftar regleringen rent allmänt till att främja ett fritt meningsutbyte och en allsidig upplysning. Den har även kommit att fungera som ett viktigt medel för kontroll av offentliga organs verksamhet. Under årens lopp har rätten att ta del av allmänna handlingar emellertid också i betydande utsträckning kommit att ligga till grund för vidareutnyttjande av förvaltningens information för såväl kommersiella som ideella ändamål. Informationen som finns i den offentliga förvaltningen har inte minst ett stort marknadsvärde och är ett viktigt utgångsmaterial för utvecklingen av nya produkter och tjänster, särskilt när den är elektroniskt tillgänglig. Regeringen har även uttalat att möjligheterna att få tillgång till, att bearbeta och att sprida förvaltningens information är centralt för förvaltningens legitimitet och dess demokratiska förankring.[71]

Vem som helst har rätt att ta del av allmänna handlingar med stöd av den angivna bestämmelsen i tryckfrihetsförordningen. Den rätten kan bara begränsas av sekretess och tystnadsplikt. I offentlighets- och sekretesslagen finns både sekretessbestämmelser och bestämmelser som anger när olika typer av sekretess får brytas. I detta sammanhang finns anledning att särskilt nämna att sekretess gäller för personuppgift, om det kan antas att ett utlämnande skulle medföra att uppgiften behandlas i strid med personuppgiftslagen.[72]

Handlingsoffentligheten innebär emellertid inte att en enskild har rätt att få ut handlingar i elektronisk form, utan bara på papper. Det s.k. utskriftsundantaget i 2 kap. 13 § tryckfrihetsförordningen innebär att en myndighet inte är skyldig att lämna ut handlingar i elektronisk form i större utsträckning än vad som följer av lag. Skälet till denna bestämmelse är framför allt skyddet för den enskildes integritet.[73] Det finns endast ett fåtal bestämmelser om skyldighet

[71] *Offentlig förvaltning för demokrati, delaktighet och tillväxt*, prop. 2009/10:175, s. 131.
[72] 21 kap. 7 § offentlighets- och sekretesslagen (ändrad lydelse föreslås fr.o.m. den 25 maj 2018 med anledning av dataskyddsreformen, se prop. 2017/18:105).
[73] *Kungl. Maj:ts proposition med förslag till ändringar i tryckfrihetsförordningen, m.m.*, prop. 1973:33, s. 85 f. och 113 samt *Offentlighetsprincipen och informationstekniken*, prop. 2001/02:70, s. 27 f. Observera även att ändringar i bl.a. 2 kap. tryckfrihetsförordningen föreslås i *Ändrade mediegrundlagar*, prop. 2017/18:49. Ändringarna innebär bl.a. ändrade beteckningar på lagrum.

att lämna ut handlingar i elektronisk form och det saknas generell reglering som anger en sådan skyldighet.[74]

Bestämmelserna i tryckfrihetsförordningen innebär inte ett förbud för myndigheter att tillhandahålla handlingar elektroniskt. Ett elektroniskt tillhandahållande kan dock begränsas bl.a. genom bestämmelser i registerförfattningar. Mot bakgrund av teknikutvecklingen för att skanna in pappersdokument för vidare digital hantering bör det emellertid här framhållas att även utlämnande av pappershandlingar med stöd av bestämmelserna om utlämnande av allmän handling har kommit att i allt större utsträckning ligga till grund för storskaliga digitala vidareutnyttjanden.

Dataskyddsregleringens inverkan på när ett utlämnande är tillåtet eller i vilken form det är tillåtet

Registerförfattningar kan innehålla regler om de ändamål för vilka myndigheten får behandla personuppgifter och i vilken utsträckning uppgifterna får lämnas ut elektroniskt (genom direktåtkomst eller annat elektroniskt utlämnande).[75] Sådana författningar kan även innehålla regler som innebär att myndigheten får tillhandahålla handlingar elektroniskt enbart för vissa ändamål.[76] Dataskyddsregleringen kan därför både ha påverkan på bedömningen av om ett utlämnande alls är tillåtet för ett visst ändamål, och på bedömningen av om det är tillåtet att tillhandahålla handlingar i elektronisk form. Dataskyddsregleringen kan också innehålla begränsningar i det avseendet att förbud för myndigheter att söka och sammanställa uppgifter också inverkar på vilka sammanställningsmöjligheter myndigheten har i förhållande till allmänhet som begär att få ta del av allmänna handlingar.[77]

Här bör nämnas att dataskyddsförordningen också innehåller reglering om i vilken form viss information ska lämnas till den registrerade i fall denne begär att få bekräftelse på om personuppgifter som rör denne behandlas och att få tillgång till personuppgifterna. Om den registrerade gör begäran i elektronisk form ska informationen

[74] T.ex. i 20 kap. 8 § försäkringsrörelselagen (1982:713).
[75] Se t.ex. förslag till 2 kap. 11 § domstolarnas brottsdatalag i SOU 2017:74.
[76] Se t.ex. 7 § lagen (2000:224) om fastighetsregister.
[77] Här avses sökförbud i registerförfattningar jämförda med den s.k. begränsningsregeln i 2 kap. 3 § tredje stycket tryckfrihetsförordningen.

tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat.[78]

Enskildas rätt att kräva att få sin myndighetspost digitalt

Utredningen om effektiv styrning av nationella digitala tjänster har föreslagit en ny reglering om infrastruktur för säkra elektroniska försändelser.[79] Förslaget innebär bl.a. att enskilda och företag ska ha rätt att få försändelser från statliga myndigheter via infrastrukturen för säkra elektroniska försändelser, om det inte finns särskilda skäl för undantag.[80] Vidare har den utredningen föreslagit att det ska vara obligatoriskt för statliga myndigheter att ansluta som avsändare till Mina meddelanden och att skicka myndighetspost digitalt. Regeringen ska dock kunna besluta om att en myndighet ska undantas från kravet. För kommunala myndigheter föreslås inte någon skyldighet, utan det ska även fortsättningsvis vara möjligt för dessa att ansluta till Mina meddelanden på frivillig basis. Dessutom bör infrastrukturen enligt utredningen öppnas upp för privata aktörer som avsändare.[81]

Utredningens förslag analyseras inte närmare i förhållande till vilken typ av postförsändelser som avses. Det framstår emellertid som att förslagen hänför sig till post som relaterar till privatpersonen eller företaget i fråga (dvs. ärenderelaterad post eller post med information till en viss privatperson eller företagare). Det framstår inte som att förslagen avser försändelser med handlingar efter en begäran om utlämnande av allmän handling.

I detta avsnitt belyses inte närmare rätten till partsinsyn, kommunikation enligt förvaltningslagen eller rätten till information om personuppgiftsbehandlingar. Se i stället kapitel 7.6.2 och kapitel 8.[82] Vårt förslag i kapitel 8.3.6 om en ny huvudregel om Digitalt först vid förvaltningens kommunikation med enskilda träffar vidare endast kommunikation som äger rum med den lagen som stöd. Förslaget har alltså inte påverkan på frågan om elektroniskt utlämnande av allmänna handlingar.

[78] Artikel 15.3 dataskyddsförordningen.
[79] *digitalforvaltning.nu* (SOU 2017:23) och SOU 2017:114.
[80] Förslag till 7 § lag om infrastruktur för säkra elektroniska försändelser i SOU 2017:114.
[81] SOU 2017:23 s. 193 f. och s. 296. Se även SOU 2017:114.
[82] Se även artikel 12.1 dataskyddsförordningen.

Övriga krav på myndigheter att tillgängliggöra information – ibland i visst format

Informationsförsörjning är i flera avseenden en central verksamhet i förvaltningen. Vissa myndigheter har, som framgått ovan, till uppdrag att just ge offentlighet åt information. Exempel på myndigheter som har informationsförsörjning som en huvuduppgift är Bolagsverket, Lantmäteriet och Statistiska centralbyrån.[83] I dessa fall är det alltså en central uppgift för myndigheten att se till att viss information finns tillgänglig i samhället, för att riksdag och regering har bedömt att det är ett offentligt åtagande att förse samhället med denna information. I vissa fall regleras inte bara informationsförsörjningen som en uppgift utan också i vilket format myndigheten ska tillhandahålla informationen.[84]

För andra myndigheter, som t.ex. har till huvuduppgift att handlägga vissa ärenden, är den information som inhämtas till eller skapas vid myndigheten snarare att se som en biprodukt från ärendehandläggningen. Även den information som genereras i denna handläggning har förstås ett värde för samhället i övrigt. Det finns emellertid normalt ingen särskild reglering om att dessa myndigheter ska tillhandahålla den information som genereras, och av naturliga skäl därmed inte heller några regler om format för tillhandahållandet.

Vidareutnyttjande av handlingar

Det s.k. PSI-direktivet[85] innehåller en uppsättning minimiregler för vidareutnyttjande av handlingar som finns hos offentliga myndigheter. Direktivet har genomförts i svensk rätt genom PSI-lagen.[86] Syftet med både direktivet och lagen är att främja utvecklingen av en informationsmarknad genom att underlätta enskildas användning av handlingar som tillhandahålls av myndigheter. Reglerna ska säkerställa rättvisa, proportionella och icke-diskriminerande villkor för vidareutnyttjande av handlingar. Huvudprincipen är alltså att upp-

[83] Se t.ex. 1 § lagen (2000:224) om fastighetsregister jämförd med 2 § förordningen (2000:308) om fastighetsregister och 1 § förordningen (2016:822) med instruktion för Statistiska centralbyrån.
[84] Se t.ex. 5 och6 §§ lagen (2010:1767) om geografisk miljöinformation.
[85] Europaparlamentets och rådets direktiv 2003/98/EG om vidareutnyttjande av information från den offentliga sektorn.
[86] Lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen.

rättade handlingar som finns hos myndigheter fritt ska kunna vidareutnyttjas, och att en myndighet inte ska kunna fatta något beslut om att hindra utnyttjandet om det inte finns särskilt stöd för detta.

Med vidareutnyttjande avses enligt lagen användning av handlingar för andra ändamål än det ursprungliga ändamål för vilket handlingarna behandlas av en myndighet. Med begreppet handling avses i lagen i stort sett detsamma som tryckfrihetsförordningens handlingsbegrepp, men varken PSI-direktivet eller lagen omfattar datorprogram.[87] Såväl direktivets som lagens handlingsbegrepp omfattar emellertid både pappershandlingar och handlingar i elektronisk form.

PSI-lagen är tillämplig oavsett vilket eventuellt författningsstöd en myndighet har när den tillhandahåller handlingar. Lagen är alltså tillämplig även när myndigheten lämnar ut handlingar utan att ha en sådan skyldighet enligt någon författning. Däremot kan lagen aldrig åberopas som grund för att få tillgång till handlingar. Med andra ord inverkar inte PSI-lagen på de rättsliga inskränkningar i möjligheten till vidareutnyttjande som finns i annan lagstiftning, bl.a. i sekretessreglering, registerförfattningar och immaterialrättslig reglering.

När PSI-lagen infördes bedömde regeringen att myndigheter, för att öka tillgängligheten och förbättra förutsättningarna för vidareutnyttjande, i så stor utsträckning som möjligt borde göra information tillgänglig i elektronisk form. PSI-direktivets bestämmelser om tillgängliga format behövde emellertid inte regleras i den föreslagna lagen. Befintliga regler ansågs uppfylla direktivets krav.[88]

Sedan den 1 juli 2015 är myndigheter enligt PSI-lagen skyldiga att på sina webbsidor publicera förteckningar över vilka datakällor som de vanligen kan tillhandahålla elektroniskt.[89] Riksarkivet har bemyndigats att meddela närmare föreskrifter om innehållet i och utformningen av den förteckning som ska publiceras.[90] Någon skyldighet för myndigheter att tillhandahålla informationen elektroniskt har dock inte införts.[91] Det finns emellertid en förväntan på

[87] 3 §6 lagen om vidareutnyttjande av handlingar från den offentliga förvaltningen.
[88] Prop. 2009/10:175 s. 158 f.
[89] 11 § andra stycket lagen om vidareutnyttjande av handlingar från den offentliga förvaltningen.
[90] 15 § arkivförordningen (1991:446).
[91] *Vidareutnyttjande av information från den offentliga förvaltningen*, prop. 2014/15:79, s. 23 f.

att tillämpningen av PSI-lagstiftningen ska innebära elektroniska utlämnanden i standardiserade format.[92]

Lagrådet har tidigare framfört att det är svårt att exakt bedöma hur PSI-regleringen förhåller sig till rättssystemet i övrigt, och vilken räckvidd lagens bestämmelser faktiskt har. För att inte den särskilda regleringen i PSI-lagen ska riskera att bidra till osäkerhet i vidare sammanhang har Lagrådet menat att det vore önskvärt att en bredare utvärdering av lagens förhållande till rättsordningen i övrigt kommer till stånd.[93] Även vår kartläggning ger för handen att det förekommer rättslig osäkerhet inom området (se kapitel 5.8.2).

Öppna data

Enligt 2010 års förvaltningspolitiska proposition bör myndigheterna aktivt sträva efter att möjliggöra ett effektivt vidareutnyttjande av offentlig information för att underlätta framväxten av en informationsmarknad och för att bidra till att stärka människors självstyre och utövande av medborgerliga rättigheter.[94]

Med öppna data menas all information som uppfyller kraven för s.k. öppen kunskap, dvs. information som tillhandahålls fritt utan krav på avgifter och med få eller inga tekniska eller rättsliga begränsningar för hur den får användas.[95] I budgetpropositionen för 2016 har regeringen uttalat att myndigheter bör sträva mot öppna data såväl mellan varandra som till enskilda.[96] Regeringen genomför under 2018 en ny satsning på öppna data och datadriven innovation inom den offentliga förvaltningen där tillgängliggörande, matchning och vidareutnyttjande av data ska främjas.[97]

Det finns, utöver den reglering om utlämnande av allmän handling och PSI-lagen som ovan nämnts, inte någon reglering som särskilt handlar om tillhandahållande av öppna data.

---

[92] Artikel 9 i Europaparlamentets och rådets direktiv 2013/37/EU av den 26 juni 2013 om ändring av direktiv 2003/98/EG om vidareutnyttjande av information från den offentliga sektorn.
[93] Se Lagrådets yttrande i prop. 2014/15:79 s. 70 f.
[94] Prop. 2009/10:175 s. 130 f.
[95] E-delegationens betänkande *Så enkelt som möjligt för så många som möjligt – samordning och digital samverkan* (SOU 2013:22) och Digitaliseringskommissionens betänkande *Gör Sverige i framtiden – digital kompetens* (SOU 2015:28), s. 18.
[96] *Budgetpropositionen för 2016*, prop. 2015/16:1, utg. omr. 22 s. 119.
[97] *Budgetpropositionen för 2018,* prop. 2017/18:1, utg. omr. 2 s. 98.

Från den 1 juli 2016 övertog Riksarkivet uppdraget att förvalta och utveckla portalen öppnadata.se. Regeringen har uttalat att till detta bör knytas uppgifter för att främja myndigheters publicering av öppna data.[98] Den 1 september 2018 tar den nya Myndigheten för digital förvaltning över regeringsuppdraget.[99]

12.2.6 Öppna data

Utredningens bedömning: Vid översynen av de författningar som särskilt reglerar åtaganden för förvaltningen att stå för samhällets informationsförsörjning bör överväganden göras om vilka uppgifter som ska tillhandahållas som öppna data. Även för annan information bör det övervägas att tydligare i rättsordningen ange skyldigheter för myndigheter att tillhandahålla uppgifter som öppna data.

Skälen för utredningens bedömning

Kartläggningsresultatet

Några av de aktörer vi haft kontakt med har pekat på en rättslig osäkerhet som rör reglering till grund för att myndigheter ska arbeta med att tillhandahålla öppna data. De rättsliga frågeställningarna är nära sammanvävda med frågeställningar kring myndigheternas prioritering av arbete med att tillgängliggöra öppna data i förhållande till myndighetens verksamhet och uppdrag i övrigt.[100] Den för oss beskrivna osäkerheten rör också hur det säkerställs att informationsmängder som tillgängliggörs som öppna data, framför allt sammantaget med andra digitala källor, inte riskerar att få negativa konsekvenser ur samhälleliga säkerhetsaspekter eller för enskildas integritet. Samtidigt som flera pekat på rättslig osäkerhet i de beskrivna avseendena har andra framhållit att en ökad grad av tillhandahållande av just

[98] Se *Uppdrag till Riksarkivet att främja statliga myndigheters arbete med att tillgängliggöra data för vidareutnyttjande*, Finansdepartementet, 16 juni 2016, dnr Fi/2015/02025/SFÖ, delvis, och Fi2016/01537/SFÖ, delvis).
[99] Inrättande av en myndighet för digitalisering av den offentliga sektorn (dir. 2017:117). Se *Uppdrag med anledning av inrättandet av en myndighet för digitalisering av den offentliga sektorn*, Finansdepartementet, 7 december 2017, Fi2017/04640/DF.
[100] Se även *Den offentliga förvaltningens arbete med att tillgängliggöra offentlig information*, Statskontoret, 9 januari 2018, 2018:2.

öppna data kan vara den viktigaste förändringsfaktorn för inte bara förvaltningens utan också för hela samhällets digitalisering.

Våra överväganden

Inom förvaltningsrätten är legalitetsprincipen av central betydelse. Kravet på författningsstöd för myndigheternas verksamhet är en utgångspunkt såväl när det gäller att handlägga och fatta beslut i ärenden som i fråga om annan verksamhet som en myndighet bedriver. All offentlig verksamhet, oavsett dess karaktär, behöver ytterst grundas på skrivna regler i rättsordningen. Samtidigt som det i enlighet med vad som redogjorts för ovan finns tydliga förväntningar på att myndigheter ska säkerställa att de har stöd i rättsordningen för sina åtgärder, förväntas det emellertid också av myndigheter att de på området för digitalt tillgängliggörande av information ska agera på frivillig basis.[101] Vår kartläggning visar dock att myndigheter bl.a. på grund av otydlighet kring de rättsliga förutsättningarna tvekar i frågor om hur politiska signaler om behovet av att öka det digitala tillgängliggörandet av information kan eller ska omsättas i praktiken. Det kan också vara svårt för myndigheter som inte ser egen verksamhetsnytta att prioritera arbete med öppna data, om detta inte krävs av myndigheterna t.ex. enligt författning.

När det gäller myndigheters åliggande att tillgängliggöra viss information finns det en historisk kontext i fråga om grunddata. Inom det området har staten tidigare tagit ställning till vilken information som också ska tillhandahållas för privata aktörer som i sin tur kunnat ta fram nya lösningar, t.ex. vad gäller folkbokföringsadresser och de digitala lösningar som nu finns för att hitta sådana kontaktuppgifter på nätet. Under kartläggningen har vi hört det nämnas att ett paradigmskifte nu förefaller äga rum där ytterligare spridning av förvaltningens information som öppna data för vidareutnyttjande uppskattas på den politiska nivån, men där den juridiska kartbilden och tankesättet hos dem som ska hantera frågorna på praktisk nivå inte hänger med.

Till skillnad från elektroniska utlämnanden av allmän handling kräver myndigheters tillgängliggörande av öppna data inte någon

[101] Se bl.a. regeringens uttalanden i prop. 2009/10:175 och prop. 2015/16:1, utg. omr. 22 s. 119.

begäran om att en viss informationsmängd ska lämnas ut eller tillgängliggöras. I stället förutsätts att öppna data görs tillgängliga oberoende av om de tidigare har efterfrågats av någon aktör. Samtidigt behöver det finnas intresse av tillgängliggörandet för att utvecklingsarbeten om tillhandahållande av öppna data ska komma till nytta. I nuläget gör myndigheter på eget initiativ bedömningar av om några informationsmängder ska publiceras som öppna data. Det tillgängliggörandet synes också förhålla sig helt fritt till frågan om uppgiftsmängden sedan tidigare är att anse som en allmän handling eller blir det när den tillgängliggörs. Till exempel kan det vara fråga om andra typer av uppgifter än färdiga elektroniska handlingar som kan vara intressanta att tillhandahålla som öppna data. Det kan också vara fråga om andra uppgifter än sådana som finns i ett beslutsunderlag, t.ex. statistikuppgifter eller andra uppgifter som genererats vid ärendehandläggningen men som inte utgör personuppgifter för att de är anonymiserade. Det har också beskrivits för oss att det för flera datamängder som inte kan lämnas ut digitalt i sitt befintliga skick på grund av sekretess eller för att de innehåller personuppgifter, som t.ex. kan behöva anonymiseras för att de ska kunna tillhandahållas som öppna data. Frågan är i vilken utsträckning myndigheterna ska prioritera sådant arbete?

Som framgått är vidare bl.a. formatfrågan av central betydelse när uppgiftsmängder tillgängliggörs som öppna data. Att myndigheter möter högt ställda förväntningar i fråga om format i samband med tillgängliggörande av öppna data går därmed utöver de krav som i dag finns reglerade i svensk lagstiftning, t.ex. i PSI-lagen.

Mot bakgrund av vad som ovan kort skisserats, och med beaktande av vad som framkommit i kartläggningen, bedömer vi att den beskrivna osäkerheten synes hämma myndigheter från att öka tillgängliggörandet av sina informationsmängder som öppna data. Det gäller delvis frågan om myndigheter utan särskilt åliggande ska eller bör prioritera utvecklingsarbete som gäller tillhandahållande av öppna data. Det gäller emellertid också frågan om vilket rättsligt stöd som bör finnas om förvaltningen nu och på sikt förväntas öka sitt bidrag till att försörja samhället med digital information i form av öppna data.

Ytterst kan förstås tillgängliggörande av myndigheters information som öppna data sägas handla om att ge offentlig insyn i förvaltningens

verksamhet, till gagn för demokratisk förankring. I allt större utsträckning förväntar sig också allmänheten att information ska finnas tillgänglig digitalt. Öppna data kommer enligt vår uppfattning att bidra till att förvaltningen nu och i framtiden både förmår vara och kan visas vara transparent.

Det finns emellertid även ett starkt inslag av närmast politiska överväganden om vilket åtagande myndigheterna ska ha att försörja samhället i stort med information för vidareutnyttjande. Intresset av att också myndigheter kan ta del av information från andra myndigheter som öppna data ska dock inte heller underskattas. I detta sammanhang behöver också beaktas vad som framkommit under kartläggningen om att myndighetsrepresentanter ser svårigheter med att, för varje myndighets enskilda informationsmängder, göra sammantagna bedömningar av om den information som förvaltningen som helhet tillgängliggör som öppna data kan leda till negativa konsekvenser ur ett säkerhetsperspektiv eller i förhållande till enskildas integritet.

Vi ser därför behov av fortsatta överväganden i frågan om befintliga rättsregler ger tillräcklig styrning och stöd för att myndigheter på frivillig basis ska tillgängliggöra öppna data i den utsträckning som synes vara politiskt önskvärt, eller om kompletterande reglering krävs eller vore önskvärd för att ge såväl handlingsdirektiv som legalt stöd för tillgängliggörande av öppna data. I samband med sådana fortsatta överväganden behöver även säkerhetsaspekter och integritetsskydd, avseende såväl persondataskydd som sekretess, beaktas.

I de arbeten som framgent kommer att göras med att se över författningar som särskilt reglerar åtaganden för förvaltningen att stå för samhällets informationsförsörjning (se kapitel 12.2.4), bör överväganden om vilka uppgifter som ska tillhandahållas som öppna data också göras. Även för annan information bör det emellertid övervägas att tydligare i rättsordningen ange skyldigheter för myndigheter att tillhandahålla uppgifter som öppna data. Frågan om rättslig reglering rörande öppna data behöver enligt vår uppfattning inte sammanblandas med reglering som avser elektroniskt utlämnande av allmän handling (se avsnitt 12.2.7), det vore möjligt att tydligare separera frågorna.

12.2.7 Elektroniskt utlämnande av allmän handling

Utredningens bedömning: Frågan om skyldighet för myndigheter att lämna ut allmänna handlingar i elektronisk form bör övervägas i samma sammanhang som det säkerställs att myndigheterna för sådant utlämnande kan ta ut avgifter.

Skälen för utredningens bedömning

E-offentlighetskommitténs överväganden och förslag

Under åren 2008–2010 hade E-offentlighetskommittén i uppdrag att göra en översyn av vissa av bestämmelserna i 2 kap. tryckfrihetsförordningen.[102] I uppdraget ingick bl.a. att överväga om det borde införas en skyldighet för myndigheter i vanlig lag, dvs. inte i grundlag, att lämna ut elektroniskt lagrade allmänna handlingar i elektronisk form.

Kommittén betraktade ett utökat elektroniskt utlämnande som en del i strävan mot en stärkt offentlighetsprincip och menade att utgångspunkten borde vara att så långt som möjligt hitta former för detta. Samtidigt skulle dock en möjlighet att kräva ett elektroniskt utlämnande av allmänna handlingar med stöd av lag kunna innebära ökad risk för intrång i enskildas personliga integritet. En lämplig balans borde enligt kommittén råda mellan dessa båda i viss mening motstående intressen. För att en ordning med en generell skyldighet att lämna ut allmänna handlingar i elektronisk form skulle kunna förordas måste fördelarna från offentlighetssynpunkt överväga nackdelarna. Utöver inverkan på skyddet för den personliga integriteten i samband med utlämnande av allmänna handlingar borde enligt kommitténs bedömning även vissa ytterligare tänkbara konsekvenser beaktas, till exempel samhälleliga säkerhetsaspekter på utökade möjligheter att få ut allmänna handlingar i elektronisk form.

Kommittén bedömde att det dåvarande regelverket till skydd för den personliga integriteten i samband med utlämnande av allmänna handlingar inte säkerställde en godtagbar skyddsnivå i fråga om intrång i enskildas personliga integritet, vilket medförde att en

[102] *Allmänna handlingar i elektronisk form – offentlighet och integritet* (SOU 2010:4).

generell skyldighet i lag att lämna ut allmänna handlingar i elektronisk form inte kunde föreslås. Den främsta orsaken till detta ansågs vara de brister som i detta avseende fanns i registerförfattningarnas reglering. Det långsiktiga målet borde emellertid enligt kommittén vara att myndigheterna skulle ha en i lag reglerad skyldighet att, i den mån det inte finns särskilda förbud mot det i lag eller förordning, lämna ut allmänna handlingar i elektronisk form om sökanden så önskar. En sådan reglering kunde dock enligt kommittén inte införas förrän en grundlig genomgång och bearbetning hade genomförts av samtliga registerförfattningar. Under mellantiden föreslog kommittén att det borde föreskrivas i lag att en myndighet ska lämna ut elektroniskt lagrade allmänna handlingar i elektronisk form om det inte är olämpligt. Kommittén föreslog därför att det skulle föras in i en ny bestämmelse i 6 kap. offentlighets- och sekretesslagen med följande lydelse.

> En myndighet ska på begäran av en enskild lämna ut en handling som förvaras elektroniskt hos myndigheten i elektronisk form, om den inte innehåller sekretessbelagda uppgifter, det i lag eller förordning finns bestämmelser som förbjuder det eller det annars är olämpligt.

Lämplighetsbedömningen skulle enligt kommittén framför allt ta sikte på integritetsskyddsaspekter, men utöver integritetsskyddsaspekter framförde kommittén att det kunde finnas andra faktorer som talade mot att lämna ut den allmänna handlingen i elektronisk form. Det kunde röra sig om säkerhetsaspekter eller tekniska och praktiska faktorer som talar mot ett elektroniskt utlämnande i det specifika fallet.

Kommitténs förslag innebar sammanfattningsvis att rätten att efter en lämplighetsbedömning få ut elektroniska handlingar i elektronisk form skulle komplettera den grundlagsfästa rätten att få ut allmänna handlingar i pappersform. Myndigheterna (såväl statliga som kommunala) skulle med andra ord enligt lag bli skyldiga att i samtliga fall ta ställning till en begäran när elektroniskt utlämnande begärs av elektroniskt lagrade allmänna handlingar.

Något förenklat menade kommittén vidare att det kunde sägas finnas tre områden där begränsningar av myndighetens skyldigheter avseende utlämnandet av handlingar förekommer, nämligen begränsningar av tillåtna sökbegrepp i registerförfattningar i kombination med den s.k. begränsningsregeln i 2 kap. 3 § tryckfrihetsförordningen,

sekretessbestämmelsen i 21 kap. 7 § offentlighets- och sekretesslagen med dess koppling till personuppgiftslagen (1998:204) samt utskriftsundantaget i 2 kap. 13 § tryckfrihetsförordningen och utlämnandebestämmelser i registerförfattningar.

Kommittén undersökte bl.a. vad effekterna skulle bli av att helt avskaffa sekretessregeln i 21 kap. 7 § offentlighets- och sekretesslagen. Givet att det inte skulle införas en lagstadgad generell skyldighet att lämna ut handlingar i elektronisk form bedömde kommittén å ena sidan att det i flertalet fall skulle vara möjligt att upprätthålla ett adekvat skydd för enskildas personliga integritet även utan den aktuella sekretessbestämmelsen. Det stod å andra sidan enligt kommitténs uppfattning klart att bestämmelsen faktiskt fyller en viss, låt vara begränsad, funktion och att den därmed bidrar till att upprätthålla skyddet för den personliga integriteten. Om sekretessbestämmelsen i 21 kap. 7 § offentlighets- och sekretesslagen inte längre skulle gälla kunde t.ex. massuttag av personuppgifter i pappersform aldrig stoppas om inte någon annan sekretessbestämmelse var tillämplig. Kommitténs slutsats blev att det då inte var lämpligt att avskaffa den nämnda sekretessbestämmelsen. Emellertid fanns det enligt kommitténs bedömning anledning att på nytt överväga behovet av sekretessbestämmelsen efter att den genomgång av registerförfattningarna som kommittén förespråkade hade genomförts.

Frågan om det borde införas en tydligare reglering beträffande avgifter för elektroniska kopior övervägdes också av E-offentlighetskommittén.[103] Kommittén ansåg att en tydligare reglering vore önskvärd, bl.a. eftersom det då för allmänheten skulle framgå i vilka situationer myndigheten har rätt att ta betalt för en elektronisk kopia av en allmän handling. Samtidigt ansåg man att det finns klara nackdelar med en ordning där myndigheten som huvudregel är ålagd att ta ut en avgift för en kopia av en allmän handling. Kommittén gjorde bedömningen att den flexibilitet som den befintliga regleringen ger är värdefull, bl.a. eftersom allt tyder på att det ofta är samhällsekonomiskt kontraproduktivt att ta betalt för enstaka, normalstora uttag av allmänna handlingar i elektronisk form. Ytterligare en faktor som utredningen framhöll var att det ofta torde möta svårigheter att på ett mer detaljerat sätt reglera avgiftsuttaget vid utlämnande av allmänna handlingar i elektronisk form. Handlingens storlek har ju i digital miljö inget direkt samband med eventuella

[103] A.a., s. 354 f.

kostnader för utlämnandet utan det som i realiteten ska prissättas är sådan arbetstid som måste läggas ned vid mer omfattande beställningar. Kommittén var därför tveksam till om detta skulle låta sig regleras på ett sätt som verkligen skulle ge en större tydlighet och förutsebarhet. Som kommittén såg det fanns det goda skäl att hävda att redan med den nuvarande regleringen i avgiftsförordningen kunde man erbjuda en ordning där det råder en rimlig balans mellan möjligheterna för allmänheten att förutse den ungefärliga kostnaden för ett uttag av en allmän handling i elektronisk form och behovet av att kunna tillgodose en flexibilitet i avgiftsuttaget. Kommittén ansåg dessutom att en tydligare reglering väcker ett antal frågor om avgiftssättning generellt sett som kommittén inte hade underlag att bedöma. Kommittén lade därför inte fram några förslag beträffande avgiftsuttag vid utlämnande av allmänna handlingar.

Våra överväganden

Under kartläggningen, och även under utredningens gång i andra sammanhang, har vi mötts av synpunkterna att frågan om förutsättningarna för förvaltningen att lämna ut allmänna handlingar i elektronisk form behöver få en lösning, inte minst mot bakgrund av allmänhetens allt ökade förväntningar på att få ta del av allmänna handlingar digitalt i stället för på papper. Samtidigt har vi också hört uppfattningen att den insyn i enskildas förehavanden som andra enskilda ges genom att med stöd av offentlighetsprincipen ta del av allmänna handlingar i elektronisk form kan uppfattas vara särskilt integritetskränkande.

Den tidigare inriktningen att registerförfattningarna borde gås igenom i syfte att, för respektive tillämpningsområde, se över frågan om vilken form för utlämnande av personuppgifter som borde tillåtas eller förbjudas har trots att flera år förflutit inte framskridit på det sätt som kan ha varit bl.a. E-offentlighetskommitténs avsikt. Inte heller vid den översyn av samtliga registerförfattningar som nu föranletts av dataskyddsreformen har den typen av frågor stått i fokus.

Parallellt med att det synes vara svårframkomligt att göra de efterfrågade översynerna av registerförfattningarna i fråga om elek-

troniskt utlämnande av allmänna handlingar som innehåller personuppgifter har även finansieringsfrågor bromsat utvecklingen vad gäller den formen för utlämnande.

En departementspromemoria om frekventa och omfattande ärenden om utlämnande av allmän handling har nyligen remitterats.[104] Några av de frågor som diskuterats med oss under kartläggningen behandlas där. Bland annat föreslås att myndigheter ska ges möjlighet att, om det i det enskilda fallet finns särskilda skäl, kräva att en sökande betalar avgift eller del av den beräknade avgiften i förskott i ärenden om utlämnande av kopior av allmänna handlingar. Promemorian behandlar dock inte frågan om enhetliga regler om avgiftsuttag för elektroniska kopior utan stannar vid att den frågan bör övervägas på nytt i samband med att avgiftsförordningen ses över.

Frågan om skyldigheter för myndigheter att lämna ut allmänna handlingar i elektronisk form bör enligt vår uppfattning övervägas i samma sammanhang som det säkerställs att myndigheterna för sådant utlämnande kan ta ut avgifter. Avgiftsuttaget vid sådant elektroniskt utlämnande borde också ses över så att det blir enhetligt.[105]

Även utan en genomgripande reformering av registerförfattningarna borde det på nytt i det sammanhanget kunna övervägas att genomföra E-offentlighetskommitténs förslag att i offentlighets- och sekretesslagen föreskriva att en myndighet ska lämna ut elektroniskt lagrade allmänna handlingar i elektronisk form om det inte är olämpligt, t.ex. på grund av säkerhetsskäl eller av integritetsskäl. Jämförelser kan också göras med förslaget om att elektroniskt utlämnande ska tillåtas i större utsträckning i *Brottsdatalag – kompletterande lagstiftning.* Där föreslås att det införs i registerförfattningarna under direktivet att personuppgifter får lämnas ut elektroniskt om det inte är olämpligt.[106]

Det kan här tilläggas att en övergång från att förvaltningen på traditionellt sätt svarar på begäran om utlämnande av allmän handling till att i stället i ökande omfattning tillhandahålla exempelvis avidentifierade eller helt anonymiserade uppgifter digitalt, t.ex. i form av öppna data (se ovan) också kan gagna öppenheten i den digitala förvaltningen utan att integritetsintressen träds för när.[107]

---

[104] *Frekventa och omfattande ärenden om utlämnande av allmän handling* (Ds 2017:37).
[105] Se bl.a. *Behov av ändringar i avgiftsförordningen*, Domstolsverket, 24 juni 2014, Fi2014/03027.
[106] SOU 2017:74 s. 371 f.
[107] Jfr det offentliga rättsinformationssystemet som regleras i rättsinformationsförordningen (1999:175).

12.2.8 Tryckfrihetsförordningen och myndighetssamverkan

Utredningens bedömning: Det bör övervägas att anpassa regleringen om allmän handling i tryckfrihetsförordningen till det förhållandet att mellanprodukter och arbetsmaterial inte längre tas fram enbart inom en verksamhets organisatoriska gränser, när digitala utvecklingsarbeten i samverkan mellan myndigheter i allt högre grad efterfrågas.

Skälen för utredningens bedömning: Som framgått i kapitel 6.2 krävs en påfallande grad av enhetlighet i såväl tolkning och tillämpning av gällande rätt, anknytande begreppsanvändning, arbetssätt och tekniska lösningar när myndigheter bedriver digitala utvecklingsarbeten i samverkan med varandra. Det sagda gäller oavsett om det rör sig om särskilda samverkansuppdrag, exempelvis när nya verksamhetsområden inom den digitala förvaltningens åtagande ska utvecklas, eller enbart mindre anpassningar i myndigheternas respektive verksamhet genom övergång till digitala lösningar. Samtidigt som det ställs nya och ökade krav på myndigheterna att samverka i utvecklingsarbeten utgår emellertid regleringen om allmänna handlingars offentlighet fortfarande från myndigheternas traditionella gränser.

Av tryckfrihetsförordningen följer att en handling är allmän om den förvaras hos myndigheten och är att anse som inkommen till eller upprättad hos myndigheten.[108] En handling anses inkommen till myndighet, när den har anlänt till myndigheten eller kommit behörig befattningshavare till handa.[109] För diarier, journaler och sådana register eller andra förteckningar som förs löpande gäller att de anses upprättade redan när de har färdigställts för anteckning eller införing.[110]

Ett utkast eller koncept till en myndighets beslut eller skrivelse och annan därmed jämställd handling som inte har expedierats ska emellertid inte anses som allmän handling, om den inte tas om hand för arkivering.[111] Av förarbetsuttalanden framgår att med mellan-

[108] 2 kap. 3 § tryckfrihetsförordningen.
[109] 2 kap. 6 § första stycket tryckfrihetsförordningen.
[110] 2 kap. 7 § andra stycket 1 tryckfrihetsförordningen.
[111] 2 kap. 9 § andra stycket tryckfrihetsförordningen.

produkter avses handlingar som befinner sig på ett tidigare framställningsstadium än den slutliga produkten. Om en handling till följd av bestämmelserna i andra stycket inte ska anses som allmän hos den myndighet som framställt den är den således inte heller allmän hos en myndighet som har tagit emot den för preliminär granskning.[112] Bestämmelsen tar alltså sikte på handlingar som är avsedda att omarbetas, även i den situationen att konsultation sker med andra myndigheter. I praxis och doktrin har däremot ett skriftligt svar på en sådan utsänd underhandsremiss ansetts utgöra allmän handling.[113]

Den sistnämnda bedömningen om att skriftliga svar på utsända underhandsremisser utgör allmän handling leder till en påtaglig tvekan hos flera myndigheter att dela med sig av ofärdiga produkter, trots att det är absolut nödvändigt för att komma vidare i ett myndighetsgemensamt utvecklingsarbete. Den tvekan som myndigheterna ger uttryck för i kartläggningsarbetet baseras inte på ovilja att ge insyn i hur utvecklingsarbetet bedrivs, utan snarare att det kan leda till betydande missförstånd om ofärdiga arbetsutkast kommer till spridning i skeden där den fortsatta inriktningen för utvecklingsarbetet i fråga ännu inte är bestämd.

Vårt kartläggningsarbete ger för handen att den nu aktuella rättsliga frågeställningen i praktiken både kan förhindra och försvåra myndighetsgemensamma utvecklingsarbeten. Samtidigt förefaller det snarare vara praxisutvecklingen än ordalydelsen i tryckfrihetsförordningen som har lett till vad som enligt oss kan sägas vara en onödigt försvårande omständighet vid myndighetssamverkan.

I dagens tekniska miljöer är det inte heller alltid fråga om att en myndighet som önskar en annan myndighets synpunkter på en mellanprodukt rent tekniskt skickar utkastet för synpunkter. Inte sällan äger ”digitala delningar” rum i miljöer som t.ex. via tjänsterna Dropbox, Projectplace eller Google Docs. Det rör sig ibland om regelrätta delningar för att inhämta synpunkter från den andra myndigheten, ibland snarare om samarbete där myndigheter gemensamt och i viss utsträckning samtidigt arbetar fram dokument som är nödvändiga för ett utvecklingsarbete.

[112] *Regeringens proposition om nya grundlagsbestämmelser angående allmän handlings offentlighet*, prop. 1975/76:160 s. 169 f.
[113] Se t.ex. RÅ 1999 ref. 36 och Kammarrätten i Göteborgs dom den 12 juni 2017 i mål nr 492-17. Se även Alf Bohlin, *Offentlighetsprincipen*, 9:e uppl., Norstedt Juridik, s. 96 f.

Utan att här nå någon lösning på den aktuella frågeställningen vill vi uppmärksamma att de allt ökande kraven på myndighetssamverkan leder till att avsevärd tid läggs på att rättsligt utreda om eller hur samverkan rent praktiskt ska gå till, bl.a. för att det inte under utvecklingsarbetets gång ska uppstå betydande missförstånd om ofärdiga arbetsutkast kommer till allmän spridning. Vi instämmer alltså i de önskemål som framförts under kartläggningen om att det bör övervägas att anpassa regleringen om allmän handling i tryckfrihetsförordningen till det förhållandet att mellanprodukter och arbetsmaterial inte längre enbart tas fram inom en myndighets organisatoriska gränser, när samverkan mellan myndigheter i allt högre grad efterfrågas. Det förefaller vara lämpligare att angripa frågan om vad som i dessa sammanhang alls ska anses utgöra en allmän handling än att möta de allt ökande kraven på myndighetssamverkan i utvecklingsarbeten med t.ex. nya sekretessbestämmelser.

12.2.9 Språklagen

Utredningens bedömning: Det kan övervägas att i annat sammanhang återkomma till frågan om vilket eller vilka språk myndigheter bör eller får använda i digitala tjänster.

Skälen för utredningens bedömning: Som framgått i kapitel 5.2.5 har vi under kartläggningen uppmärksammats på frågor om vilket eller vilka språk myndigheter bör eller får använda i digitala tjänster. Enligt 10 § språklagen (2009:600) är språket svenska i domstolar, förvaltningsmyndigheter och andra organ som fullgör uppgifter i offentlig verksamhet. I annan lag finns särskilda bestämmelser om rätt att använda nationella minoritetsspråk och annat nordiskt språk.[114]

Internationella, främst EU-rättsliga, krav på gränsöverskridande informationsutbyten och för unionen gemensamma portaler som

[114] Här avses rätten att inom vissa förvaltningsområden använda samiska, finska och meänkieli (enligt lagen [1999:1175] om rätt att använda samiska hos förvaltningsmyndigheter och domstolar och lagen [1999:1176] om rätt att använda finska och meänkieli hos förvaltningsmyndigheter och domstolar) och rätten att i vissa ärenden inom det sociala området och inom hälso- och sjukvård använda de språk som talas i våra nordiska grannländer (enligt lagen [1995:479] om nordisk konvention om socialt bistånd och sociala tjänster).

ingång för vissa tjänster gentemot privatpersoner och företag ställer emellertid särskilda krav. Det finns enligt vår bedömning anledning att vara uppmärksam på utvecklingen av EU-rättsliga krav och hur dessa förhåller sig till språklagen, och om det framöver uppkommer någon situation när svenska myndigheter riskerar att behöva åsidosätta språklagen för att fullgöra åligganden enligt unionsrätten. Något konkret exempel på en klar konflikt mellan språklagen och unionsrätten har dock inte uppmärksammats under kartläggningen, varför den beskrivna problematiken inte ger anledning att nu närmare överväga anpassningar i språklagen i syfte att främja förvaltningens digitalisering.

Det finns emellertid även andra skäl att överväga hur regleringen kring språk, tolkning och översättning förhåller sig till digitaliseringen inom offentlig förvaltning. En allt mer ökad användning av digitala tjänster innebär att myndigheters stöd till enskilda i flera avseenden lämnas i ett tidigt skede i processen. Det äger med andra ord rum en förskjutning, som innebär att stöd och service i högre grad lämnas redan innan ett ärende i förvaltningslagens mening har hunnit inledas vid myndigheten (se vidare bl.a. kapitel 8 om inledandet av ett ärende i förvaltningslagens mening). Att tillhandahålla en sådan service redan innan ett ärende inleds skapar förutsättningar för underlag av god kvalitet, och möjliggör därigenom bl.a. fortsatt automatiserad handläggning av ärendet (se vidare kapitel 7 om automation). Förvaltningslagen[115] uppställer emellertid allmänna krav på tolkning respektive översättning av handlingar först om det under handläggningen av ett ärende behövs för att den enskilde ska kunna ta till vara sin rätt när myndigheten har kontakt med någon som inte behärskar svenska.

Det är viktigt att allmänheten har fortsatt tillit till den digitala förvaltningen. Digitala tjänster behöver också vara ändamålsenliga. Med detta i beaktande skulle det kunna finnas anledning att närmare analysera behov av förändringar avseende i vilket skede allmänna förvaltningsrättsliga krav på tolkning och översättning bör inträda, dvs. om kraven borde inträda tidigare i processen. Ett annat alternativ vore att närmare analysera om 10 § språklagen skulle behöva anpassas för att i vart fall säkerställa myndigheters valfrihet att erbjuda digitala tjänster som redan i serviceskedet, innan ett ärende inleds, finns tillgängliga exempelvis på andra språk än svenska.

[115] 13 § förvaltningslagen (2017:900).

Frågan ligger emellertid inte närmast den inriktning som vårt uppdrag har. Vi har därför inte prioriterat att ytterligare analysera denna fråga, men ser att regeringen skulle kunna överväga att i annat sammanhang återkomma till frågeställningen.

13 Rapportering av arbete med it och digitalisering

13.1 Bättre underlag för bättre styrning

Det övergripande målet för regeringens it-politik är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.[1] Under de senaste åren har emellertid internationella mätningar indikerat att Sverige tappar placeringar när det gäller den offentliga sektorns digitalisering.[2] Även om mätningar av detta slag ska tolkas med viss försiktighet beskrivs bilden på ett likartat sätt och pekar till stor del på samma problemområden. Digitaliseringen i Sverige går långsammare i offentlig sektor än i näringslivet och samtidigt utvecklas Sveriges offentliga sektor i detta hänseende sakta ur ett EU-perspektiv.

Som beskrivits i kapitel 7.2.4 ger digital informationshantering i förvaltningen nya möjligheter till analys, kunskap och underlag för styrning. En digital förvaltning ska också utöva den ändamålsenliga och kostnadseffektiva verksamhet som förväntas, parallellt med att förvaltningen främjar digitala förfaranden som möjliggör nya former för service och tjänster till privatpersoner och företag. Det krävs en god kontroll över de kostnader som digitaliseringen för med sig och en styrning mot digitalisering av de förfaranden där störst mervärde kan skapas.

It utgör en betydande kostnad för staten som helhet. Enligt Ekonomistyrningsverkets uppskattning för år 2016 låg de samlade it-kostnaderna för statsförvaltningen på mellan 25 och 30 miljarder

[1] *Budgetpropositionen för 2012*, prop. 2011/12:1, utg. omr. 22 avsnitt 4.
[2] Se t.ex. *eGovernment Benchmark 2016 – A turning point for eGovernment development in Europe?*, Europeiska kommissionen, 2016 och *The Global Information Technology Report 2016*, World Economic Forum, 2016.

kronor per år och utgjorde ungefär nio procent av myndigheternas verksamhetskostnader.[3] It-kostnader är därmed det andra största utgiftsslaget i statsförvaltningens verksamhetskostnader. För kommuner, landsting och regioner saknas motsvarande uppgifter om it-kostnadernas storlek. Det har emellertid nämnts att uppskattningsvis 45 miljarder kronor läggs på it årligen i myndigheter, kommuner och landsting.[4]

Det är svårt, både för riksdagen, regeringen, myndighetsledningar och andra aktörer t.ex. Riksrevisionen och Statskontoret, att bedöma om it används effektivt. Ett skäl till detta är att det inte finns några generella system eller processer som fångar it-kostnader eller uppgifter om myndigheternas it-verksamhet vilket kan leda till bristande styrnings- och kostnadskontroll. Det kan också försvåra styrning mot en effektiv it-användning och digitalisering i förvaltningen som har potential att skapa de största mervärdena.

I syfte att skapa god uppföljning och styrning är det angeläget att såväl riksdagen och regeringen som andra aktörer i förvaltningen och även allmänheten kan få en god bild av den offentliga sektorns användning av, och kostnader för, it och digitalisering. En förbättrad uppföljning har potential att öka transparensen och skapa förutsättningar för bättre styrning och samordning av den offentliga förvaltningens digitala utveckling. Förbättrad uppföljning kan tydliggöra var digitaliseringen kan bidra till ytterligare effektivisering och mervärden för enskilda i den offentliga förvaltningen. Förbättrad uppföljning kan också öka den digitala mognaden och kompetensen inom den offentliga förvaltningen.

13.2 Befintlig rapportering av it och digitalisering

I dagsläget saknas möjlighet för bl.a. regeringen att på ett samlat sätt följa hela den offentliga förvaltningens arbete med, och kostnader för, it och digitalisering. Till viss del sker obligatorisk rapportering, för statliga myndigheter, i årsredovisningar och redovisningssystem

[3] *Myndigheters strategiska it-projekt och it-kostnader, Delrapport it-användningsuppdraget,* Ekonomistyrningsverket, 21 december 2017, P-2017-77.
[4] Se presentation på e-legitimationsdagen 2018 på https://elegnamnden.se/download/18.769a0b711614b669f29c3/1517927834469/Ardalan_Shekarabi-Digitalt_forst-nu_okar_vi_takten_i_det_offentliga_Sverige.pdf

(Hermes). Men uppgifterna som lämnas är inte alltid i standardiserade format och det samlade underlaget är inte tillräckligt detaljerat för att mer ingående kunna följa upp och styra den digitala utvecklingen i statsförvaltningen.

Nedan redogörs för ett par av de etablerade kanaler och pågående initiativ som i dag finns på plats för den offentliga förvaltningens, frivilliga eller obligatoriska, redovisning av uppgifter som helt eller delvis rör förvaltningens löpande arbete med, och kostnader för, it och digitalisering.

Årsredovisningar

För statliga myndigheter, kommuner och landsting gäller att de ska hushålla väl med ekonomiska medel i sin verksamhet.[5] Statliga myndigheter lämnar årligen årsredovisning och budgetunderlag till regeringen. Handlingarna utgör underlag för regeringens uppföljning, prövning eller budgetering av myndighetens verksamhet.[6] För kommuner och landsting är det kommun- respektive landstingsstyrelsen som ansvarar för att upprätta årsredovisning.[7] Årsredovisningen lämnas till fullmäktige.[8]

Ekonomistyrningsverket (ESV) har i en förstudie undersökt möjligheterna att effektivisera och digitalisera statliga myndigheters inlämning av årsredovisningar. Målsättningen är att statliga myndigheter ska lämna in årsredovisningar i ett digitalt, maskinläsbart, format till en enda inlämningspunkt. Digitaliserad inlämning av årsredovisning kan underlätta för Regeringskansliet att göra systematiska analyser av informationen i myndigheternas årsredovisningar.[9]

[5] 1 kap. 3 § budgetlagen (2011:203), 3 § myndighetsförordningen (2007:515) och 11 kap. 1 § kommunallagen (2017:725).
[6] 1 kap. 3 § förordningen (2000:605) om årsredovisning och budgetunderlag.
[7] 3 kap. 4 § lagen (1997:614) om kommunal redovisning.
[8] 11 kap. 20 § kommunallagen.
[9] *Digitaliserad årsredovisning – en förstudie*, Ekonomistyrningsverket, 20 december 2017, ESV 2017:76.

Hermes

Hermes är ett gemensamt informationssystem för Regeringskansliet och myndigheterna i den statliga redovisningsorganisationen. Systemet ger stöd i arbetet med statens budget och i uppföljningen av statens ekonomi och verksamhet. Vissa delar av it-kostnaderna i statsförvaltningen kan följas upp genom statliga inrapporteringskoder, s.k. S-koder, som används i Hermes. Genom S-koder rapporteras bl.a. köp av datatjänster från annan statlig myndighet eller från annan utomstående aktör.

Fördjupat it-kostnadsuppdrag och ramverk för it-kostnader

ESV har i uppdrag att utveckla och förvalta den ekonomiska styrningen av den statliga verksamheten. ESV har en författningsreglerad rätt att från andra statliga myndigheter få den information som myndigheten behöver för sin verksamhet.[10]

På uppdrag av regeringen har ESV utarbetat förslag till hur mätning och rapportering av de statliga myndigheternas it-användning kan utvecklas och hur statsförvaltningens digitalisering kan följas upp.[11] I arbetet har ESV identifierat ett antal nyckeltal som bl.a. kan användas som underlag för uppföljning av it-kostnader.[12] ESV har inom ramen för uppdraget redovisat tre rapporter.[13]

ESV har därtill ett pågående regeringsuppdrag där verket, tillsammans med ett antal myndigheter, undersöker möjligheten att använda ett gemensamt och internationellt accepterat ramverk bl.a. för att kunna göra jämförelser av it-kostnader och kundnöjdhet samt för att ta tillvara digitaliseringens möjligheter.[14] Uppdraget genomförs som ett pilotprojekt, där ett antal utvalda myndigheter redovisar

[10] 30 § förordningen (2010:1764) med instruktion för Ekonomistyrningsverket.
[11] *Uppdrag att fördjupa arbetet med jämförelser av it-kostnader och att kartlägga it-projekt med hög risk*, regeringsbeslut den 15 januari 2015, N2015/738/EF.
[12] Se även *It-kostnadsmodell, Ett första steg mot ett gemensamt språk,* Ekonomistyrningsverket, 1 oktober 2014, 2014:50.
[13] *Fördjupat it-kostnadsuppdrag, delrapport 1: Kartläggning av strategiska it-projekt med hög risk* Ekonomistyrningsverket, 3 mars 2015, 2015:48, *Fördjupat it-kostnadsuppdrag, delrapport 2: Kartläggning av it-kostnader*, Ekonomistyrningsverket, 23 oktober 2015, ESV 2015:58 och *Fördjupat it-kostnadsuppdrag, slutrapport: Förslag inför framtiden*, Ekonomistyrningsverket, 23 december 2015, ESV 2015:64.
[14] Ekonomistyrningsverkets regleringsbrev 2018, Fi2017/04757/RS.

it-kostnader med stöd av ramverket Technology Business Management (TBM). ESV har hittills levererat en delrapport inom ramen för uppdraget.[15]

eBlomlådan

eBlomlådan är ett verktyg för utvärdering av digital service och verksamhetsutveckling i kommuner. Med hjälp av eBlomlådan kan kommuner identifiera sina förbättringsområden och skapa ett underlag för lokala prioriteringar. Verktyget är tänkt att ge en övergripande, men konkret, bild av var kommunen befinner sig i sin digitaliseringsutveckling. eBlomlådan, som är frivillig att använda, är framtagen av Sveriges Kommuner och Landsting i samarbete med kommunrepresentanter.

Kolada

I Kommun- och landstingsdatabasen (Kolada) kan man följa kommunernas och landstingens verksamheter från år till år. I Kolada ges en samlad ingång till nyckeltal om resurser, volymer och kvalitet i kommuners och landstings alla verksamheter. Nyckeltalen bygger ofta på nationell statistik från de statistikansvariga myndigheterna, men också på uppgifter från andra källor. Exempelvis deltar de flesta kommuner och landsting i frivillig redovisning av kvalitet i olika verksamheter.

13.3 Nyligen avslutat utredningsarbete

Utredningen om effektiv styrning av nationella digitala tjänster har i sitt slutbetänkande lämnat förslag på hur regeringen kan åstadkomma en effektivare styrning av främst statliga myndigheter, genom att bl.a. införa ett gemensamt mål för den offentliga förvaltningens digitaliseringsarbete. Utredningens förslag omfattar ett antal steg som nedan redogörs för kortfattat.[16]

[15] *Pilotprojekt om ramverk för it-kostnader (TBM)*, Ekonomistyrningsverket, 30 augusti 2017, 2017:63.
[16] *reboot – omstart för den digitala förvaltningen*, (SOU 2017:114), 7 kap.

- Riksdagen föreslås besluta om ett gemensamt mål för den offentliga förvaltningens digitaliseringsarbete. Målet innebär att den offentliga förvaltningens användning av digitala medel ska leda till att det blir så enkelt som möjligt för så många som möjligt att utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av förvaltningens service. Den offentliga förvaltningens användning av digitala medel ska vara säker samt öka kvaliteten och effektiviteten i den offentliga förvaltningen som helhet.
- Regeringen beslutar om ett gemensamt mål (som speglar det mål riksdagen föreslås besluta om) för de statliga myndigheternas digitalisering. Detta mål regleras i en ny förordning med mål för de statliga myndigheternas digitaliseringsarbete. I samma förordning åläggs myndigheterna, att i sin årsredovisning, redovisa sina resultat i förhållande till regeringens mål.
- Myndigheten för digital förvaltning[17] ska stödja regeringens arbete med en samlad analys och bedömning av resultatet av den offentliga sektorns digitaliseringsarbete. Resultatet ska redovisas i en årlig rapport. Regeringen ska ge den nya myndigheten ett särskilt uppdrag att utforma en metod och process för denna uppgift.

Den reglering som utredningen föreslår omfattar inte hela den offentliga förvaltningen utan träffar bara statliga myndigheter. Utredningen rekommenderar emellertid att fullmäktige i kommuner och landsting utformar egna mål för sitt digitaliseringsarbete. Dessa mål bör formuleras i samma anda som de mål utredningen föreslår att riksdagen och regeringen ska besluta om.

13.4 Reglering av uppgiftsskyldighet

Föreskrifter som avser åligganden, t.ex. uppgiftsskyldighet, för kommuner och landsting, ska meddelas genom lag.[18] En lagreglerad skyldighet för kommuner och landsting att redovisa uppgifter om sitt arbete med och kostnader för it och digitalisering saknas i dag, varför dessa uppgifter enbart kan samlas in på frivillig väg.

[17] *Inrättande av en myndighet för digitalisering av den offentliga sektorn,* (dir: 2017:117).
[18] 8 kap. 2 § första stycket 3 regeringsformen.

Det finns emellertid flera exempel där kommuner och landsting i lag har ålagts olika former av uppgiftsskyldighet. Här kan bl.a. nämnas lagen (2001:99) om den officiella statistiken och lagen (2010:1350) om uppgiftsskyldighet i fråga om marknads- och konkurrensförhållanden. Enligt lagen om den officiella statistiken är kommuner och landsting skyldiga att till statistikansvariga myndigheter lämna uppgifter för den officiella statistiken. Lagen om uppgiftsskyldighet i fråga om marknads- och konkurrensförhållanden reglerar skyldigheten för en kommun eller ett landsting, som driver verksamhet av ekonomisk eller kommersiell natur, att vid Konkurrensverkets åläggande redovisa kostnader och intäkter i verksamheten.

När det gäller statliga myndigheter kan uppgiftsskyldighet regleras på förordningsnivå. ESV har, som nämnts i kapitel 13.2, en förordningsreglerad rätt att få den information som myndigheten behöver för sin verksamhet. ESV:s uppdrag att följa de statliga myndigheternas användning av it och att mäta och följa upp hur nyttan av it och digitalisering realiseras, kommer emellertid att flyttas över till den nya Myndigheten för digital förvaltning som startar sin verksamhet den 1 september 2018.[19]

13.5 Våra överväganden och förslag

13.5.1 Några utgångspunkter

Vi ska enligt våra direktiv analysera och lämna förslag på hur en utvidgad, men kostnadseffektiv och inte alltför administrativt betungande, rapportering av hela den offentliga förvaltningens löpande arbete med it och digitalisering kan åstadkommas och utformas.

Vi har uppfattat att målsättningen med en rapportering av den offentliga förvaltningens löpande arbete med it och digitalisering bl.a. är att skapa förutsättningar för bättre uppföljning, styrning, samordning och kostnadskontroll av hela den offentliga förvaltningens digitala utveckling. Den svenska förvaltningsmodellen utgår från fristående myndigheter och självstyrande kommuner och landsting men regeringen har ett styrningsansvar i förvaltningsövergripande frågor som rör digitalisering av den offentliga sektorn. En

[19] Dir. 2017:117.

förutsättning för att regeringen ska kunna utöva sitt uppdrag att styra och samordna den digitala utvecklingen i den offentliga förvaltningen är att det finns ett tillförlitligt underlag att grunda styrningen på.

13.5.2 Skyldighet att lämna uppgifter om it-kostnader

Utredningens bedömning: Den offentliga förvaltningen bör i författning åläggas en skyldighet att lämna uppgifter om it-kostnader.

Skälen för utredningens bedömning

Befintlig rapportering uppfyller inte behoven

Som ovan framgått finns ett antal befintliga rapporteringskanaler, t.ex. Hermes, årsredovisningar, eBlomlådan och metoder som är under utveckling, t.ex. ESV:s pilotprojekt att införa ramverket TBM hos utvalda myndigheter. Dessa uppfyller emellertid inte regeringens behov av en samlad uppföljning av hela den offentliga förvaltningens löpande arbete med it och digitalisering. För det första omfattar ingen av de befintliga rapporteringskanalerna hela den offentliga förvaltningen. För det andra är de uppgifter som rapporteras i t.ex. statliga myndigheters årsredovisningar och Hermes inte tillräckligt standardiserade och detaljerade. För det tredje grundar sig kommuners och landstings rapportering om användning av, och kostnader för, it och digitalisering främst på frivillighet. Sammantaget ger befintlig rapportering inte en helhetsbild över bl.a. kostnadsutvecklingen för it i förvaltningen.

Löpande arbete med it och digitalisering

I våra direktiv anges inte närmare vad som avses med löpande arbete med it och digitalisering i vidsträckt bemärkelse. Rapportering av löpande arbete med it och digitalisering kan dock, i detta sammanhang, antas innebära en omfattande uppgiftsbörda för de uppgiftsskyldiga myndigheterna. Det bör därför övervägas dels i vilken

utsträckning skyldighet att lämna uppgifter bör författningsregleras, dels när uppgiftslämnande kan ske på frivillig väg. Därtill finns, enligt vår uppfattning, flera syften med att ålägga hela den offentliga förvaltningen en uppgiftsskyldighet för sitt löpande arbete med it och digitalisering.

För det första behöver bl.a. regeringen, i syfte att förbättra uppföljning, styrning, samordning och kostnadskontroll, en god överblick över hela den offentliga förvaltningens samlade it-kostnader. En samlad bild av it-kostnaderna i hela den offentliga förvaltningen kan underlätta förvaltningsövergripande beslut om prioritering och samordning inom ett område där resurserna är begränsade men där utmaningarna kan vara desto mer omfattande. För att uppnå detta mål krävs att hela den offentliga förvaltningen åläggs en skyldighet att redovisa uppgifter om it-kostnader. Vi har uppfattat att regeringens behov av att få en grundläggande överblick av de samlade it-kostnaderna i den offentliga förvaltningen är angeläget. Vår bedömning är därför att den offentliga förvaltningen ska åläggas en författningsreglerad skyldighet att rapportera uppgifter om it-kostnader.

För det andra kan en mer fördjupad redovisning av den offentliga förvaltningens löpande arbete med it och digitalisering ha potential att generera nytta för bl.a. riksdagen, regeringen och för varje enskild myndighetsledning. En fördjupad uppgiftsinsamling har potential att fånga vilka effekter den offentliga förvaltningens digitalisering har på samhället i stort men också internt hos varje myndighet, vilka förmågor (ledarskap, styrning, kompetens, kultur etc.) som finns, eller som behöver utvecklas, hos respektive myndighet samt vilka tidsmässiga och personella resurser som går åt i myndigheters digitala utvecklingsarbeten. Genom att utveckla mätmetoder och analysmodeller där de inrapporterande myndigheterna kan ta del av det sammantagna resultatet, göra jämförelser med andra myndigheter och ta del av goda exempel från myndigheter som har kommit långt i sin digitala utveckling kan en fördjupad rapportering vara till gagn också för de uppgiftslämnande myndigheterna, ett s.k. dubbelt lärande. Även allmänheten har enligt vår bedömning ett beaktansvärt intresse av att kunna följa förvaltningens digitalisering.

Eftersom den digitala utvecklingen är ständigt pågående och föränderlig behöver den mätmetod som utvecklas för denna fördjupade rapportering vara dynamisk och flexibel och kunna anpassas utifrån rådande behov. En sådan rapportering som avses här har

också delvis ett annat syfte än den snävare rapporteringen av it-kostnader som beskrivits ovan. Där en obligatorisk rapportering av it-kostnader i första hand avser att uppfylla regeringens behov av överblick, kostnadskontroll och underlag för styrning och samordning, syftar en mätmetod för fördjupad redovisning av det löpande arbetet med it och digitalisering som här avses, till att ge också andra typer av nyttor för en bredare målgrupp.

En sådan mätmetod som i denna andra del åsyftas är komplex till sin natur och kräver ett grundligt utrednings- och utvecklingsarbete. Därtill bör det övervägas i vilken utsträckning den redovisning av uppgifter som här avses kan uppnås genom myndigheternas frivilliga rapportering. Mot bakgrund av de snäva tidsramar som är satta för vårt uppdrag och att vårt uppdrag främst är rättsligt orienterat saknar vi förutsättningar att lämna mer konkreta förslag i denna del. Vi finner dock att regeringen bör överväga fortsatt utrednings- och utvecklingsarbete i syfte att uppnå en mer komplett mätmetod som i ett långsiktigt perspektiv kan gagna digitaliseringen i hela den offentliga förvaltningen. Det uppdrag som ovan skisseras bör lämpligen utföras av den myndighet som får i uppgift att samla in och analysera uppgifter om it-kostnader i den offentliga förvaltningen (se nedan kapitel 13.5.3).

13.5.3 Ny uppgiftsskyldighet förs in i statistikregleringen

Utredningens förslag: I förordningen om den officiella statistiken ska föreskrivas att

- kommuner, landsting och kommunalförbund ska för den officiella statistiken lämna uppgifter om it-kostnader,
- Myndigheten för digital förvaltning är ansvarig myndighet för den officiella statistiken för statistikområdet it-kostnader, och
- it-kostnader är ett statistikområde under ämnesområdet offentlig ekonomi.

Regeringen ska i förordning med instruktion för Myndigheten för digital förvaltning utfärda nödvändiga föreskrifter för uppdraget.

Skälen för utredningens förslag

Vilka aktörer bör omfattas av uppgiftsskyldigheten?

Vårt uppdrag att lämna förslag på hur myndigheterna kan rapportera om sitt löpande arbete med it och digitalisering omfattar hela den offentliga förvaltningen dvs. förvaltningsmyndigheter, domstolar, kommuner och landsting. I den kommunala sektorn förekommer samverkan över kommungränserna genom att kommunalförbund inrättas. Sådan samverkan rör inte sällan gemensam it-drift. För att uppnå en mer rättvisande bild av hela den offentliga förvaltningens it-kostnader bör det därför framgå att även kommunalförbund omfattas av en uppgiftsskyldighet.

Reglering av uppgiftsskyldighet

En uppgiftsskyldighet för kommuner, landsting och kommunalförbund kräver, som tidigare framhållits, stöd i lag.[20] Vi har i vårt utredningsarbete å ena sidan övervägt att föreslå ny lagreglering för den offentliga förvaltningens rapportering av it-kostnader. Å andra sidan har vi övervägt om en uppgiftsskyldighet kan utgå i från en redan befintlig reglering. Här har vi övervägt om regelverket kring den officiella statistiken kan utgöra en lämplig rättslig infrastruktur.

Syftet med den officiella statistiken är att den ska finnas för allmän information, utredningsverksamhet och forskning.[21] Statistik om olika samhällsområden är en mycket viktig informationskälla i en demokrati och tillgången till statistik kan ses som en rättighet för alla medborgare. Statistiken används som grund för politiska beslut, för den allmänna debatten, forskning och utvärdering m.m.[22] Den rättsliga regleringen kring statistikproduktion borgar därtill för hög kvalitet och att jämförelser kan göras över tid av de statistiska beräkningarna.

Enligt vår bedömning kan den uppgiftsinsamling som krävs för att uppnå målsättningen om en samlad bild av hela den offentliga förvaltningens it-kostnader genomföras genom kompletterande rättsregler i det befintliga statistikregelverket.

[20] 8 kap. 2 § första stycket 3 regeringsformen.
[21] 3 § lagen (2001:99) om den officiella statistiken.
[22] *Vad är officiell statistik, En översyn av statistiksystemet och SCB,* (SOU 2012:83), s. 102.

Den officiella statistiken och uppgiftsskyldigheter

Den officiella statistiken regleras i lagen (2001:99) om den officiella statistiken och förordningen (2001:100) om den officiella statistiken (härefter statistiklagen och statistikförordningen). I statistikförordningen specificeras den officiella statistiken i ett antal ämnesområden vilka i sin tur är indelade i olika statistikområden. Statistikförordningen anger vilken myndighet som är ansvarig för respektive statistikområde. Statistikens innehåll och omfattning inom ett statistikområde beslutas av den myndighet som är statistikansvarig på området.

Inom ramen för statistikregelverket finns en författningsreglerad uppgiftsskyldighet för kommuner, landsting och kommunalförbund.[23] Vilka uppgifter som omfattas av uppgiftsskyldigheten regleras, för kommuner, landsting och kommunalförbund, i statistikförordningen .[24] Det rör sig bl.a. om uppgifter om investeringar och beställningar, köp, försäljningar och leveranser av varor och tjänster. Uppräkningen av vilka uppgifter som kan komma ifråga för uppgiftslämnande är uttömmande men en statistikansvarig myndighet får inom sitt verksamhetsområde meddela föreskrifter om verkställighet av bestämmelserna om uppgiftsskyldighet .[25] Sådana föreskrifter har bl.a. Statistiska centralbyrån utfärdat om skyldighet för företag att lämna uppgifter till statistik om företagens utgifter för it och marknadsföring och föreskrifter om skyldighet för företag att lämna uppgifter avseende it-användning i företag.[26]

För att ålägga kommuner, landsting och kommunalförbund en skyldighet att lämna uppgifter om it-kostnader bör detta enligt vår bedömning kunna regleras som en uppgiftsskyldighet i statistikförordningen.

När det gäller statliga myndigheters uppgiftsskyldighet är den mer vidsträckt och kräver ingen ytterligare reglering för att uppgifter om it-kostnader ska kunna samlas in. En statlig myndighet ska till statistikansvariga myndigheter lämna de uppgifter som behövs för

[23] 7 § första stycket 4 statistiklagen.
[24] 5 § 1–7, 5 c § och 5 d § statistikförordningen.
[25] 15 § statistikförordningen.
[26] SCB-FS 2017:3 och 2017:4. Näringsidkares uppgiftsskyldighet, som regleras i 5 § statistikförordningen, överensstämmer i vissa delar med kommuners, landstings och kommunalförbunds uppgiftsskyldighet.

framställning av officiell statistik. Uppgifterna ska lämnas vid den tidpunkt och på det sätt myndigheterna har kommit överens om .[27]

Uppgiftslämnarbördan

Den officiella statistiken bygger på uppgifter som hämtas från olika källor. En allmän målsättning är att minska bördan för uppgiftslämnarna och en statistikansvarig myndighet behöver kontinuerligt arbeta med att uppgiftslämnarbördan inte ska bli allt för belastande. Nödvändiga uppgifter bör så långt det är möjlighet hämtas från tillgängliga, administrativa källor. En sådan källa kan t.ex. vara myndigheternas årsredovisningar.[28]

I syfte att tydliggöra behovet av att minska uppgiftslämnarbördan för de aktörer som är skyldiga att lämna uppgifter till statistikansvariga myndigheter har i statistikförordningen införts ett krav på att statistikansvariga myndigheter ska sträva efter att begränsa uppgiftslämnarbördan.[29] Av bestämmelsen framgår att uppgifter för den officiella statistiken ska samlas in på ett sådant sätt att uppgiftslämnandet blir så enkelt som möjligt, står i proportion till användarnas behov och är en rimlig arbetsbörda för uppgiftslämnarna. Det ankommer på varje statistikansvarig myndighet att hitta metoder som kan minska uppgiftslämnarbördan.[30]

I förordningen (1982:668) om statliga myndigheters inhämtande av uppgifter från näringsidkare och kommuner ställs vissa krav som ska iakttas av statliga myndigheter vid uppgiftsinhämtning i syfte att minska uppgiftslämnarbördan. Regleringen av samrådsskyldighet i 3 § torde bl.a. innebära att den uppgiftsinhämtande myndigheten måste samråda med Sveriges Kommuner och Landsting, när uppgifter ska hämtas in från kommunerna.

Uppgifter om it-kostnader i den offentliga förvaltningen får anses utgöra ett viktigt underlag för regeringsbeslut som har bäring både på den ekonomiska politiken och på politiken kring digitalisering och it inom offentlig förvaltning. Uppgifter om it-kostnader får också anses vara av sådan karaktär att det är naturligt att de ska kunna vara föremål för granskning, särskilt när förvaltningen blir allt

[27] 6 § statistikförordningen.
[28] Se kapitel 13.2 om ESV:s rapport *Digitaliserad årsredovisning – en förstudie*.
[29] 4 § statistikförordningen.
[30] *Ändringar i statistiklagstiftningen*, prop. 2013/14:7 s. 16.

mer digital. Ett statistiskt underlag om den offentliga förvaltningens it-kostnader har potential att förbättra bl.a. regeringens möjlighet att följa upp, analysera, styra och samordna relevanta frågor kopplade till digitaliseringen av den offentliga förvaltningen i stort.

Skälen för att den offentliga förvaltningens uppgiftsskyldighet ska omfatta även it-kostnader anser vi sammantaget väger tyngre än målsättningen att uppgiftslämnarbördan inte ska bli alltför belastande för de uppgiftsskyldiga myndigheterna. Vi föreslår därför att den uppgiftsskyldighet som här diskuteras införs i statistikförordningen.

It-kostnader blir nytt statistikområde

Det saknas en allmänt vedertagen definition av vilka slags utgifter som omfattas av begreppet it-kostnad. ESV har inom ramen för sitt uppdrag att utveckla en it-kostnadsmodell definierat it-kostnader enligt följande.

> It-kostnader är de kostnader som kan härledas till it-funktioner, och begränsas inte nödvändigtvis till it-organisationen. Kostnaderna består av kostnader inklusive avskrivningar (för materiella och immateriella it-investeringar) för drift, förvaltning och utveckling av it-system och utrustning.[31]

I förslag till it-kostnadsmodell har ESV identifierat ett antal nyckeltal som bedöms ge mest nytta och som inte är allt för komplicerade att beräkna. Bland dessa nyckeltal finns it-kostnad som andel av total verksamhetskostnad, it-kostnad per användare, kostnad för utkontrakterad it-verksamhet som andel av total it-kostnad m.fl. Sådana nyckeltal kan också tjäna som ledning och stöd vid avgörande av vilka slags utgifter som omfattas av begreppet it-kostnader.

Utöver att det saknas en förvaltningsgemensam definition av begreppet it-kostnad kan det också förutsättas att myndigheternas interna redovisning av sina kostnader för it skiljer sig åt. Därtill kan det antas att vilka kostnader som, allmänt sett, ska anses utgöra en it-kostnad kommer att förändras över tid i takt med myndigheternas verksamhetsutveckling och den tekniska utvecklingen i samhället.

Avsaknad av exakta definitioner av centrala begrepp förekommer allmänt i den offentliga förvaltningen och bör inte ses som ett hinder

[31] *It-kostnadsmodell, Ett första steg mot ett gemensamt språk,* Ekonomistyrningsverket, 1 oktober 2014, 2014:50, s. 17.

mot uppföljning i syfte att t.ex. uppnå bättre styrning och kostnadskontroll. Här kan exempelvis nämnas begreppet ärende som är ett etablerat begrepp i förvaltningslagen (2017:900) men som saknar en enhetlig och vedertagen definition.[32]

I statistikförordningens bilaga finns en uppräkning av olika ämnesområden för statistik varav ett är offentlig ekonomi. Varje ämnesområde är i sin tur konkretiserat i olika statistikområden. Gemensamt för de statistikområden som räknas upp i bilagan till statistikförordningen är att de till sin natur är vida och kan omfatta ett stort antal statistikprodukter med olika syften och inriktningar. Här kan t.ex. nämnas statistikområdena finanser för den kommunala sektorn och utfallet av statsbudgeten, som båda sorterar under ämnesområdet offentlig ekonomi.

Ett bakomliggande syfte till att lagstiftaren har valt att använda relativt vida och oprecisa begrepp för att beskriva befintliga statistikområden är bl.a. att statistikansvariga myndigheter, i sin statistikproduktion, ska ha utrymme för flexibilitet och kunna anpassa statistiken över tid, efter samhällets utveckling och behov.

Det förhållandet att begreppet it-kostnad saknar en enhetlig definition och avgränsning kan därför, i statistiska sammanhang, vara till fördel eftersom det ger den statistikansvariga myndigheten utrymme att anpassa uppgiftsinsamlingen och statistikproduktion efter vad som efterfrågas över tid t.ex. genom användning av olika nyckeltal. Mot denna bakgrund föreslår vi att statistikområdet it-kostnader bör införas i statistikförordningens bilaga.

Dataskydd och sekretess

Som beskrivits ovan saknas en vedertagen definition av begreppet it-kostnader. En tämligen självklar utgångspunkt bör emellertid vara att det inom ramen för it-kostnader inte kommer vara fråga om insamling av personuppgifter som ska bearbetas för statistiska ändamål.[33] Hanteringen av uppgifter som rör it-kostnader bör därför falla utanför dataskyddsförordningens tillämpningsområde.

[32] Se vidare om definition av begreppet ärende i kap. 7.4.1.

[33] Begreppet personuppgifter definieras i artikel 4 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.

Statistiksekretessen regleras i 24 kap. 8 § offentlighets- och sekretesslagen (2009:400). Som huvudregel gäller sekretess i sådan särskild verksamhet hos en myndighet som avser framställning av statistik för uppgift som avser en enskilds personliga eller ekonomiska förhållanden och som kan hänföras till den enskilde. Med enskild avses fysiska personer och privaträttsliga juridiska personer.

Statistiksekretessen syftar till att skydda enskildas personliga och ekonomiska förhållanden och inte allmänna intressen. Uppgifter om it-kostnader som härrör från det allmänna, omfattas därmed inte av statistiksekretessen i 24 kap. 8 § offentlighets- och sekretesslagen. Därtill bör uppgifterna som samlas in för statistisk bearbetning, som ovan anförts, inte omfatta uppgifter som är hänförliga till en enskild.

Vem bör få uppdraget som statistikansvarig myndighet?

I dag finns 28 statistikansvariga myndigheter. Vilka de statistikansvariga myndigheterna är framgår av bilagan till statistikförordningen. Uppdrag som statistikansvarig myndighet regleras vanligen i respektive myndighets instruktion.[34] Varje statistikansvarig myndighet ansvarar för officiell statistik inom sina respektive samhällssektorer eller motsvarande. Till de statistikansvariga myndigheternas huvuduppgifter hör att utifrån såväl eget som andra användares statistikbehov ta ställning till hur mycket resurser som ska läggas på statistiken, vilken statistik som ska produceras och hur produktionen ska ordnas. Statistiken ska utvecklas löpande och anpassas till samhällets behov. Dessutom ska en statistikansvarig myndighet bestämma statistikens innehåll, form och frekvens m.m. Statistiken ska dokumenteras och kvalitetskontrolleras före publicering och den officiella statistiken ska göras allmänt tillgänglig i tryckt form eller via it-baserade medier. Detta innebär att det i praktiken ingår i ansvarsuppgiften att avgöra vilken statistik på respektive område som ska tas fram i syfte att tillgodose allmänintresset av samhällsinformation.[35]

Regeringen har beslutat att inrätta en Myndighet för digital förvaltning, med uppgift att utveckla, samordna och stödja den förvaltningsövergripande digitaliseringen. Myndigheten ska inleda

[34] Se t.ex. 2 § 1 förordningen (2016:1201) med instruktion för Brottsförebyggande rådet och 5 § 2 förordningen (2015:284) med instruktion för Socialstyrelsen.
[35] SOU 2012:83 s. 138 f.

sin verksamhet den 1 september 2018 och en särskild utredare har fått i uppdrag att förbereda och genomföra bildandet av den nya myndigheten.[36]

Av utredningsdirektiven[37] framgår att myndigheten ska bistå regeringen med underlag för utvecklingen av politiken för digitalisering och it inom den offentliga sektorn och verka för en ökad digitalisering av den. Myndigheten ska därtill utveckla möjligheten att mäta och följa upp hur nyttan av it och digitalisering realiseras i det offentliga Sverige. Mot bakgrund av vad som kan utläsas av utredningsdirektiven kommer den nya myndigheten ha särskild kompetens när det gäller den offentliga sektorns digitalisering.

En utgångspunkt för att den nya Myndigheten för digital förvaltning ska kunna mäta och följa upp nyttan av it och digitalisering är att myndigheten har nödvändiga förutsättningar att hämta in uppgifter från relevanta aktörer i den offentliga förvaltningen. Genom att utse den nya myndigheten till statistikansvarig myndighet för statistikområdet it-kostnader ges myndigheten förutsättningar att ta ställning till vilken statistik som är relevant att producera inom området och vilka uppgifter som behöver hämtas in för att producera statistiken i fråga. Uppgiftsinsamlingen och statistikproduktionen kan därmed, på ett ändamålsenligt och effektivt sätt, bidra till myndighetens uppgift att bistå regeringen med underlag för utvecklingen av politiken för digitalisering och it inom den offentliga sektorn. Mot denna bakgrund föreslår vi att Myndigheten för digital förvaltning ska vara ansvarig statistikmyndighet för statistikområdet it-kostnader. Uppdraget som statistikansvarig myndighet behöver, utöver föreslagen komplettering i statistikförordningens bilaga, även anges i den kommande instruktionen för den nya myndigheten.

13.5.4 Konsekvenser av förslagen

Förslaget om att införa en uppgiftsskyldighet för it-kostnader i statistikförordningen kan väntas förbättra möjligheterna till uppföljning, analys och styrning av den offentliga förvaltningens digitala utveckling. Förslaget väntas därtill leda till ökad transparens i förhållande till allmänheten som har ett berättigat intresse att följa

[36] *Utredningen om inrättande av en myndighet för digitalisering av den offentliga sektorn*, (Fi 2017:09).
[37] Dir. 2017:117.

utvecklingen av, och kostnaderna för, digitalisering av den offentliga förvaltningen.

Förslaget om en ny skyldighet att lämna uppgifter om it-kostnader innebär inte att ett nytt ämnesområde för statistik inrättas utan att uppgiftsskyldigheten inom ett redan befintligt ämnesområde (offentlig ekonomi) utvidgas. Den uppgiftsinsamlande myndigheten ska vidta åtgärder i syfte att uppgiftslämnarbördan inte ska bli allt för belastande. En särskilt specificerad uppgiftsskyldighet kommer emellertid leda till en viss ökad uppgiftslämnarbörda för myndigheterna i den offentliga förvaltningen och därmed kan en viss kostnadsökning förutses för stat, kommun och landsting. Kostnadsökningen för uppgiftslämnandet bedöms dock bli marginell och ryms därför inom befintliga ekonomiska ramar.

Förslaget att utse den nya Myndigheten för digital förvaltning till ansvarig statistikmyndighet för statistikområdet it-kostnader ligger inom ramen för det uppdrag som den nya myndigheten kommer att ha att ge stöd till regeringens satsning att utveckla möjligheten att mäta och följa upp hur nyttan av it och digitalisering realiseras. Att myndigheten utför detta uppdrag inom ramen för den officiella statistiken innebär emellertid att behov uppstår av personal med särskild kompetens inom området för produktion av officiell statistik. Vi uppskattar att detta behov motsvarar två årsarbetskrafter. Finansieringen för denna ytterligare kostnad behöver ingå i regeringens resurssättning av den nya myndigheten. För generella konsekvenser av våra förslag hänvisas till kapitel 14.2.

14 Konsekvenser

14.1 Finns det ett nollalternativ?

För att värdera en utrednings förslag är det önskvärt att utöver förväntade effekter av olika åtgärder också beskriva konsekvenserna av att inga förändringar görs. Förslagen bör alltså kunna jämföras med ett s.k. nollalternativ.

Utredningen om effektiv styrning av nationella digitala tjänster har i sitt slutbetänkande konstaterat att den digitala utvecklingen har begränsningar vad gäller förutsebarhet.[1] Vi instämmer i detta och att utvecklingen styrs av många olika faktorer. Ibland går utvecklingen långsammare än vad som kunnat förutses, ibland görs snabbt något större tekniksprång. Till detta kommer även det förhållandet att våra förslag måste ses i relation till andra insatser som regeringen gör eller som kan komma att genomföras efter andra utredningars förslag. Ett nollalternativ är därför knappast realistiskt att föreställa sig.

Att den offentliga förvaltningen ska följa teknik- och samhällsutvecklingen för att dra nyttor av t.ex. ny teknik torde egentligen vara att se som ett grundläggande krav, bl.a. med beaktande av skyldigheten att hushålla med ekonomiska medel.[2] I kapitel 4 har vi emellertid inlett med att beskriva den risk vi sett för två alternativa scenarier om inte också rättsutvecklingen bedrivs i takt med teknik- och samhällsutvecklingen i övrigt. Vi har å ena sidan sett en risk för att den offentliga förvaltningens digitalisering kan stagnera om gällande reglering hindrar eller hämmar en önskad utveckling. Det kan leda till att förvaltningen framöver får en minskad förmåga att möta kommande samhällsutmaningar och att förtroendet för förvaltningen därför avtar. Den offentliga förvaltningen kan i det sammanhanget inte ses fristående från samhället i övrigt. En förvaltning som

[1] *reboot – omstart för den digitala förvaltningen*, (SOU 2017:114), s. 433.
[2] 1 kap. 3 § budgetlagen (2011:203), 3 § myndighetsförordningen (2007:515) och 11 kap. 1 § kommunallagen (2017:725).

inte är tillräckligt föränderlig kan också leda till bristande förmåga till innovation och utveckling i övriga samhället med ekonomiska eller andra konsekvenser som följd. Vi har å andra sidan också sett en risk för att andra incitament eller styrmedel snabbt driver utvecklingen i offentlig verksamhet vidare utan att regleringen anpassas eller beaktas i tillräcklig utsträckning. Det kan leda till att lagstiftningen slutligen står för långt i från verkliga förhållanden, eller att centrala värden t.o.m. går förlorade. Särskilt bör risker för rättsosäkerhet lyftas fram om förvaltningsutvecklingen inte möts av en rättsutveckling som speglar digitaliseringen.

14.2 Generella konsekvenser

Våra förslag är inriktade på att ge juridiskt stöd, i rättsregler eller andra former, för utvecklingen i den digitala förvaltningen. Förslagen kommer enligt vår bedömning på ett övergripande plan att bidra eller leda till dels konsekvensen att förvaltningen de kommande åren vågar ta sig an förändringar och bedriva digital utveckling, dels konsekvensen att utvecklingen bedrivs på ett sätt som bibehåller eller stärker rättssäkerheten genom bl.a. transparens och öppenhet. Förslagen förväntas därmed bidra till att förvaltningen kan nyttja digitaliseringens fördelar samtidigt som dess negativa konsekvenser på såväl samhällsnivå som individnivå minimeras.

Våra förslag kommer att leda till konsekvenser för såväl enskilda som för statliga myndigheter, kommuner och landsting. För privatpersoner och företag bedömer vi att förslagen kommer att bidra till enklare och säkrare förfaranden i förvaltningen. Förslagen bidrar också till att förvaltningen som helhet kan erbjuda enskilda en likvärdig digital service. Företagen gynnas av en effektivare användning av förvaltningens resurser och ökad digital tillgänglighet till förvaltningen. Vi bedömer också att förslagen medför positiva konsekvenser för de företag som samverkar med förvaltningen i olika former, bl.a. leverantörer, eftersom en tydligare reglering medför bättre förutsebarhet och ökad säkerhet. Vi bedömer också att förslagen bidrar till att gynna innovation.

Våra förslag innebär inte några absoluta skyldigheter för myndigheter att t.ex. ta fram nya digitala tjänster eller anpassa it-system, även om förslaget till bl.a. nya huvudregler om Digitalt först i

förvaltningslagen (2017:900) innebär att förväntningarna höjs på förvaltningens förmåga att vara digitalt tillgänglig för enskilda. Inom ramen för förslagen finns dock utrymme att beakta bl.a. kostnadsaspekter i de enskilda fallen (se vidare kapitel 8.3.3 och 8.3.9). I förlängningen bidrar förslagen enligt vår bedömning till kostnadsbesparingar och effektiviseringar både ur ett förvaltningsövergripande perspektiv och för respektive myndighet.

De förslag som lämnas rör inte enbart statliga myndigheter utan även kommuner och landsting. Övergripande kan sägas att förslagen inte bedöms inverka på den kommunala självstyrelsen på något nytt sätt. Se vidare ytterligare konsekvensanalyser, bl.a. avseende den kommunala finansieringsprincipen, i anslutning till aktuella förslag (se hänvisning nedan).

Den reglering som föreslås bedöms inte stå i strid med de skyldigheter som följer av Sveriges anslutning till Europeiska unionen.

Förslagen förväntas främja den digitala utvecklingen och därmed en övergång från pappersbaserade förfaranden. Detta kan ur miljösynpunkt väntas leda till positiva konsekvenser. Förslagen har inte några särskilda konsekvenser för kvinnor och män eller effekter för jämställdheten.

I kapitel 7.7.5 belyses att våra förslag som rör god offentlighetsstruktur vid vissa automatiserade förfaranden kommer att gagna vissa områden, bl.a. effektiva kontroller av utbetalningar i välfärdssystemen, genom den rättsliga tydlighet som förslagen medför. Förslagen kan i den bemärkelsen ses som ett led i att bidra till att minska brottsligheten eller att öka uppklarningen av brott, samtidigt som skyddet för enskilda stärks. I övrigt kan inte några särskilda konsekvenser för brottsligheten och det brottsförebyggande arbetet väntas av våra förslag. Förslagen bedöms inte få några särskilda konsekvenser för mål- och ärendetillströmningen till domstolarna.

Inga direkta konsekvenser med bäring på sysselsättningen eller negativa konsekvenser i fråga om möjligheterna att nå de integrationspolitiska målen kan förväntas av de förslag som här lämnas.

14.3 Ytterligare konsekvenser av författningsförslagen

14.3.1 Tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring

Ytterligare konsekvenser har beskrivits i anslutning till förslagen, se kapitel 10.6.7.

14.3.2 God offentlighetsstruktur för insyn i förvaltningens ärendehantering vid vissa automatiserade förfaranden

Ytterligare konsekvenser har beskrivits i anslutning till förslagen, se kapitel 7.7.5.

14.3.3 Digital kommunikation

Ytterligare konsekvenser har beskrivits i anslutning till förslagen, se kapitel 8.3.9.

14.3.4 Skyldighet att lämna uppgifter om it-kostnader

Ytterligare konsekvenser har beskrivits i anslutning till förslagen, se kapitel 13.5.4.

14.4 Ytterligare konsekvenser av övriga förslag

14.4.1 Rättssäkra AI-förfaranden i en samverkande förvaltning

Ytterligare konsekvenser har beskrivits i anslutning till förslaget, se kapitel 7.8.2.

14.4.2 Digitala tjänster med eget utrymme

Ytterligare konsekvenser har beskrivits i anslutning till förslaget, se kapitel 8.4.5.

14.4.3 Informationssäkerhet

Ytterligare konsekvenser har beskrivits i anslutning till förslaget, se kapitel 9.7.2.

14.4.4 Utökat stöd för it-avtal och personuppgiftsbiträdesavtal

Ytterligare konsekvenser har beskrivits i anslutning till förslaget, se kapitel 11.6.4.

14.4.5 Organisation för beredning av författningsförslag

Ytterligare konsekvenser har beskrivits i anslutning till förslaget, se kapitel 12.1.3.

15 Ikraftträdande

15.1 Ikraftträdande avseende den nya lagen och lagändringar

Utredningens förslag: Den nya lagen och lagändringarna ska träda i kraft den 1 juli 2019.

Skälen för utredningens förslag: Vi bedömer det angeläget att den föreslagna nya lagen och de föreslagna lagändringarna träder i kraft så snart som möjligt till stöd för förvaltningens digitalisering. Med hänsyn till den tid som kan beräknas gå åt för remissförfarande, fortsatt beredning inom Regeringskansliet och riksdagsbehandling bör de lagbestämmelser utredningen föreslår tidigast kunna träda i kraft den 1 juli 2019. Förslagen innebär inte absoluta krav på t.ex. utveckling av it-system vid myndigheterna eller annat som av dylika skäl kan påverka tidpunkten för ikraftträdande.

Förslagen är inte av den arten att de kräver några särskilda övergångsregler.

15.2 Ikraftträdande avseende förordningsändring

Utredningens förslag: Förordningsändringen ska träda i kraft den 1 januari 2019.

Skälen för utredningens förslag: Vi bedömer det angeläget att även den föreslagna förordningsändringen träder i kraft så snart som möjligt. Med hänsyn till den tid som kan beräknas gå åt för fortsatt beredning bör den förordningsändring utredningen föreslår tidigast kunna träda i kraft den 1 januari 2019. Förslaget innebär inte absoluta

krav på t.ex. utveckling av it-system vid myndigheterna eller annat som av dylika skäl kan påverka tidpunkten för ikraftträdande.

Inte heller dessa förslag är av den arten att de kräver några särskilda övergångsregler.

16 Författningskommentar

16.1 Förslaget till lag (2019:000) om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring

Lagens tillämpningsområde

1 §

I paragrafen, som behandlas i kapitel 10.6.3 och 10.6.6, anges lagens tillämpningsområde. Lagen gäller när en myndighet uppdrar åt en privat leverantör att behandla uppgifter för enbart teknisk bearbetning eller teknisk lagring för myndighetens räkning.

Begreppet teknisk bearbetning eller teknisk lagring härrör från bestämmelsen i 2 kap. 10 § första stycket tryckfrihetsförordningen och utgångspunkten är att innebörden av begreppet är detsamma som i den lagen. Till följd av inte minst den omfattande tekniska utveckling som skett sedan begreppet infördes finns emellertid anledning att här förtydliga innebörden av begreppet enligt denna lag. Teknisk bearbetning eller teknisk lagring som avses i denna lag innefattar åtgärder såsom utveckling, införande, drift, förvaltning eller avveckling av en it-relaterad tjänst där tjänsten kan avse både teknisk funktionalitet och arbete utfört av personal som är hänförligt till den tekniska bearbetningen eller lagringen, t.ex. support. Exempel på tjänster som omfattas av nämnda begrepp är bearbetning eller lagring av uppgifter i ett datacenter eller av uppgifter i e-arkiv, molntjänster eller andra it-baserade funktioner. Även storskalig skanning av dokument är exempel på en tjänst som faller in under begreppet. Beskrivningen är inte avsedd att vara uttömmande.

Lagen tillämpas på tjänster eller funktioner som enbart innebär teknisk bearbetning eller teknisk lagring för myndighetens räkning.

Tjänster eller funktioner som innefattar moment av teknisk bearbetning eller teknisk lagring, men som inte enbart avser sådan bearbetning eller lagring omfattas därför inte av lagen.

Med uttrycket privat leverantör avses en utomstående enskild aktör som levererar en tjänst eller en funktion. Lagen omfattar inte en myndighets köp av varor av en privat leverantör, eftersom leverantören då inte tekniskt bearbetar eller lagrar uppgifter. Lagen omfattar inte heller när en myndighet anlitar en osjälvständig uppdragstagare, eftersom en sådan uppdragstagare inte är en utomstående part utan anses delta i myndighetens verksamhet.

2 §

Paragrafen, som behandlas i kapitel 10.6.6, anger vilka organ och verksamheter som jämställs med en myndighet vid tillämpningen av lagen. Syftet är att sådana organ eller verksamheter som trätt i stället för en myndighet ska omfattas av lagen. Lagen gäller således även när ett organ eller en verksamhet som anges i paragrafen uppdrar åt en privat leverantör att behandla uppgifter för enbart teknisk bearbetning eller teknisk lagring för organets eller verksamhetens räkning.

Av *första punkten* framgår att aktiebolag, handelsbolag, ekonomiska föreningar och stiftelser där kommuner, landsting eller kommunalförbund utövar ett rättsligt bestämmande inflytande, jämställs med en myndighet vid tillämpningen av lagen. Med rättsligt bestämmande inflytande avses detsamma som i 2 kap. 3 § andra och tredje styckena offentlighets- och sekretesslagen (2009:400).

Enligt *andra punkten* jämställs även de organ som anges i bilagan till offentlighets- och sekretesslagen, i de verksamheter som nämns där, med en myndighet vid tillämpningen av lagen.

Vidare jämställs, enligt *tredje punkten*, en yrkesmässigt bedriven enskild verksamhet som till någon del är offentligt finansierad och som anges i 2 § första stycket lagen (2017:151) om meddelarskydd i vissa enskilda verksamheter, med en myndighet vid tillämpningen av lagen. Hänvisningen till nämnda bestämmelse innebär att lagen ska tillämpas i yrkesmässigt bedriven enskild verksamhet som tillhör skolväsendet, de särskilda utbildningsformerna eller annan pedagogisk verksamhet eller utgör hälso- och sjukvård, tandvård eller socialtjänst.

Hänvisningen är dynamisk, vilket innebär att den avser bestämmelsen i den vid varje tidpunkt gällande lydelsen. Även eventuella framtida ändringar i bestämmelsen kommer således att omfattas av hänvisningen.

Med offentlig finansiering avses ett direkt stöd eller betalning från det allmänna för att driva verksamheten inom de aktuella verksamhetsområdena. Det kan t.ex. vara fråga om bidrag till fristående skolor som utgår med stöd av skollagen (2010:800), ersättning som utgår med stöd av lagen (1993:1651) om läkarvårdsersättning eller verksamhet som upphandlas av det allmänna. Det är tillräckligt att en enskild verksamhet till någon del uppbär offentlig finansiering för att en sådan verksamhets utkontraktering till en privat leverantör ska omfattas av lagen. Den offentliga finansieringen måste dock vara kopplad till bedrivandet av verksamheten. Om en verksamhet endast finansieras av allmänna medel under en begränsad tid, t.ex. när en privat läkarmottagning under en viss period tar emot patienter från landstinget, är lagen endast tillämplig under den perioden.

Med verksamhet avses i lagen även verksamhet inom skola, vård och omsorg som bedrivs som en verksamhetsgren i en större verksamhet. Om en verksamhetsgren är offentligt finansierad medan en annan inte är det, gäller lagen bara i den förstnämnda verksamhetsgrenen.

Att den utkontrakterande verksamheten är yrkesmässigt bedriven innebär att verksamheten bedrivs kontinuerligt och i förvärvssyfte.

3 §

Av paragrafen, som behandlas i kapitel 10.6.6, framgår att lagen är subsidiär i förhållande till den nya säkerhetsskyddslagen (2018:000) som träder i kraft den 1 april 2019 och säkerhetsskyddsförordningen (1996:633). Finns det bestämmelser i nämnda lag eller förordning som avviker från denna lag, ska i stället de bestämmelserna tillämpas. Bestämmelserna om tystnadsplikt i den nya säkerhetsskyddslagen ska alltså ha företräde.

Tystnadsplikt

4 §

I paragrafen föreskrivs en tystnadsplikt för dem som är verksamma hos en privat leverantör enligt denna lag. Paragrafen behandlas i kapitel 10.6.2 och 10.6.3.

Av *första stycket* framgår att tystnadsplikten gäller för den som är anställd eller utför ett uppdrag, t.ex. en utomstående konsult, hos en privat leverantör och som tekniskt bearbetar eller tekniskt lagrar uppgifter för en myndighets räkning. Tystnadsplikten gäller även när anställda och uppdragstagare har lämnat sin befattning. Anställda eller uppdragstagare hos en underleverantör till leverantören omfattas också av tystnadsplikten om de tekniskt bearbetar eller tekniskt lagrar uppgifter, eftersom det görs för den utkontrakterande myndighetens räkning.

Vad som avses med begreppet tekniskt bearbetar eller tekniskt lagrar uppgifter framgår av kommentaren till 1 §. Tystnadsplikten omfattar uppgifter som är sekretessreglerade hos myndigheten såväl till skydd för enskilds personliga eller ekonomiska förhållanden, som till skydd för allmänna intressen. Uppgifter som inte är sekretessreglerade hos myndigheten omfattas inte av tystnadsplikten. Att en uppgift inte får röjas eller utnyttjas obehörigen innebär att uppgiften får lämnas ut om tillåtelse föreligger från den som har rätt att förfoga över uppgiften eller om det finns en skyldighet att lämna ut uppgiften som följer av lag eller förordning.

Brott mot tystnadsplikten är straffsanktionerat i 20 kap. 3 § brottsbalken.

I *andra stycket* finns en upplysning om att i det allmännas verksamhet gäller i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Ikraftträdandebestämmelse

Ikraftträdandebestämmelsen anger att lagen träder i kraft den 1 juli 2019. Bestämmelsen behandlas i kapitel 15.

16.2 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

4 kap.

3 §

Paragrafen, som behandlas i kapitel 7.7.1 och 7.7.3, reglerar dokumentation av underlag vid handläggning av mål eller ärenden i samband med vissa automatiserade förfaranden.

Av *första stycket första meningen* framgår att uppgifter som utgör underlag för handläggning av ett mål eller ärende ska tillföras handlingarna i det enskilda målet eller ärendet i läsbar form. Ändringarna innebär en modernisering för att anpassa bestämmelsen till digitala miljöer. Bestämmelsen ska tillämpas när sådant underlag härrör från olika databaser eller andra digitala källor via automatiserade förfaranden. Med andra digitala källor avses exempelvis datafiler eller sensorsystem. Även när underlag inhämtas från exempelvis internetbaserade källor är bestämmelsen tillämplig.

Enligt *första stycket andra meningen* behöver en myndighet inte tillföra underlaget till handlingarna i målet eller ärendet enligt första meningen om det finns särskilda skäl mot det. Ändringarna utgör en språklig anpassning samtidigt som det klargörs att bestämmelsen är fortsatt tillämplig i digitala miljöer. Om det finns tekniska möjligheter att tillgängliggöra ett underlag för parter och andra utan att en dubblett lagras i det enskilda målet eller ärendet kan detta utgöra särskilda skäl mot att tillföra underlaget till handlingarna i målet eller ärendet. Betydande kostnader för dubbel digital lagring av uppgifter kan också vägas in i den sammantagna bedömningen av om det finns särskilda skäl mot att tillföra underlaget till handlingarna i målet eller ärendet. Det kan t.ex. gälla när stora datamängder utgör beslutsunderlag.

Andra stycket är nytt. Där framgår att när en myndighet enligt första stycket andra meningen inte tillför underlag till handlingarna

i det enskilda målet eller ärendet ska myndigheten ändå se till att information kan lämnas om vilken eller vilka databaser eller andra digitala källor som innehåller ett underlag för handläggningen av målet eller ärendet. Bestämmelsen ska inte påverka tillämpningen av sekretessbestämmelser. Att förmågan och funktionen att kunna lämna informationen säkerställs får när sekretess gäller främst betydelse för myndighetens egenkontroll och vid tillsyn.

3 a §

Paragrafen, som är ny, reglerar hur myndigheter ska åstadkomma god offentlighetsstruktur när algoritmer eller datorprogram används som helt eller delvis påverkar utfall eller beslut vid automatiserade förfaranden. Övervägandena behandlas i kapitel 7.7.1 och 7.7.2.

En myndighet ska enligt paragrafen se till att kunna lämna information om hur myndigheten använder vissa algoritmer eller datorprogram vid handläggning av mål eller ärenden. Bestämmelsen gäller för de algoritmer eller datorprogram som används vid helt automatiserat beslutsfattande, dvs. beslut som fattas helt utan mänsklig inblandning. Även algoritmer eller datorprogram som genererar förslag till beslut (beslutsstöd) eller delvis automatiserade beslut omfattas. Algoritmer eller datorprogram som används vid automatiserade förfaranden för urval, t.ex. som syftar till att i förväg bedöma vilken sannolikhet det finns för att en individ ska agera felaktigt, omfattas också av den aktuella bestämmelsen oavsett om urvalet resulterar i ett beslut eller inte. Bestämmelsen ska tillämpas oavsett om en algoritm eller ett datorprogram utgör allmän handling eller inte.

En myndighet ska enligt bestämmelsen se till att information kan lämnas om hur myndigheten vid handläggning av mål eller ärenden använder de algoritmer eller datorprogram som omfattas av regleringen. Att en myndighet ska se till att information kan lämnas innebär att myndigheten ska säkerställa sin förmåga att kunna lämna information, vare sig myndigheten med egen personal utvecklar de aktuella algoritmerna eller datorprogrammen eller anlitar en utomstående leverantör.

Förmågan och funktionen att kunna lämna information enligt paragrafen kan fullgöras på olika sätt beroende på vilket automatiserat förfarande som avses. En övergripande beskrivning av hur de

algoritmer med anknytande datorprogram som omfattas av regleringen används av myndigheten ska emellertid alltid kunna lämnas. I flera fall kan det vidare vara av värde för allmänheten att myndigheten kan redogöra för vilka kategorier av indata som används vid det automatiserade förfarandet, t.ex. om det är uppgifter som hämtats från enskilda, från internetbaserade källor, från databaser på annat håll inom förvaltningen eller från sensorer utplacerade i en viss stad. Den typen av information kan därför också bli aktuell att lämna. Om varken sekretess, immaterialrättsliga förhållanden eller annat hindrar, kan ett sätt att lämna mer än den övergripande informationen vara att programkoden hålls öppen. Paragrafen innebär dock inte någon rättighet för allmänheten att ta del av myndigheters programkod.

Myndigheten är inte skyldig att utan förfrågan lämna eller tillhandahålla informationen, men kan välja att t.ex. publicera den på sin webbplats.

Bestämmelsen ska inte påverka tillämpningen av sekretessbestämmelser. Att förmågan och funktionen att kunna lämna informationen säkerställs får när sekretess gäller främst betydelse för myndighetens egenkontroll och vid tillsyn eller andra liknande förfaranden.

10 kap.

2 a §

Paragrafen, som behandlas i kapitel 10.6.4 och 10.6.5, innehåller en sekretessbrytande bestämmelse.

I *första stycket* föreskrivs att sekretess inte hindrar att en uppgift lämnas ut till en enskild eller till en annan myndighet som utför uppdrag för enbart teknisk bearbetning eller teknisk lagring för den utlämnande myndighetens räkning, om uppgiften behövs för att utföra uppdraget.

Begreppet teknisk bearbetning eller teknisk lagring härrör från bestämmelsen i 2 kap. 10 § första stycket tryckfrihetsförordningen och utgångspunkten är att innebörden av begreppet är detsamma. Begreppet avses också ha samma betydelse som i 1 § lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring och utvecklas i kommentaren till nämnda bestämmelse. Bestämmelsen

ska bara tillämpas när uppdrag utförs enbart för teknisk bearbetning eller teknisk lagring för den utlämnande myndighetens räkning

En förutsättning för att en sekretessbelagd uppgift ska få lämnas ut med stöd av bestämmelsen är att leverantören har behov av uppgiften för att utföra uppdraget från myndigheten. Behovet ska vara konkret. Det är den utlämnande myndigheten som avgör om leverantören behöver uppgifterna. Det krävs inte att det görs en behovsprövning i varje enskilt fall, utan en bedömning kan göras utifrån de behov som typiskt sett finns för en kategori av uppgifter.

Andra stycket innebär undantag till sekretessgenombrottet i första stycket. Enligt *första punkten* ska en uppgift inte lämnas ut om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut. Detta innebär att den utlämnande myndigheten ska göra en intresseavvägning innan en uppgift lämnas ut. Det krävs inte heller här att det görs en prövning i varje enskilt fall, utan en bedömning kan göras utifrån de behov av sekretess som typiskt sett finns för en kategori av uppgifter.

Vid intresseavvägningen ska som utgångspunkt sekretesskyddet hos mottagaren vägas in i bedömningen. Uppgifterna skyddas hos en privat leverantör genom att tystnadsplikt gäller för uppgifterna enligt lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring och hos en offentlig leverantör genom sekretessbestämmelserna i 11 kap. 4 a § och 40 kap. 5 §. Sekretesskyddet för uppgifterna hos mottagaren väger därmed tungt i intresseavvägningen.

Intresset av att lämna ut sekretessbelagda uppgifter till en utomstående leverantör bedöms vidare exempelvis utifrån om utkontraktering av it-drift eller andra it-baserade funktioner bidrar till en mer ändamålsenlig och kostnadseffektiv förvaltning eller en förvaltning som i ökad grad finns tillgänglig för privatpersoner och företag. Även möjligheten att utnyttja ny teknik och en leverantörs expertkompetens på området kan vara skäl som talar för utlämnande vid sådan utkontraktering.

Vissa kategorier av uppgifter kan vara särskilt känsliga till sin natur och det kan finnas skäl till att inte lämna ut dem om inte motstående intressen väger ännu tyngre. Exempel på sådana särskilt känsliga uppgifter kan vara de som anges i artikel 9.1 i dataskyddsförordningen eller sådana som är undantagna från tillämpningsområdet för 10 kap. 27 §. Att särskilt beakta vid intresseavvägningen är

emellertid att utlämnandet av uppgifterna endast görs till ett mindre antal personer hos leverantören för att tekniskt bearbeta eller lagra dem och att avsikten är att de i normalfallet inte ska ta del av uppgifterna.

Kravet på övervägande skäl ger uttryck för att behovet av utkontraktering av it-drift och andra it-baserade funktioner har företräde framför andra intressen. Sammantaget råder därmed en presumtion för sådant uppgiftsutlämnande som enligt första stycket har bedömts behövas för att utföra uppdraget.

Av *andra punkten* framgår att en uppgift inte får lämnas ut om det av andra skäl är olämpligt. Exempel på faktorer som kan inverka på den bedömningen är om det utlämnande som prövas avser en stor mängd sekretessbelagda uppgifter, en gemensam lokalisering i samma datahall av flera sådana uppgiftsmängder eller en viss geografisk lokalisering för bearbetning eller lagring av uppgifterna. Även vem som är mottagare av uppgifterna och om uppgifterna skyddas av tillräckliga säkerhetsåtgärder efter utlämnandet kan vägas in i olämplighetsbedömningen.

Ikraftträdandebestämmelse

Ikraftträdandebestämmelsen anger att lagen träder i kraft den 1 juli 2019. Bestämmelsen behandlas i kapitel 15.

16.3 Förslaget till lag om ändring i förvaltningslagen (2017:900)

7 a §

Paragrafen, som är ny, behandlas i kapitel 8.3.3. I förhållande till de grundläggande kraven på tillgänglighet i 7 § specificeras i denna paragraf att myndigheter ska vara digitalt tillgängliga.

Enligt paragrafen ska en myndighet vara digitalt tillgänglig genom att tillhandahålla och på lämpligt sätt anvisa en eller flera digitala mottagningsfunktioner dit handlingar kan förmedlas. Förutom digitala tjänster dit skriftliga handlingar förmedlas kan digitala mottagningsfunktioner t.ex. omfatta tjänster där handlingar tas emot som innefattar information i form av ljud eller bild. Myndigheten avgör

de närmare formerna och lösningarna för den digitala tillgängligheten.

Med att myndigheten ska anvisa en eller flera digitala mottagningsfunktioner menas att det är myndigheten som informerar allmänheten om hur och när kontakter kan tas, så att det blir enkelt för enskilda att förstå vilka digitala kontaktvägar som de förväntas använda för att kontakta myndigheten.

En myndighet ska inte tillhandahålla en mottagningsfunktion om det är olämpligt av säkerhetsskäl. Viss verksamhet i den statliga förvaltningen kan med beaktande av säkerhetsaspekter vara av sådan karaktär att det inte är lämpligt med digital kommunikation i förhållande till enskilda, i vart fall inte med nu kända medel. Även med hänsyn till överväganden om kostnadseffektivitet eller av andra skäl kan det i vissa fall bedömas vara olämpligt att en myndighet tillhandahåller en digital mottagningsfunktion. Vid den bedömning som en myndighet gör av om det är olämpligt att tillhandahålla en digital mottagningsfunktion bör dock enskildas intressen av digital tillgänglighet till myndigheten särskilt vägas in.

8 a §

Paragrafen, som är ny, behandlas i kapitel 8.3.6. I paragrafen fastläggs principen om Digitalt först när en myndighet ska kommunicera skriftliga underrättelser eller andra handlingar till enskilda.

Enligt *första stycket* ska en myndighets skriftliga underrättelser eller andra handlingar till enskilda som huvudregel förmedlas digitalt. Det är upp till myndigheten att, med beaktande av allmänna krav i bl.a. 6 och 9 §§, först ta ställning till om underrättelse ska lämnas muntligen eller skriftligen (se även 25 och 33 §§). Bestämmelsen är tillämplig när underrättelse eller andra handlingar ska kommuniceras skriftligen.

Paragrafen innebär inte någon skyldighet för myndigheter att förmedla skriftliga underrättelser eller andra handlingar genom någon specifik form eller via någon specifik teknisk lösning. Myndigheten avgör de närmare formerna och lösningarna för den digitala kommunikationen. Av rättssäkerhetsskäl krävs det emellertid normalt att myndigheten aktivt kommunicerar skriftliga underrättelser i sin helhet eller att myndigheten på annat sätt aktivt kommunicerar var

innehållet i underrättelsen finns tillgängligt så att den enskilde enkelt och smidigt kan ta del av den. Det kan exempelvis göras genom ett meddelande med en länk eller någon annan form av notisfunktion som aktivt uppmärksammar den enskilde på förekomsten av och tillgängligheten till den information som en underrättelse avser.

Bestämmelsen hindrar inte att huvudregeln frångås när det på grund av avsaknad av uppgifter om digitala kontaktvägar inte finns förutsättningar för digital kommunikation. Om annan författning innehåller bestämmelser om form för kommunikation av skriftliga underrättelser eller andra handlingar tillämpas den regleringen, vilket följer av 4 §.

Av första stycket följer vidare att skriftliga underrättelser eller andra handlingar inte ska kommuniceras digitalt om det är olämpligt av säkerhetsskäl eller av andra skäl. Viss verksamhet i den statliga förvaltningen kan med beaktande av säkerhetsaspekter vara av sådan karaktär att det inte är lämpligt med digital kommunikation i förhållande till enskilda, i vart fall inte med nu kända medel. Det kan vidare vara något i det enskilda fallet, som t.ex. framkommit i tidigare kontakter med den enskilde, eller för en viss typ av handlingar som gör att myndigheten bedömer det vara olämpligt med digital kommunikation.

Av *andra stycket* följer att enskilda kan meddela att de inte önskar ta emot skriftliga underrättelser eller andra handlingar från myndigheten digitalt. Det kan vara fråga om att den enskilde själv meddelar myndigheten i det enskilda ärendet att denne inte önskar få del av skriftliga handlingar från myndigheten i digital form, eller att det utvecklas nya system och rutiner för att enskilda mer generellt till förvaltningen ska kunna ge besked om önskad form för kommunikation. I linje med den allmänna serviceskyldigheten bör en myndighet hörsamma enskildas uttryckliga önskan i detta avseende och i stället t.ex. översända underrättelser eller andra handlingar per papperspost om inte muntlig kommunikation bedöms lämpligare (se bl.a. 25 och 33 §§). Bestämmelsen inverkar inte på myndighetens möjligheter att bestämma om underrättelse ska ske genom delgivning.

22 §

Paragrafen, som behandlas i kapitel 8.3.4, reglerar hur ankomstdagen för handlingar bestäms. Det införs i *fjärde stycket* en ny hjälpregel om att en handling som förmedlats till en anvisad digital mottagningsfunktion ska anses ha kommit in till myndigheten när den tagits emot där. Det innebär exempelvis att handlingar i form av meddelanden som innehåller skadlig kod, och därför stoppas i myndighetens säkerhetssystem innan de når den digitala mottagningsfunktionen, inte anses ha inkommit till myndigheten. I andra fall kan en handling finnas på en myndighets server endast för att befordras eller lagras av myndigheten för en användares räkning, t.ex. när en enskild fyller i en digital ansökan. Handlingen ska då inte anses ha tagits emot i den anvisade digitala mottagningsfunktionen. Paragrafen är i övrigt oförändrad.

22 a §

Paragrafen, som är ny, behandlas i kapitel 8.3.5. I paragrafen regleras myndigheters skyldigheter att lämna digitala underrättelser om ankomst när en handling tagits emot i en digital mottagningsfunktion.

Av *första stycket* följer att en myndighet digitalt ska förmedla underrättelse till avsändaren när en handling har anlänt till en anvisad digital mottagningsfunktion. Av paragrafens placering följer att bestämmelsen ska tillämpas inom ramen för en myndighets ärendehandläggning. Det kan röra sig om t.ex. en ansökan som ska ha kommit in till myndigheten inom en viss tidsfrist eller en registreringsåtgärd som får rättsverkningar för den enskilde.

I *andra stycket* regleras att myndigheten under vissa förutsättningar inte behöver förmedla en särskild underrättelse till avsändaren enligt första stycket.

Enligt *första punkten* krävs det inte att myndigheten lämnar en aktiv underrättelse enligt första stycket om det på annat sätt framgår för avsändaren att handlingen har tagits emot, t.ex. genom att en enskild som är inloggad i en digital tjänst hos myndigheten för att där fylla i och förmedla en ansökan direkt kan se att handlingen tagits emot. I sådant fall behöver myndigheten inte dessutom aktivt kommunicera en underrättelse om att handlingen har tagits emot.

Av *andra punkten* framgår att sådan underrättelse inte heller behöver lämnas om myndigheten tagit emot en handling som utan onödigt dröjsmål kommer att besvaras digitalt med ett helt eller delvis automatiserat beslut. Vad som avses med onödigt dröjsmål får avgöras med beaktande av omständigheterna i den enskilda situationen. Vare sig beslutsfattandet innefattar mänskliga ställningstaganden eller inte krävs emellertid att det digitala svaret med ett helt eller delvis automatiserat beslut förmedlas skyndsamt.

Enligt *tredje punkten* får myndigheten avstå från att lämna sådan underrättelse om det är olämpligt att underrätta avsändaren om att handlingen har mottagits. Det kan exempelvis vara fråga om att enskilda i något sammanhang har rätt att eller behöver kunna agera anonymt när de via en digital tjänst kommunicerar med en myndighet, och det därför bedöms vara olämpligt att anordna tekniska förutsättningar för återkoppling till den enskilde om att meddelandet har tagits emot.

25 §

Paragrafen reglerar krav på kommunikation innan en myndighet fattar beslut i ett ärende. Övervägandena finns i kapitel 8.3.6.

Ändringen i *andra stycket* är en följd av att det i 8 a § införs en ny huvudregel om att en myndighets kommunikation av skriftliga underrättelser och andra handlingar ska ske digitalt, om det inte är olämpligt av säkerhetsskäl eller av andra skäl. Genom ändringen klargörs att den nya huvudregeln om digital kommunikation inte inverkar på myndighetens val att kommunicera material muntligen, t.ex. via telefon eller videokonferens, i samband med ett besök hos myndigheten eller på ett servicekontor eller vid syn eller besiktning som myndigheten utför. Det allmänna kravet på service och de allmänna utgångspunkterna för handläggningen i 6 och 9 §§ måste beaktas när myndigheten väljer om underrättelse ska ske muntligen eller skriftligen.

Paragrafen är i övrigt oförändrad.

33 §

I paragrafen finns bestämmelser om underrättelse till den som är part om innehållet i ett beslut och hur ett överklagande går till. Övervägandena finns i kapitel 8.3.6.

Ändringen i *tredje stycket* är en följd av att det i 8 a § införs en ny huvudregel om att en myndighets kommunikation av skriftliga underrättelser och andra handlingar ska ske digitalt, om det inte är olämpligt av säkerhetsskäl eller av andra skäl. Genom ändringen klargörs att den nya huvudregeln om digital kommunikation inte inverkar på myndighetens val att kommunicera material muntligen, t.ex. via telefon eller videokonferens, i samband med ett besök hos myndigheten eller på ett servicekontor eller vid syn eller besiktning som myndigheten utför. Det allmänna kravet på service och de allmänna utgångspunkterna för handläggningen i 6 och 9 §§ måste beaktas när myndigheten väljer om underrättelse ska ske muntligen eller skriftligen.

Paragrafen är i övrigt oförändrad.

Ikraftträdandebestämmelse

Ikraftträdandebestämmelsen anger att lagen träder i kraft den 1 juli 2019. Bestämmelsen behandlas i kapitel 15.

Kommittédirektiv 2016:98

Rättsliga förutsättningar för en digitalt samverkande förvaltning

Beslut vid regeringssammanträde den 24 november 2016

Sammanfattning

En särskild utredare ges i uppdrag att kartlägga och analysera i vilken utsträckning det förekommer lagstiftning som i onödan försvårar digital utveckling och samverkan inom den offentliga förvaltningen. Utredaren ska lämna förslag till de författningsändringar som bedöms ha störst potential att stödja den fortsatta digitaliseringen av den offentliga förvaltningen. Författningsförslagen ska vara motiverade utifrån en sammantagen bedömning, där samtliga relevanta intressen och perspektiv har beaktats och vägts mot varandra. Utredaren ska särskilt beakta behovet av skydd av den personliga integriteten och av uppgifter utifrån sekretesskäl samt behovet av informationssäkerhet och rättssäkerhet.

Utredaren ska särskilt analysera sådan lagstiftning som i onödan försvårar digitalt informationsutbyte inom den offentliga förvaltningen och genomförandet av regeringens målsättning om att digitala tjänster, så långt det är möjligt och när det är relevant, ska vara förstahandsval vid den offentliga sektorns kontakter med medborgare, organisationer och företag. Utredaren ska vidare bl.a. lämna förslag till hur en utvidgad rapportering av hela den offentliga förvaltningens löpande arbete med it och digitalisering kan utformas samt hur aktörerna inom förvaltningen som helhet kan samverka kring behovet av ny eller ändrad lagstiftning för att främja digitaliseringen.

Uppdraget ska redovisas senast den 31 mars 2018.

Behovet av lagstiftning som stödjer digitalisering och samverkan

Digitaliseringskommissionen har i sitt betänkande Digitaliseringens transformerande kraft – vägval för framtiden (SOU 2015:91) konstaterat att digitaliseringen ändrar förutsättningarna för de offentligt finansierade verksamheterna genom att den erbjuder stora möjligheter till effektivisering och rationalisering, och en högre kvalitet i de tjänster som tillhandahålls. Kommissionen framhåller att detta ställer nya krav på den offentliga sektorn, bl.a. på transparens och interaktion i den service och information som ges. Verksamhetsutvecklingen i denna sektor handlar enligt kommissionen alltmer om att använda digitaliseringens möjligheter för att möta utvecklingen i omvärlden.

Regeringen har konstaterat att det finns en stor potential i ökad digital samverkan för att ge medborgare enklare och sammanhängande e-tjänster, minska behovet av uppgiftslämnande och effektivisera myndigheternas verksamheter (prop. 2015/16:1 utg.omr. 22 avsnitt 4.4.2.2). Behovet av samverkan mellan myndigheterna har även uppmärksammats av riksdagen, som har tillkännagett för regeringen att den dels bör se till att de statliga myndigheterna på ett bättre sätt samverkar över myndighetsgränserna med e-förvaltningsprojekt, dels säkerställer att myndigheterna lägger ett ökat fokus på att ta fram fler e-tjänster (bet. 2015/16:FiU25, rskr. 2015/16:208).

Efter att länge ha varit en av de ledande nationerna på e-förvaltningsområdet har Sverige de senaste åren tappat placeringar och uppvisat ett mer varierat resultat i internationella mätningar. E-delegationen anför i sitt slutbetänkande En förvaltning som håller ihop (SOU 2015:66) att den svenska offentliga sektorn hittills inte har varit tillräckligt sammanhållen i sättet att utveckla e-tjänster för medborgare och företag. Enskilda myndigheter bedriver omfattande och ambitiösa projekt på området, men för att möta behoven och förväntningarna från privatpersoner och företag krävs även e-tjänster som är gemensamma för flera myndigheter. Enligt E-delegationen innebär myndigheternas fristående roll en risk för att de utgår från det egna uppdraget, och inte i tillräcklig utsträckning samverkar med varandra för att tillgodose behovet av sammanhållna e-tjänster som kan bidra till en enklare vardag för privatpersoner och företag. Delegationen konstaterar också att juridiken sätter ramarna för hur

myndigheterna bedriver sitt gemensamma utvecklingsarbete och bedömer att det finns behov av att lösa de samverkanshinder som motverkar de övergripande e-förvaltningsmålen om en enklare, öppnare och mer effektiv förvaltning.

I rapporten Delegerad digitalisering – en utvärdering av E-delegationen (2014:12) pekar Statskontoret på att det finns ett behov av att utreda vad som krävs för att göra olika system och tjänster inom den offentliga sektorn kompatibla med varandra samt hur en ökad effektivitet på systemnivå inom statsförvaltningen kan uppnås. Vidare har Digitaliseringskommissionen i sitt betänkande Digitaliseringens transformerande kraft – vägval för framtiden (SOU 2015:91) framhållit att befintliga regelverk många gånger behöver anpassas när välfärdstjänster automatiseras eller digitaliseras för att den nya tekniken ska kunna användas. Kommissionen har därför föreslagit att regeringen ska tillsätta en utredning i syfte att göra en kartläggning över lagstiftning som försvårar digitalisering i samhället.

Riksrevisionen konstaterar i granskningen Den offentliga förvaltningens digitalisering – En enklare, öppnare och effektivare förvaltning? (RIR 2016:14) att det kvarstår stora utmaningar i mötet mellan digital teknik och gällande lagstiftning, vilket har lett till att olika aktörer har olika uppfattning om de rättsliga förutsättningarna på området och att den rättsliga grunden för vissa e-tjänster är osäker. Myndigheten rekommenderar därför regeringen att på ett samlat sätt utreda vilka författningsändringar som behövs för att kunna skapa en digital förvaltning.

E-delegationen har i två av sina delbetänkanden analyserat lagstiftning som försvårar digitaliseringen och lämnat förslag i syfte att underlätta digital samverkan inom den offentliga förvaltningen (SOU 2014:75 och SOU 2014:39). Vidare har Informationshanteringsutredningen haft i uppdrag att se över den mycket omfattande registerlagstiftning som tillsammans med bl.a. personuppgiftslagen (1998:204) reglerar hur statliga och kommunala myndigheter ska behandla personuppgifter. I delbetänkandet Överskottsinformation vid direktåtkomst (SOU 2012:90) har utredningen lämnat förslag till ändrade sekretessregler vid s.k. direktåtkomst till uppgifter. I slutbetänkandet Myndighetsdatalag (SOU 2015:39) har utredningen lämnat förslag till en sammanhållen myndighetsdatalag för den offentliga sektorn. Betänkandena har remissbehandlats och bereds för närvarande inom Regeringskansliet.

Slutligen har Ekonomistyrningsverket (ESV) i sin rapport Fördjupat it-kostnadsuppdrag – Förslag inför framtiden (ESV 2015:64) lyft fram behovet av att fler myndigheter omfattas av arbetet med att följa upp digitaliseringen av den offentliga sektorn. Mätmetoderna behöver enligt ESV utvecklas då en bättre uppföljning skapar transparens och tydliggör var digitaliseringen kan bidra till ytterligare effektivisering.

Uppdraget

Kartlägga lagstiftning som försvårar digitaliseringen och lämna författningsförslag

Utöver de betänkanden från E-delegationen och Informationshanteringsutredningen som nämnts ovan saknas det mer utförliga översyner av vilken lagstiftning som kan anses i onödan försvåra den fortsatta digitaliseringen av den offentliga förvaltningen. Dessa utredningar har vidare varit avgränsade till vissa lagstiftningsområden. Det finns därför ett tydligt behov av en kartläggning och analys som i ett bredare perspektiv tar sikte på lagstiftning som i onödan försvårar digitalisering och digital samverkan i den offentliga förvaltningen. Kartläggningen bör inte omfatta lagstiftning som visserligen försvårar eller hindrar digitalisering, men är motiverad av olika berättigade skyddsintressen, såsom exempelvis behovet av informationssäkerhet, rättssäkerhet och sekretess eller skydd av den personliga integriteten.

Det finns även behov av en utförlig analys av hur olika lagstiftningsåtgärder på digitaliseringsområdet bör prioriteras och vägas mot varandra. För det första krävs en analys av vilken potentiell nytta som respektive lagstiftningsåtgärd innebär. I denna analys bör flera faktorer beaktas, såsom åtgärdens förutsättningar att lösa problem som är gemensamma för stora delar av den offentliga förvaltningen, hur stor effekt åtgärden väntas ha på den digitala tjänsteutvecklingen hos myndigheterna och vilka konkreta tjänster hos myndigheterna som kan stimuleras genom åtgärden. För det andra krävs en analys av vilka möjligheter det finns att genomföra lagstiftningsärendet på kort och lång sikt. Här bör hänsyn tas till bl.a. andra pågående lagstiftningsåtgärder som hanterar frågor med koppling till utvecklingen av den digitala offentliga förvaltningen.

Vidare bör det, för att undvika ensidiga förslag som saknar bredare förankring, säkerställas att samtliga relevanta intressen och perspektiv vägs in i bedömningen. Det kan exempelvis röra sig om avvägningar mellan å ena sidan ökad effektivitet och öppenhet och å andra sidan behovet av informationssäkerhet och rättssäkerhet samt skydd av den personliga integriteten och av uppgifter utifrån sekretesskäl.

Utredaren ska mot denna bakgrund

- kartlägga och analysera i vilken utsträckning det förekommer lagstiftning som i onödan försvårar digital utveckling och samverkan inom den offentliga förvaltningen,
- i samband med kartläggningen även behandla lagstiftning som efter en analys inte nödvändigtvis visar sig vara direkt hindrande, men där det inom den offentliga förvaltningen finns en rättslig osäkerhet som har en hämmande inverkan på den digitala utvecklingen,
- prioritera kartläggning och analys av sådan lagstiftning som i sin helhet eller i stora delar påverkar den offentliga förvaltningen,
- i möjligaste mån visa på konkreta fall där utvecklingen av digitala tjänster hindrats som en följd av den aktuella lagstiftningen, och
- lämna förslag till sådana författningsändringar som utifrån en sammanvägd bedömning av potentiell nytta och genomförbarhet har störst potential att stödja den fortsatta digitaliseringen av den offentliga förvaltningen, samtidigt som behovet av skydd av den personliga integriteten och av uppgifter utifrån sekretesskäl samt behovet av informationssäkerhet och rättssäkerhet särskilt beaktas.

Författningsförslagen bör som utgångspunkt vara teknikneutrala till sin utformning. Utredaren bör vidare undvika att lämna förslag avseende speciallagstiftning som enbart påverkar enstaka verksamhetsområden inom den offentliga förvaltningen.

Författningsförslagen ska inte omfatta ändringar av grundlag. Vidare pågår för närvarande ett omfattande författningsarbete som syftar till att anpassa den svenska regleringen på personuppgiftsområdet till Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana

uppgifter och om upphävande av direktiv 95/46/EG och genomförandet av Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, kallad EU:s dataskyddsreform. Denna reform både förutsätter och möjliggör kompletterande nationella bestämmelser av olika slag och det pågår flera utredningar för att genomföra det nya dataskyddsdirektivet och för att anpassa den nationella lagstiftningen till dataskyddsförordningens krav. Mot denna bakgrund ska inte utredaren lämna några förslag till ändringar på personuppgiftsområdet.

Prioriterade områden vid kartläggningen

Regeringen anser att digitala tjänster, så långt det är möjligt och där det är relevant, ska vara förstahandsval vid den offentliga sektorns kontakter med medborgare, organisationer och företag (prop. 2015/16:1 utg.omr. 22 avsnitt 4.5.1). Detta är grunden i regeringens satsning Digitalt först. Den nya tekniken innebär en stor effektiviseringspotential och kan också bidra till att förstärka förvaltningens öppenhet (prop. 2009/10:175 s. 2). För att målsättningen ska kunna uppnås krävs bl.a. att den offentliga förvaltningen har rättsliga förutsättningar att styra relevanta ärendeflöden och interaktioner med individer och företag till digitala lösningar. Samtidigt är det viktigt att den grundlagsfästa likabehandlingsprincipen i 1 kap. 9 § regeringsformen och myndigheternas allmänna serviceskyldighet enligt 4 § förvaltningslagen (1986:223) samt behovet av informationssäkerhet, rättssäkerhet, sekretess och skydd för den personliga integriteten iakttas även vid tillhandahållandet av digitala tjänster.

Flera rättsliga utmaningar uppstår i samband med digital samverkan och informationsutbyte inom den offentliga förvaltningen. Samtidigt är det i de förvaltningsgemensamma lösningarna som en stor del av den samhällsekonomiska potentialen i digitaliseringen av den offentliga förvaltningen finns. Regeringens målsättning är att uppgifter, i de fall det är möjligt och lämpligt, bara ska behöva lämnas en gång (prop. 2016/17:1 utg.omr. 22 avsnitt 4.5.1). Motsvarande

initiativ finns även på europeisk nivå och principen kommer till uttryck i bl.a. Europeiska kommissionens strategi för den digitala inre marknaden. Detta ställer ökade krav på myndigheterna när det gäller digitalt utbyte av information, inte bara på nationell nivå, utan även över landsgränserna. Det är därför angeläget att säkerställa att lagstiftningen ger ett tillräckligt tydligt stöd för ett sådant informationsutbyte. Det osäkra rättsläge som myndigheterna upplever i samband med informationsutbyte, bl.a. när det gäller offentlighet och sekretess, och som kommit till uttryck i bl.a. E-delegationens betänkanden och Riksrevisionens granskning, verkar hämmande på utvecklingen av en effektiv digitalt samverkande förvaltning. Samtidigt är det vid ett ökat digitalt informationsutbyte viktigt att säkerställa att behovet av informationssäkerhet och skydd av den personliga integriteten samt allmänhetens rätt till insyn tillgodoses. I detta sammanhang aktualiseras frågor om transparens och öppenhet samt individens möjligheter och rättsliga förutsättningar till kontroll över den information som skickas mellan myndigheterna.

Stora delar av den kommunala verksamheten utförs i privat regi. Privata utförare av offentligt finansierade uppgifter bör ha rättsliga förutsättningar att erbjuda offentlig service med hjälp av digitala tjänster på lika villkor, och med samma skyldigheter, som offentliga utförare.

Utredaren ska mot denna bakgrund

- särskilt analysera och föreslå vilket författningsstöd som krävs för att tillvarata den fulla potentialen i regeringens satsning Digitalt först för att därigenom möjliggöra en övergång från traditionella ärendeflöden till digitala interaktioner mellan den offentliga förvaltningen och individer eller privata aktörer,
- särskilt analysera sådan lagstiftning som i onödan försvårar digitalt informationsutbyte inom den offentliga förvaltningen och utifrån denna analys bedöma om och lämna förslag till hur lagstiftningen kan anpassas för att skapa bättre förutsättningar för ett informationsutbyte som uppfyller högt ställda krav på effektivitet och öppenhet samt behovet av skydd av den personliga integriteten, sekretess och informationssäkerhet, och

- inom ramen för analysen avseende digitalt informationsutbyte även behandla frågor om informationsutbyte mellan den offentliga förvaltningen och privata utförare av offentligt finansierade uppgifter.

De avgränsningar och prioriteringar som utredaren ska beakta vid den generella kartläggningen och vid framtagandet av författningsförslag med anledning av den kartläggningen ska även gälla vid genomförandet av de ovan nämnda deluppdragen.

Rapportering av den offentliga förvaltningens arbete med it och digitalisering

It-kostnader är i dag det andra största utgiftsslaget i den offentliga förvaltningens verksamhetskostnader och utvecklingen av it-stödet är en central del av förvaltningens verksamhetsutveckling. För att kunna ta till vara digitaliseringens möjligheter finns behov av att öka den digitala mognaden och kompetensen inom hela den offentliga förvaltningen. Ett sätt att åstadkomma detta är att skapa en bättre uppföljning och styrning och att analysera relevanta frågor kopplade till digitalisering inom den offentliga förvaltningen. I detta ingår också att sammanställa en bättre bild av var de stora utmaningarna och potentialen finns för digitaliseringen av den offentliga förvaltningen. Regeringen har redan i dagsläget ställt krav på de statliga myndigheternas rapportering på området, men förutsättningarna för att kunna säkerställa en mer omfattande rapportering av arbetet med it och digitalisering som omfattar hela den offentliga förvaltningen behöver utredas och om möjligt förbättras.

Utredaren ska mot denna bakgrund

- analysera och lämna förslag på hur en utvidgad, men kostnadseffektiv och inte alltför administrativt betungande, rapportering av hela den offentliga förvaltningens löpande arbete med it och digitalisering kan åstadkommas och utformas, samt
- sammanställa och redovisa de kostnader som är förknippade med en sådan rapportering.

Vid utformningen av förslaget ska utredaren utgå från den modell för rapportering av it-kostnader som ESV föreslagit i sin slutrapport Fördjupat it-kostnadsuppdrag – Förslag inför framtiden (ESV 2015:64).

Bättre förutsättningar för hantering av rättsliga utmaningar

Digitaliseringen beskrivs som vår tids starkaste förändringsfaktor. Den utveckling som skett på området den senaste tioårsperioden, exempelvis när det gäller tillgången till smarta mobiltelefoner och stora datamängder, sakernas internet, dvs. anslutningen av alltmer teknisk utrustning till internet, och delningsekonomin, kommer att påverka den offentliga förvaltningens förhållningssätt samt dess tillhandahållande av service till individer och företag. Det är angeläget att den offentliga förvaltningens verksamhet bygger på anpassade och långsiktigt hållbara rättsliga regler som ger stöd för digital utveckling, samtidigt som de säkerställer behovet av informationssäkerhet och skydd av den personliga integriteten, och allmänhetens rätt till insyn och tillgång till god offentlig service.

Den snabba förändringstakten kräver ett mer proaktivt arbete med att analysera hur den offentliga förvaltningen påverkas av digitaliseringen. Regeringen behöver bl.a. tidigt uppmärksammas på behov av anpassning av lagstiftningen för att kunna stödja utvecklingen när den äger rum. Lagstiftningen bör vidare utformas med teknikneutralitet och framtida digitala samhällsförändringar i åtanke för att den digitala utvecklingen ska vara möjlig. Den bör exempelvis inte innefatta onödiga krav på pappersbaserade förfaranden eller manuella processer. På ett område som präglas av snabb utveckling kan det även vara svårt att tillräckligt snabbt hitta den reglering som skapar bäst förutsättningar över tid.

Samverkan sker redan i dag inom den offentliga förvaltningen för att identifiera behov av ny eller ändrad lagstiftning på området för digitalisering av den offentliga förvaltningen. Förutsättningarna för samverkan kan dock utvecklas, bl.a. för att säkerställa att mer fullständiga underlag tas fram, som väger in samtliga relevanta intressen, och för att involvera fler delar av förvaltningen i arbetet.

Utredaren ska mot denna bakgrund

- analysera den pågående digitala utvecklingen utifrån ett rättsligt perspektiv för att skapa en förståelse för vilka områden och företeelser som i förlängningen kommer att kräva lagstiftningsåtgärder för att de möjligheter som digitaliseringen och den tekniska utvecklingen skapar för den offentliga förvaltningen ska kunna tas till vara,
- analysera och lämna förslag till hur den offentliga förvaltningen som helhet kan samverka kring behovet av ny eller ändrad lagstiftning för att främja digitaliseringen av förvaltningen, och
- lämna förslag till andra åtgärder som syftar till att skapa bättre förutsättningar för hantering av rättsliga utmaningar med anledning av digitaliseringen av den offentliga förvaltningen.

Konsekvensbeskrivningar

Utredaren ska utifrån de förslag som lämnas redovisa de konsekvenser och kostnader som uppstår för den offentliga förvaltningen samt för privata aktörer och enskilda. Utredaren ska i sin redovisning särskilt redogöra för hur hänsyn tagits till behovet av informationssäkerhet, rättssäkerhet, skydd för den personliga integriteten samt allmänhetens rätt till insyn.

Utredaren ska även analysera vilka konsekvenser förslagen får för kvinnor och män samt förslagens effekter för jämställdheten.

Samråd och redovisning av uppdraget

Kartläggningen av lagstiftning som i onödan försvårar digital utveckling och digital samverkan i den offentliga förvaltningen ska bl.a. genomföras genom dialog med de aktörer inom den offentliga förvaltningen som har kommit långt i sitt arbete med digitalisering, samt i relevanta delar även med representanter för näringslivet.

Utredaren ska vidare särskilt samråda med Datainspektionen, Myndigheten för samhällsskydd och beredskap samt Sveriges Kommuner och Landsting. I relevanta delar ska utredaren även inhämta synpunkter från Försvarsmakten. Utredaren ska också hålla sig

informerad om och beakta sådant arbete som på området pågår inom Regeringskansliet och på EU-nivå.

Utredaren ska även ta hänsyn till pågående digitaliseringsarbeten inom olika sektorer och beakta tidigare utredningar på området, bl.a. det arbete som utförts av E-delegationen och Informationshanteringsutredningen.

Utredaren ska ta särskild hänsyn till pågående utredningsarbete i samband med EU:s dataskyddsreform och i lämplig omfattning följa de utredningar som tillsatts för att anpassa svensk rätt till reformen. Utredaren ska även följa andra på området relevanta utredningar och lagstiftningsförslag, bl.a. utredningen om effektiv styrning av nationella digitala tjänster i en samverkande förvaltning (N 2016:01). Vidare ska utredaren ta hänsyn till regeringens kommande strategi om informations- och cybersäkerhet (prop. 2016/17:1 utg.omr. 6 avsnitt 4.3).

Uppdraget ska redovisas senast den 31 mars 2018.

(Finansdepartementet)

Mötesstöd

Mötesstödet utgör ett underlag för de aktörer som deltar i den kartläggning som utförs inom ramen för Digitaliseringsrättsutredningens uppdrag (dir. 2016:98).

1. Kartläggning – lagstiftning som försvårar digitalisering inom offentlig förvaltning

Rättsliga hinder eller utmaningar inom prioriterade områden för kartläggningen

Med utgångspunkt i redan befintligt it-stöd, pågående och/eller planerat digitaliseringsarbete beskriv era erfarenheter av:

- direkt hindrande författningar,
- oklar tillämpning av författningar, eller
- avsaknad av författningar

fördelat på följande områden:

- Utveckling och användning av egna digitala tjänster för (extern) kommunikation med enskilda (privatpersoner eller företag)
  - i samband med ärendehandläggning,
  - i samband med service, eller
  - i samband med affärsverksamhet eller uppdragsverksamhet.
- Digital ärendehandläggning.
- Helt eller delvis automatiserat beslutsfattande.

- Helt eller delvis automatiserat faktiskt handlande (dvs. verksamhetsutövning som varken utgör ärendehandläggning eller service till enskilda).
- Myndighetsgemensamma digitaliseringsprojekt (eller program etc.).
- Digitaliseringsprojekt (eller program etc.) i samverkan med privata aktörer.
- Informationsutbyte mellan myndigheter (statliga eller kommunala).
- Informationsutbyte mellan myndighet och privat utförare av offentligt finansierade tjänster.
- Informationsutbyte över nationsgränserna mellan myndigheter och/eller privat utförare av offentligt finansierade tjänster.

Rättsliga hinder eller utmaningar inom andra relevanta områden

Med utgångspunkt i redan befintligt it-stöd, pågående och/eller planerat digitaliseringsarbete beskriv era erfarenheter, i förhållande till rättsliga hinder eller utmaningar, inom nedan angivna områden.

Digital service och ärendehandläggning

- E-tjänster som tillhandhålls enskilda för exempelvis ansökan eller anmälan.
- ”The Once Only Principle”, dvs. att enskilda endast ska behöva lämna samma uppgift en gång.
- Kommunikation med enskilda via digitala kanaler.
- Enskildas användning av s.k. ”eget utrymme[1]” inom ramen för myndighetens verksamhet.

[1] E-delegationen har definierat ”eget utrymme” som ett förvar som myndigheten tillhandahåller åt en användare endast som led i teknisk bearbetning eller teknisk lagring för användarens räkning (SOU 2014:39 s. 28).

Digitaliseringsprojekt i samverkan med myndigheter och/eller privata aktörer

- Ansvarsfrågor exempelvis i förhållande till integritetsskydds- och sekretesslagstiftningen m.m.
- Avsaknad av gemensamma (öppna) standarder, specifikationer och format.

Arkivering m.m.

- Arkivering och gallring i digitala miljöer.
- Formkrav som kräver pappershantering.

Outsourcing

- Outsourcing av it (infrastruktur, tjänster m.m.) till andra myndigheter eller privata aktörer (upphandling).

Övrigt

- It- och informationssäkerhetsmässiga utmaningar i egna och/eller förvaltningsgemensamma digitaliseringsprojekt.
- Information för vidareutnyttjande (Public Sector Information, PSI) och/eller öppen data.

Exempel på relevant lagstiftning

- Arkivlagstiftning
- eIdas-förordning
- Ensamrätter/upphovsrätt
- Förvaltningslagen
- Integritetsskyddslagstiftning
- Kameraövervakningslag

- Kommunallag
- Lag om ansvar för elektroniska anslagstavlor
- Lag om elektronisk kommunikation
- Lag om vidareutnyttjande av handlingar från den offentliga förvaltningen (PSI)
- Sekretesslagstiftning
- Statsstödsreglering
- Säkerhetslagstiftning
- Tryckfrihetsförordningen
- Upphandlingslagstiftning

2. Kartläggning – bättre förutsättningar att hantera rättsliga utmaningar

Samverkan i den offentliga förvaltningen kring behov av ny eller ändrad lagstiftning

Beskriv med utgångspunkt i nuläget hur samverkan sker med andra aktörer inom den offentliga förvaltningen för att främja digitaliseringen.

- Inom vilka områden och i vilka former samverkar ni med andra aktörer i den offentliga förvaltningen?
- Vilka samverkansformer och kanaler ser ni att det finns behov av för att främja digitaliseringsutveckling och anpassning av lagstiftning såväl inom den egna verksamheten som i hela den offentliga förvaltningen?
- Andra tankar och förslag kring hur bättre förutsättningar för hantering av rättsliga utmaningar kan uppnås genom samverkan?

Reflektioner inför framtida digital utveckling och rättsliga utmaningar

Beskriv, i förhållande till befintliga rättsliga hinder eller utmaningar, hur ni kan, eller kan komma att, använda er av bl.a. nedan uppräknade tekniker eller tjänster.

- Appar.
- API:er.
- Artificiell intelligens.
- Big data, öppna data, PSI.
- Biometri.
- Blockchain-teknik.
- Digitala kameror.
- Förstärkt verklighet (Augmented Reality).
- Geotaggning.
- Molntjänster.
- Sakernas internet (Internet of Things).
- Sensorer.
- Sociala medier.
- Virituell verklighet.

Statens offentliga utredningar 2018

Kronologisk förteckning

1. Ett reklamlandskap i förändring – konsumentskydd och tillsyn i en digitaliserad värld. Fi.
2. Stärkt straffrättsligt skydd för blåljusverksamhet och andra samhällsnyttiga funktioner. Ju.
3. En strategisk agenda för internationalisering. U.
4. Framtidens biobanker. S.
5. Vissa processuella frågor på socialförsäkringsområdet. S.
6. Grovt upphovsrättsbrott och grovt varumärkesbrott. Ju.
7. Försvarsmaktens långsiktiga materielbehov. Fö.
8. Kunskapsläget på kärnavfallsområdet 2018. Beslut under osäkerhet. M.
9. Ökad trygghet för studerande som blir sjuka. U.
10. Myndighetsgemensam indelning – samverkan på regional nivå. Volym 1. Myndighetsgemensam indelning – författningsändringar till följd av ny landstingsbeteckning. Volym 2. Fi.
11. Vårt gemensamma ansvar – för unga som varken arbetar eller studerar. U.
12. Uppdrag: Samverkan 2018. Många utmaningar återstår. A.
13. Finansiering av infrastruktur med skatt eller avgift? Fi.
14. Bidragsbrott och underrättelseskyldighet vid felaktiga utbetalningar från välfärdssystemen – en utvärdering. Fi.
15. Mindre aktörer i energilandskapet – genomgång av nuläget. M.
16. Vägen till självkörande fordon – introduktion. Del 1 + 2. N.
17. Med undervisningsskicklighet i centrum – ett ramverk för lärares och rektorers professionella utveckling. U.
18. Statens stöd till trossamfund i ett mångreligiöst Sverige. Ku.
19. Forska tillsammans – samverkan för lärande och förbättring. U.
20. Gräsrotsfinansiering. Fi.
21. Flexibel rehabilitering. A.
22. Ett ordnat mottagande – gemensamt ansvar för snabb etablering eller återvändande. A.
23. Konstnär – oavsett villkor? Ku.
24. Tid för utveckling. A.
25. Juridik som stöd för förvaltningens digitalisering. Fi.

Statens offentliga utredningar 2018

Systematisk förteckning