Så enkelt som möjligt för så många som möjligt

Bättre juridiska förutsättningar för samverkan och service

Betänkande av E-delegationen

Stockholm 2014

STATENS OFFENTLIGA UTREDNINGAR

SOU 2014:39

SOU och Ds kan köpas från Fritzes kundtjänst.
Beställningsadress: Fritzes kundtjänst, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: order.fritzes@nj.se
fritzes.se

För remissutsändningar av SOU och Ds svarar Fritzes Offentliga Publikationer
på uppdrag av Regeringskanslets förvaltningsavdelning.
Svara på remiss – hur och varför.
Statsrådsberedningen, SB PM 2003:3 (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/remiss.

Layout: Kommittéservice, Regeringskansliet.
Omslag: Elanders Sverige AB.
Tryck: Elanders Sverige AB, Stockholm 2014.

ISBN 978-91-38-24127-1
ISSN 0375-250X

Till statsrådet Anna-Karin Hatt

Vid regeringssammanträdet den 26 mars 2009 bemyndigade regeringen statsrådet Mats Odell att tillkalla en delegation med uppdrag att samordna myndigheternas it-baserade utvecklingsprojekt och skapa goda möjligheter för myndighetsövergripande samordning (dir. 2009:19). Delegationen fick den 25 mars 2010 ett tilläggsdirektiv (dir. 2010:32) med uppdrag om vidareutnyttjande av offentlig information och riktlinjer för myndigheters användning av sociala medier. Den 25 april 2013 fick delegationen ett tilläggsuppdrag kring it-standardisering inom vård och omsorg.

Generaldirektören Mats Sjöstrand förordnades att vara ordförande i Delegationen för e-förvaltning (Fi 2009:01) från och med den 26 mars 2009. Längst bak i detta missiv finns en förteckning över delegationens övriga ledamöter, experter samt sekretariatet. Mats Sjöstrand entledigades den 1 augusti 2011, och generaldirektören Annika Bränström förordnades samma dag till delegationens nya ordförande.

Claes Thagemark anställdes som kanslichef från och med den 7 december 2009 till och med den 1 april 2012. Cecilia Bredenwall var t.f. kanslichef under perioden 1 april 2012 till och med 11 november 2012. Ewa Carlsson anställdes som kanslichef från och med 12 november 2012.

Delegationen har antagit namnet E-delegationen.

Delegationen överlämnade den 19 oktober 2009 sitt första betänkande *Strategi för myndigheternas arbete med e-förvaltning* (SOU 2009:86). Därefter har följande betänkanden redovisats:

- Så enkelt som möjligt för så många som möjligt – från strategi till handling för e-förvaltning (SOU 2010:20)
- Så enkelt som möjligt för så många som möjligt. Under konstruktion – framtidens e-förvaltning (SOU 2010:62)

– Så enkelt som möjligt för så många som möjligt – En bit på väg (SOU 2011:27)
– Så enkelt som möjligt för så många som möjligt – vägen till effektivare e-förvaltning (SOU 2011:67)
– Så enkelt som möjligt för så många som möjligt – den mjuka infrastrukturen på väg (SOU 2012:18)
– Så enkelt som möjligt för så många som möjligt – förstärkt samordning av förvaltningsgemensamma tjänster (SOU 2012:68)
– Så enkelt som möjligt för så många som möjligt – samordning och digital samverkan (SOU 2013:22)
– Organisering av framtidens e-förvaltning (SOU 2013:75)
– Så enkelt som möjligt för så många som möjligt – it-standardisering inom socialtjänsten (SOU 2013:77)

Delegationen överlämnar härmed sitt elfte betänkande, *Så enkelt som möjligt för så många som möjligt – Bättre juridiska förutsättningar för samverkan och service* (SOU 2014:39). Betänkandet ska enligt direktiven överlämnas senast den 1 oktober 2014.

Delegationen fortsätter sitt arbete i enlighet med direktiven.

Stockholm i juni 2014

Annika Bränström

Anders Danielsson
Dan Eliasson
Ingemar Hansson
Bengt Kjellson
Claes Ljungh
Per Mosseby
Mikael Sjöberg
Katrin Westling Palm
Leif Denneberg
Christina Gellerbrant Hagberg
Björn Jordell
Helena Lindberg
Therese Mattsson
Gunilla Nordlöf
Bengt Svenson
Staffan Widlert

/Ewa Carlsson

Cecilia Bredenwall

Karolina Brogan

Johan Bålman

Lars Dannemann

Marit Dozzi

Margareta Eriksson

Viktoria Hagelstedt

Björn Hagström

Per Lannerö

Catharina Nyström

Anna Pegelow

Odd Sivertzen

Jan Sjösten

Lena Olofsson Warstrand

Förteckning över delegationens ledamöter och experter

Ordförande	**Förordnad**
Generaldirektör Annika Bränström[1]	2011-08-01
Ledamöter	
Generaldirektör Anders Danielsson	2012-04-23
Generaldirektör Leif Denneberg	2012-09-01
Generaldirektör Dan Eliasson	2009-09-01
Generaldirektör Christina Gellerbrant Hagberg	2011-03-03
Generaldirektör Ingemar Hansson	2010-04-20
Riksarkivarie Björn Jordell	2010-05-01
Generaldirektör Bengt Kjellson	2011-08-01
Generaldirektör Helena Lindberg	2009-03-26
Generaldirektör Claes Ljungh	2009-03-26
Generaltulldirektör Therese Mattsson	2011-08-15
Avdelningschef Per Mosseby	2013-01-01
Generaldirektör Gunilla Nordlöf	2013-06-01
Generaldirektör Mikael Sjöberg	2014-04-29
Rikspolischef Bengt Svenson	2009-03-26
Generaldirektör Katrin Westling Palm	2010-04-20
Generaldirektör Staffan Widlert	2009-03-26
Experter	
Lena Hägglöf	2013-10-01
Christina Henrysson	2013-10-01

Tidigare ledamöter och experter	
Generaldirektör Angeles Bermudez-Svankvist	2009-03-26 – 2013-09-03
Generaldirektör Mats Sjöstrand (ordf.)	2009-03-26 – 2011-07-31
Överdirektör Roland Höglund (expert)[2]	2009-04-14 – 2010-12-31
Projektchef Lennart Jonasson	2012-01-01 – 2012-12-31
Generaldirektör Stig Jönsson	2009-03-26 – 2011-04-30
Generaldirektör Adriana Lender	2009-03-26 – 2011-09-30
Riksarkivarie Tomas Lidman	2009-03-26 – 2010-04-30
Generaldirektör Christina Lugnet	2009-03-26 – 2012-08-09
Tf. generaldirektör Clas Olsson	2014-01-01 – 2014-04-29

[1] Annika Bränström har varit ledamot i delegationen sedan 2009-03-26, innan hon förordnades till ordförande.
[2] Roland Höglund entledigades som expert fr.o.m. den 10 maj 2010 och anställdes samma dag som kommittésekreterare. Anställningen varade till och med den 31 december 2010.

Generaldirektör Mats Persson	2009-03-26 – 2012-08-31
Generaltulldirektör Karin Starrin	2009-03-26 – 2010-12-31
Verkställande direktör Håkan Sörman	2009-03-26 – 2011-12-31
Generaldirektör Kerstin Borg Wallin	2010-04-20 – 2011-03-02
Ämnesråd Magnus Enzell (expert)	2009-04-14 – 2013-09-30
Ämnessakkunnig Anneli Hagdahl (expert)	2011-08-01 – 2013-09-30

Förteckning över delegationens sekretariat

Sekretariatet

Ewa Carlsson (Kanslichef)	2012-11-12
Cecilia Bredenwall	2011-09-01
Karolina Brogan	2012-10-01
Johan Bålman	2010-03-08
Lars Dannemann	2013-03-01
Marit Dozzi	2009-10-01
Margareta Eriksson	2013-02-15
Viktoria Hagelstedt	2014-01-02
Björn Hagström	2011-11-01
Catharina Nyström	2012-10-15
Anna Pegelow	2012-05-01
Odd Sivertzen	2013-01-07
Jan Sjösten	2012-01-01
Lena Olofsson Warstrand	2010-02-01

Tidigare anställda i sekretariatet

Homa Abdolrasouli	2012-10-01 – 2013-03-31
Maximilian Amormet[3]	2009-05-01 – 2012-08-08
Anneli Hagdahl	2010-03-01 – 2011-07-31
Mårten Janerud	2010-08-16 – 2013-10-31
Peter Krantz	2009-11-16 – 2011-11-24
Eva Sartorius	2010-01-01 – 2011-04-30
Claes Thagemark	2009-12-04 – 2012-04-01
Patrik Åkesson	2012-11-01 – 2013-03-31

[3] Tidigare Dano Kostovski.

Innehåll

Bilagor

Sammanfattning

Utkontraktering, elektroniska förvar och andra tjänster

Utkontraktering av it-drift har blivit en allt viktigare del i myndigheternas samverkan för en effektiv och väl fungerande elektronisk förvaltning. Eftersom hanteringen av tekniska hjälpmedel i många fall inte kan ske utan tillgång till specialistkompetens behövs *utkontraktering*.

Det har vidare blivit en allmänt spridd myndighetspraxis att tillhandahålla s.k. *elektroniskt förvar* – även kallat eget utrymme. Där kan den som använder en myndighets e-tjänst upprätta handlingar och i övrigt hantera information. Hanteringen ska ske så att skyddet för privatlivet upprätthålls, utan insyn från den myndighet som tillhandahåller förvaret. Myndighetens hantering av uppgifter i ett sådant förvar ska alltså vara endast teknisk.

För att myndigheters e-tjänster ska fungera väl behövs också *hjälptjänster* där tekniskt krångel eller andra svårigheter att förstå eller hantera uppgifter i e-tjänster kan avhjälpas. Slutligen har det visat sig vara angeläget att enskilda som en service ska kunna få uppgifter insamlade och sammanställda i en *presentationstjänst* så att enskilda kan få en överblick över sina engagemang.

Handlingssekretess och tystnadsplikt

Sekretess innebär inte bara en begränsning av rätten att ta del av allmänna handlingar utan även en tystnadsplikt, dvs. ett förbud för myndighetens personal att röja en uppgift, vare sig det sker muntligen, genom utlämnande av allmän handling eller på något annat sätt. Till den del en sekretessbestämmelse innebär en tystnadsplikt begränsar den yttrandefriheten för myndighetens personal.

Avgörande för behovet av handlingssekretess är om uppgifterna kan anses vara behandlade endast tekniskt – endast som led i

teknisk bearbetning eller teknisk lagring för annans räkning – så som det uttrycks i ett undantag enligt 2 kap. 10 § TF från allmän handling. Om en handling som förvaras hos en myndighet behandlas *endast* för sådant ändamål behöver det emellertid övervägas om en tystnadsplikt gäller.

För att en myndighet ska kunna utkontraktera sin it-drift till en annan myndighet behöver motsvarande sekretess gälla hos tjänsteleverantören som hos beställaren. För elektroniskt förvar tillkommer att information, som innehavaren av ett sådant förvar med fog uppfattar som sin privata, inte bör löpa risk att bli utlämnad som allmän och offentlig handling eller röjd t.ex. muntligen av den tjänstelevererande myndighetens personal.

Delegationens bedömning av frågan om handlingsoffentlighet

Handlingar som anses förvarade hos en tjänstelevererande myndighet, som tillhandahåller *it-drift* för en beställares räkning, är inte att anse som allmänna hos tjänsteleverantören, eftersom de behandlas där endast som led i teknisk bearbetning eller teknisk lagring för beställarens räkning. Enligt delegationens bedömning får detta undantag från handlingsoffentlighet anses vara tillämpligt även på handlingar som är förvarade hos en myndighet i ett *elektroniskt förvar* som myndigheten tillhandahåller åt annan.

En sekretessreglering för uppgifter som förvaras hos en tjänstelevererande myndighet behövs därmed endast i form av en tystnadsplikt för myndighetens personal, såvitt avser it-drift för annan och tillhandahållande av elektroniskt förvar.

När en myndighet tillhandahåller en hjälp- eller en presentationstjänst är situationen emellertid en annan. Tjänsten gå inte ut på att bearbeta och lagra uppgifter för annans räkning utan myndigheten tillhandahåller en tjänst i eget namn där det centrala är antingen den information som myndigheten ställer samman och visar eller den information myndigheten ger om hur ett problem kan avhjälpas eller hur vissa uppgifter bör förstås. Vid sådana förhållanden är det inte fråga om *endast* teknisk bearbetning eller teknisk lagring.

En sekretessreglering av uppgifter i en sådan tjänst behövs alltså både som en tystnadsplikt för befattningshavare och ett förbud mot att lämna ut allmänna handlingar.

Delegationens förslag

Delegationen föreslår att tystnadspliktens föremål, i verksamhet för att tillhandahålla *it-drift och elektroniskt förvar*, vidgas så att uppgift om en enskilds personliga eller ekonomiska förhållanden skyddas även om uppgiften inte är en personuppgift. Genom denna anpassning införs en tystnadsplikt även för företagsuppgifter. En sådan ändring föreslås genom att begränsningen i 40 kap. 5 § OSL till personuppgifter som avses i personuppgiftslagen (1998:204) utmönstras.

Sekretessen för uppgifter hos en myndighet som vill utkontraktera sin *it-drift* kan avse även s.k. allmänna intressen. Här avses andra uppgifter än enskilds personliga eller ekonomiska förhållanden, dvs. uppgifter som inte omfattas av sekretessen enligt 40 kap. 5 § OSL. För sådana fall finns risk för att sekretessen – och därmed tystnadsplikten – inte kommer att gälla hos den tjänstelevererande myndigheten. Det kan också vara så att uppgiften är sekretessreglerad hos båda myndigheterna men att olika skyddsnivåer kommer att gälla hos dem, t.ex. att sekretessen är absolut hos den ena myndigheten medan ett skaderekvisit gäller hos den andra myndigheten.

För att det inte ska uppkomma luckor i sekretessen för allmänna intressen endast till följd av att uppgifter behandlas tekniskt av en annan myndighet föreslår delegationen en bestämmelse om överföring av sekretessen hos den myndighet som beställer tjänsten. En sådan bestämmelse föreslås som en ny 11 kap. 4 a § OSL enligt vilken berörda sekretessbestämmelser ska vara tillämpliga även hos den mottagande myndigheten.

Delegationen föreslår vidare såväl handlingssekretess som tystnadsplikt för uppgifter om en enskilds personliga eller ekonomiska förhållanden i myndighets verksamhet för att tillhandahålla service genom *en hjälptjänst för elektroniskt förvar*. Muntlig hjälp och stöd via e-post har sedan länge getts av myndigheter utan att något särskilt behov av sekretess har ansetts föreligga.

Vad som är nytt, och kan anses ge hjälpsökande en befogad förväntning att uppgifter inte röjs, är de elektroniska förvaren. När uppgifter som en användare har i sitt elektroniska förvar överförs till en hjälptjänst – t.ex. i form av skärmbilder – behövs sekretess för att användare av elektroniskt förvar ska känna sig trygga och ta emot den hjälp som myndigheter erbjuder. En sådan bestämmelse föreslås som en ny 40 kap. 5 a § OSL enligt vilken sekretess ska

gälla i myndighets verksamhet för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar för uppgift om en enskilds personliga eller ekonomiska förhållanden. I denna del föreslås vidare att tystnadsplikten ska inskränka rätten att meddela och offentliggöra uppgifter.

Slutligen föreslår vi, som en ny 40 kap. 5 b § OSL, en bestämmelse om att sekretess ska gälla för uppgift om en enskilds personliga eller ekonomiska förhållanden i verksamhet för att presentera en sammanställning för en enskild av uppgifter som helt eller delvis har hämtats in från annan, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs. Sekretessen föreslås gälla endast om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs. Rätten att meddela och offentliggöra uppgifter bör inte inskränkas.

I betänkandet övervägs även alternativa bestämmelser. Delegationen finner emellertid att de vi lägger fram bäst balanserar effektivitet med behovet av sekretess, styrkan i sekretessregleringen och intresset av insyn.

1 Författningsförslag

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

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

dels att 40 kap. 5 och 8 §§ ska ha följande lydelse,

dels att det ska införas tre nya paragrafer, 11 kap. 4 a § och 40 kap. 5 a och 5 b §§, och tre nya rubriker närmast före 11 kap. 4 a § samt 40 kap. 5 a och 5 b §§ av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	11 kap.
	Teknisk bearbetning och teknisk lagring för annan
	4 a §
	Får en myndighet i sin verksamhet för enbart teknisk bearbetning eller teknisk lagring för en annan myndighets räkning en uppgift som av hänsyn till ett allmänt intresse är sekretessreglerad där, blir sekretessbestämmelsen tillämplig på uppgiften även hos den mottagande myndigheten.
	40 kap.
	5 §
Sekretess gäller i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon	Sekretess gäller i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon

annans räkning *av personuppgifter som avses i personuppgiftslagen (1998:204)* för uppgift om en enskilds personliga eller ekonomiska förhållanden.	annans räkning för uppgift om en enskilds personliga eller ekonomiska förhållanden.
	Hjälptjänst
	5 a §
	Sekretess gäller i myndighets verksamhet för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar för uppgift om en enskilds personliga eller ekonomiska förhållanden.
	Presentationstjänst
	5 b §
	Sekretess gäller för uppgift om en enskilds personliga eller ekonomiska förhållanden i verksamhet för att presentera en sammanställning för en enskild av uppgifter som helt eller delvis har hämtats in från annan, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs.
	8 §
Den tystnadsplikt som följer av 1, 2, 4, *och 5 §§* inskränker rätten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.	Den tystnadsplikt som följer av 1, 2, 4, *5, och 5 a* §§ inskränker rätten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Denna lag träder i kraft den 1 januari 2015.

2 Uppdraget

Vid regeringssammanträdet den 26 mars 2009 beslutade regeringen att tillkalla en delegation med uppdrag att samordna myndigheternas it-baserade utvecklingsprojekt och skapa goda möjligheter för myndighetsövergripande samordning. Delegationens uppdrag framgår av kommittédirektivet (dir. 2009:19). Delegationen antog namnet E-delegationen. En sammanställning över delegationens ledamöter, arbetsgrupp, expertgrupp, referensgrupp samt sekretariat finns på delegationens webbplats. Delegationens uppdrag sträcker sig över en längre tid och ska slutredovisas den 31 december 2014. Delbetänkanden ska under mellantiden lämnas två gånger per år, 20 mars och 1 oktober.

Delegationen delredovisade sitt uppdrag för första gången i oktober 2009 i betänkandet Strategi för myndigheternas arbete med e-förvaltning (SOU 2009:86). En remissammanställning (Fi2009/6838) finns publicerad på delegationens webbplats. I mars 2010 redovisades delegationens andra betänkande Så enkelt som möjligt för så många som möjligt – från strategi till handling för e förvaltning (SOU 2010:20). Den 25 mars 2010 fick delegationen ett tilläggsdirektiv (dir. 2010:32), som omfattar främjande och samordning av myndigheternas arbete med att förbättra förutsättningarna för vidareutnyttjande av offentlig information (PSI direktivet), samt att ta fram riktlinjer för myndigheters användning av sociala medier. Den 25 april 2013 fick delegationen ett tilläggsdirektiv (dir. 2013:40), som omfattar en behovsinventering beträffande standarder inom socialtjänstens område samt angränsande områden inom hälso- och sjukvård inom ramen för regeringens överenskommelse med Sveriges Kommuner och Landsting om stöd till en evidensbaserad praktik för god kvalitet inom socialtjänsten. I oktober 2010 lämnade delegationen sin tredje delredovisning, Så enkelt som möjligt för så många som möjligt Under konstruktion – framtidens e-förvaltning (SOU 2010:62) och i mars 2011 den fjärde

delredovisningen, Så enkelt som möjligt för så många som möjligt – en bit på väg (SOU 2011:27). I oktober 2011 lämnades det femte betänkandet, Så enkelt som möjligt för så många som möjligt – vägen till effektivare e-förvaltning (SOU 2011:67). I mars 2012 överlämnades det sjätte betänkandet, Så enkelt som möjligt för så många som möjligt – den mjuka infrastrukturen på väg (SOU 2012:18). I oktober 2012 överlämnades det sjunde betänkandet, Så enkelt som möjligt för så många som möjligt – förstärkt samordning av förvaltningsgemensamma tjänster (SOU 2012:68). I mars 2013 överlämnades det åttonde betänkandet, Så enkelt som möjligt för så många som möjligt – samordning och digital samverkan (SOU 2013:22).

I oktober 2013 överlämnades det nionde betänkandet, Organisering av framtidens e-förvaltning (SOU 2013:75). Betänkandet avsåg uppdraget att föreslå hur E-delegationens arbete kan föras vidare i ett längre perspektiv. Förslaget skulle enligt direktiven lämnas senast den 20 mars 2014. Skälet till ett tidigareläggande är att E-delegationen på detta sätt vill ge regeringen tillräckligt med tid, under förutsättningen att delegationens arbete ska fortsätta i någon form, att föra över pågående verksamhet i den nya formen utan att det uppstår ett glapp. I december 2013 redovisades betänkandet Så enkelt som möjligt för så många som möjligt – it-standardisering inom socialtjänsten (SOU 2013:77), som är en särredovisning utifrån tilläggsuppdraget kring it-standardisering inom vård och omsorg (dir. 2013:40).

Detta betänkande, Så enkelt som möjligt för så många som möjligt – Bättre juridiska förutsättningar för samverkan och service (SOU 2014:39), innehåller delegationens elfte delredovisning av uppdraget.

Delegationen ska i enlighet med sina direktiv redovisa till regeringen om den i sitt arbete identifierar regelverk som på ett olämpligt sätt hindrar elektroniskt informationsutbyte. Vid behov ska delegationen lämna förslag till författningsändringar.

Betänkandet innehåller förslag som syftar till att utkontraktering, s.k. outsourcing, mellan myndigheter, elektroniskt förvar som myndigheter tillhandahåller åt enskilda samt hjälp och presentationstjänster som myndigheter inrättar ska kunna bedrivas utan att enskildas information, som de med fog uppfattar som sin privata, ska löpa risk att bli utlämnad som allmän och offentlig handling. En central del i förslagen är en tystnadsplikt för befattningshavare som endast har en teknisk uppgift.

I betänkandet lämnas förslag till ändringar i 11 och 40 kap. offentlighets- och sekretesslagen (2009:400).

Genom dessa ändringar anpassas reglerna till den utveckling som har ägt rum inom offentlig förvaltning.

Lagändringarna är avsedda att träda i kraft den 1 januari 2015.

3 It-baserade tjänster

3.1 Den pappersbaserade hanteringen

När enskilda kommunicerar med offentlig förvaltning brukar pappershandlingar sändas via post eller ges in vid personligt besök hos en myndighet. Det ”gränssnitt” som möter enskilda har byggt på pappersbaserade handlingar som utväxlas för att t.ex. initiera ärenden, förelägga den som anhängiggjort ett ärende att komplettera sina uppgifter eller att underrätta parter och andra om myndighetens beslut. I denna miljö upprättar den enskilde sina handlingar på papper, ”off-line” med full kontroll över materialet, som inte anses inkommet till myndighet när det befinner sig på en plats som myndigheten saknar tillträde till och inte heller på annat sätt förfogar över.

En pappershandling behöver inte heller anses inkommen till myndighet för att den har kommit in i myndighetens lokaler, om det är så att närvaron där beror på att en besökare t.ex. har burit med sig handlingen i sin väska och därefter gått ut från myndigheten utan att ge in handlingen. Inte ens när en besökare har visat en halvt ifylld ansökan för en befattningshavare som gett den enskilde hjälp som en service från myndigheten har handlingen ansetts inkommen, om den enskilde gått därifrån utan att ge in sin ansökan.

Denna syn på material som fysiskt innehas av enskild eller som myndigheten annars inte får förfoga över, för att den enskilde inte lämnat det ifrån sig, har ansetts så självklar att den knappt berörts i doktrinen. På motsvarande sätt är det genom traditionella fysiska gränser tydligt hur olika förvaltningsmyndigheter avgränsas från varandra och hur enskildas åtgärder och vad enskilda innehar skiljs från en myndighets åtgärder och dokument.

Särskilda tjänster har införts för att myndigheter med en väl anpassad organisation och på ett effektivt sätt ska kunna uppfylla sin

serviceskyldighet enligt förvaltningslagen. Genom dessa tjänster lämnas upplysningar, vägledning, råd och annan sådan hjälp till enskilda i en omfattning som ofta går längre än den skyldighet som följer av 4 och 5 §§ förvaltningslagen (1986:223).

3.2 Tjänster i elektronisk miljö

När elektroniska rutiner används för att kommunicera blir gränserna inte lika tydliga mellan de miljöer som respektive organisation svarar för. Från ett traditionellt fysiskt betraktelsesätt och med den utformning som användargränssnitt ofta har kan ett elektroniskt ”utrymme” eller ”förvar” som en myndighet tillhandahåller åt en enskild (användare) lätt uppfattas som en integrerad del av myndighetens it-miljö.

Denna risk för sammanblandning mildras inte av att det numera är vanligt att myndigheter delar med sig av eller tillhandahåller it-baserade funktioner åt andra myndigheter; se t.ex. Statens servicecenter, projektet Verksamt och tjänster som övervägs för att myndigheter ska ta i bruk uppgifter från andra myndighet för förvaltningsgemensam nytta. Det har således blivit vanligt att en myndighet behandlar uppgifter för en annan myndighets räkning genom utkontraktering; även kallad outsourcing eller it-drift. Sådan behandling hos en myndighet för en annan myndighets räkning kan allmänt avse it-drift men det kan också vara fråga om speciella funktioner eller viss infrastruktur som regeringen har funnit det lämplig att ett visst offentligt organ utvecklar och tillhandahåller.

För att motverka risken för sammanblandning mellan olika aktörers it-miljöer och ansvarsområden har särskilda användargränssnitt, föreskrifter och avtal införts för att tydliggöra gränser mellan en myndighets

- verksamhetssystem, där behandlingar sker för myndighetens egen räkning, till skillnad från
- produktion och leverans av funktioner som myndigheten tillhandahåller i form av it-baserade tjänster,
  - *antingen* inom sitt eget verksamhetsområde, till sina egna sökande,
  - *eller* åt andra myndigheter eller enskilda för att de ska kunna använda eller tillhandahålla tekniska funktioner åt andra.

Med verksamhetssystem menas här en it-miljö där en organisation och dess befattningshavare handlägger ärenden eller annars hanterar nyttoinformation för organisationens räkning. Nyttoinformation står här för uppgifter som är till för enskilda eller befattningshavare till skillnad från drift- och säkerhetsrelaterad information som endast är till för tekniker; se E-delegationens juridiska vägledning för verksamhetsutveckling inom e-förvaltningen (version 1.0), beslutad av E-delegationen den 8 juli 2013.[4]

Myndigheter har sedan länge *inom sitt eget verksamhetsområde* tillhandahållit s.k. *ärendetjänster*, som brukas av enskilda i elektronisk miljö för att utforma utkast till handlingar och – när utkasten är färdiga – ge in dem till den myndighet som tillhandahåller ärendetjänsten. Med *ärendetjänst* menas, enligt den nämnda vägledningen, en e-tjänst där användare i ett serviceskede och i ett eget utrymme, kan (1) utforma handlingar för att ge in dem, och (2) i vissa sådana tjänster få uppgifter eller handlingar förifyllda eller annars utlämnade av (i) den som tillhandahåller utrymmet, eller (ii) ett annat organ, med stöd av en bastjänst (s.k. egen hämtning).

En användare kan i vissa ärendetjänster få en uppgift eller en handling utlämnad till sig av myndighet så att användaren delvis endast behöver granska att det som därefter ges in är riktigt; jfr en förtryckt deklarationsblankett. När användaren är klar behöver han eller hon endast skriva under elektroniskt – eller legitimera sig för uppgiftslämnande – samt klicka på ”skicka” för att en överföring ska ske till myndighetens funktion för att motta och ankomstregistrera sådana handlingar, ett s.k. anvisat elektroniskt mottagningsställe.[5]

Till detta kommer nya elektroniska tjänster. Hit hör dels tjänster för att hjälpa användaren när en it-baserad tjänst inte fungerar för denne (s.k. *hjälptjänster,* eng. helpdesk), dels tjänster för att enskilda ska kunna få uppgifter eller handlingar från ett eller flera organ visade, efter att uppgifterna eller handlingarna har kommit in

[4] Här bör även noteras att tre skilda miljöer, enligt betänkandet Säkerhetskopiors rättsliga status, kan identifieras i en myndighets it-system, dels *verksamhetsmiljön,* som utgör den del av myndighetens it-miljö där den vanlige datoranvändaren (befattningshavaren) befinner sig, där *nyttoinformation* finns i form av ”originalhandlingar”, dels *driftmiljön* som innehåller information som har betydelse för driften av systemet, dels *säkerhetskopiemiljön,* som endast har till syfte att garantera verksamhets- och driftmiljöns existens. I säkerhetskopiemiljön finns bl.a. ”kopior” av både allmänna och icke allmänna handlingar från verksamhetsmiljön samt diverse information från driftmiljön (prop. 2009/10:58, bilaga 1, s. 40).

[5] Jfr Förvaltningslagsutredningens betänkande (SOU 2010:29) En ny förvaltningslag, 18 §, s. 40.

till och blivit allmän handling hos den som tillhandahåller tjänsten (s.k. *presentationstjänster*)[6].

E-delegationen har verkat för att presentationstjänster ska utvecklas så att enskilda elektroniskt ska kunna få vissa typer av information samlad och visad. Exempelvis har lösningar tagits fram för att en enskild ska kunna få en översikt över sina mottagna och lämnade fullmakter (Mina fullmakter) och över sina ärenden hos myndigheter (Min ärendeöversikt). En myndighet som tillhandahåller en sådan tjänst kan på olika sätt hämta in material som finns hos andra organ – efter en visningsbegäran från en användare av en presentationstjänst. Sådan insamling kan ske momentant, direkt från de organ som har det begärda underlaget, men det kan också ske genom insamling på förhand, antingen till den myndighet som tillhandahåller presentationstjänsten eller till en annan myndighet som ges i uppdrag att förvara dessa handlingar.[7]

Den insamling som sker leder till att handlingar kommer in till myndigheten och därmed blir allmänna handlingar. Eftersom enskilda inte vill använda en presentationstjänst om den leder till att var och en kan få ut uppgifterna under åberopande av reglerna om handlingsoffentlighet, gallrar myndigheten – när så får ske – de insamlade uppgifterna snarast efter att de har presenterats för användaren. Sker sådan gallringen genast blir sannolikheten i praktiken försumbar för att uppgifterna lämnas ut som allmän handling.[8]

Det förekommer också att upplysningar, vägledning och annan hjälp lämnas av en befattningshavare genom en *hjälptjänst*, t.ex. när en e-tjänst inte fungerar och användaren behöver få tala med någon hos en myndighet som kan hjälpa till att lösa problemet. I andra fall ges hjälp för att användare ska kunna förstå vissa uppgifter eller ställa samman dem på lämpligt sätt. Dessa hjälptjänster går längre än ren presentation av visst material och det är ofta en förutsättning för att en sådan tjänst ska bli verkningsfull att den enskilde

[6] Definierad i E-delegationens juridiska vägledning för verksamhetsutveckling inom e-förvaltningen som en e-tjänst där en enskild kan få uppgifter eller handlingar från flera organ visade, efter att uppgifterna eller handlingarna har kommit in till den som tillhandahåller tjänsten, utan att det som visas blir tillgängligt för annan.

[7] En insamling till en annan myndighet än den som tillhandahåller presentationstjänsten kan aktualiseras t.ex. för att det under den tid förvaringen sker ska kunna säkerställas att handlingarna förvaras endast som led i teknisk bearbetning eller teknisk lagring för annans räkning (2 kap. 10 § första stycket TF).

[8] Den behandling som myndigheten utför är från rättslig utgångspunkt knuten till myndighetens presentationstjänst så att teknisk bearbetning och lagring som myndigheten utför inte kan sägas ske endast för ändamål som avses i 2 kap. 10 § första stycket TF. Myndigheten behandlar uppgifterna även för att kunna tillhandahålla en service åt användaren.

lämnar viss information till en befattningshavare. De uppgifter som användaren kan behöva lämna eller bidra till att visa upp blir dock att anse som inkomna enligt tryckfrihetsförordningen och därmed allmän handling hos den myndighet där befattningshavaren är verksam. Samtidigt utgår användarna normalt från att uppgifterna inte kommer till utomståendes kännedom. Här pågår en utveckling för att kunna effektivisera hjälparbetet, t.ex. så att den som ger hjälp ska kunna se den hjälpsökandes skärmbild och kanske till och med styra dennes dator.[9]

3.3 Elektroniskt förvar – ett eget utrymme

För att det ska bli praktiskt möjligt för dem som använder en myndighets elektroniska tjänster att upprätta utkast och vidta andra åtgärder utan att materialet anses vara inkommet till myndighet redan i detta förberedande skede behöver myndigheten tillhandahålla ett ”utrymme” eller ett ”förvar” som är endast användarens. Ett sådant ”utrymme” kan emellertid komma att uppfattas som en integrerad del av myndighetens verksamhetssystem och den nyttoinformation (jfr vid not 4) som myndigheten behandlar där för sin egen räkning. Denna risk för sammanblandning finns i vart fall när tjänster och funktioner har utformats så att det är svårt att se eller annars uppfatta de gränser som är avsedda. ”Utrymmet” finns visserligen i en myndighets it-miljö men användaren utgår från att det som finns där är användarens eget material och att myndigheten varken tar del av det eller röjer det som finns där för någon annan.[10]

Av detta skäl har det bland myndigheter som tillhandahåller ärendetjänster utvecklats en it-arkitektur samt en terminologi för att närmare beskriva de virtuella ”utrymmen” eller ”förvar” som myndigheter tillhandahåller åt sina användare av elektroniska

[9] Detta reser ett antal frågor om bl.a. persondataskydd och informationssäkerhet som är av central betydelse för e-förvaltningen. Det finns emellertid här inte utrymme för en närmare genomgång av dessa frågor. Medvetenheten framstår dock som begränsad om riskerna från informationssäkerhetssynpunkt och om de juridiska konsekvenser som kan följa med en hjälptjänst som har beskriven funktionalitet. Något samordnat arbete har inte bedrivits kring hur hjälptjänster bör utformas. Utvecklingsarbetet bedrivits lokalt utan enhetlig utformning.

[10] Jfr om ett utkast till en ännu inte undertecknad och färdigställd årsredovisning för ett börsbolag, som tagits fram i Bolagsverkets ärendetjänst för årsredovisning, hade blivit allmän och offentlig handling innan den getts in eller att andra av enskilda i myndigheters elektroniska tjänster halvt ifyllda elektroniska blanketter och liknande skulle kunna begäras ut som allmän handling av var och en.

tjänster. Alternativet hade varit att låta användaren enbart i sin dator upprätta och ge in handlingen, utan sådan hjälp som en myndighet kan ge genom en e-tjänst; jfr att sitta hemma utan hjälp med att besöka en myndighet och ställa frågor när en pappershandling upprättas.

E-delegationen har i grundutförande kallat ett sådant virtuellt ”utrymme” eller ”förvar” för användarens *”eget utrymme”* och definierat detta som ett förvar som myndigheten tillhandahåller åt en användare endast som led i teknisk bearbetning eller teknisk lagring för användarens räkning. Ett sådant ”utrymme” finns endast en kort stund under en viss session, som vanligtvis avslutas med att en där upprättad handling ges in eller att det som behandlats där tas bort så att användaren därefter får börja om på nytt.[11] I vissa ärendetjänster kan användaren emellertid mellanlagra sina handlingar i ett eget utrymme, så att användaren senare kan hämta upp dem och fortsätta sitt arbete. Användarens ”eget utrymme” betecknas då *”konto”*.[12] Till detta kommer konto för säker elektronisk post, en *”e-brevlåda”;* dvs. ett konto där säker elektronisk post kan levereras.

”Eget utrymme” har därmed blivit ett vedertaget juridiskt synsätt inom offentlig förvaltning som med utgångspunkt i gällande rätt tillämpas på vissa elektroniska företeelser. ”Utrymmet” brukas av användaren under den närmast självklara förutsättningen att ingen annan – inte ens den myndighet som tillhandahåller ”utrymmet” – får bereda sig tillgång till de uppgifter och handlingar som finns där. Myndigheten ska inte heller på annat sätt röja de uppgifter och handlingar som finns där; jfr en servicebyrås roll vid outsourcing.[13] En del i detta är myndighetsinterna regler som förbjuder befattningshavare, hos den myndighet som tillhandahåller det egna utrymmet, att bereda sig tillgång till en användares ”eget utrymme” eller att ta del av information som finns där. Som undantag brukar endast anges sådan åtkomst som är nödvändig för att rätta tekniska fel eller att tillgodose informationssäkerheten.

[11] Se vidare E-delegationens juridiska vägledning för verksamhetsutveckling inom e-förvaltningen.
[12] *Konto* definieras i E-delegationens vägledning som eget utrymme som har registrerats för en viss fysisk eller juridisk person, så att denne permanent (persistent) kan bevara och i övrigt behandla uppgifter där (termen persistent används av teknikansvariga).
[13] En myndighet får visserligen inte utan bemyndigande erbjuda tjänster som faller utanför myndighetsuppdraget men det är en annan fråga som inte behandlas här.

I praktiken innebär detta att det vid straffansvar är förbjudet för befattningshavare att i strid med de myndighetsinterna reglerna bereda sig tillgång till en användares ”eget utrymme” eller att annars ta del av information som finns där. Detta gäller oberoende av om samma uppgift eller handling finns tillgänglig för befattningshavaren någon annanstans, t.ex. i myndighetens verksamhetssystem för ärendehandläggning.

Inledningsvis växte denna it-arkitektur fram för att skilja handlingar som är inkomna enligt 10 § förvaltningslagen från användares eget arbetsmaterial och för att få till stånd motsvarande fördelning som i pappersmiljö av risken för att en handling försenas, förvanskas eller inte kommer fram. Analysen av de rättsliga förutsättningarna för att hantera uppgifter i ett ”eget utrymme” har emellertid fortgått så att sådana utrymmen numera också brukar beskrivas med utgångspunkt från bestämmelserna om allmänna handlingars offentlighet. En användare skulle som framgått knappast godta ett utrymme där hans eller hennes handlingar blir offentliga.

Vid bedömningen av om en handling i ett ”eget utrymme” är allmän blir ett undantag som föreskrivs i 2 kap. 10 § tryckfrihetsförordningen, förkortad TF, av särskilt intresse. Där sägs att handling som förvaras hos en myndighet endast som led i teknisk bearbetning eller teknisk lagring för annans räkning inte anses som allmän handling hos den myndigheten.[14]

Den hantering som i praktiken äger rum när en användare brukar en ärendetjänst har utifrån detta undantag beskrivits, i E-delegationens juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, så att användarens uppgifter behandlas i

- *ett serviceskede,* dvs. ett förlopp där service ges av en myndighet enligt 4 § förvaltningslagen, förkortad FL, ärendehandläggning inte äger rum, endast den enskilde ges insyn och en handling inte har kommit in till myndigheten enligt 10 § FL, och
- *ett eget utrymme* som är användarens, dvs. ett skyddat förvar som myndigheten enligt 2 kap. 10 § TF tillhandahåller endast som led i teknisk bearbetning eller teknisk lagring för annans räkning.

[14] Se även 2 kap. 6 § tredje stycket tryckfrihetsförordningen, där det föreskrivs att åtgärd som någon vidtager endast som led i teknisk bearbetning eller teknisk lagring av handling, som myndighet har tillhandahållit, inte ska anses leda till att handling är inkommen till den myndigheten.

Myndigheter som tillhandahåller sådana utrymmen har bedömt att de uppgifter och handlingar som innehavaren har där – nyttoinformationen – så länge den finns endast i den enskildes ”eget utrymme”, inte anses vara inkommen till myndigheten enligt förvaltningslagen eller allmän handling där. Som sin egen ser däremot myndigheten den drift- och säkerhetsrelaterade information som behandlas för att kunna tillhandahålla ”eget utrymme”.

Beträffande frågan om personuppgiftsansvar för ”eget utrymme” har, i E-delegationens juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, noterats att en myndighet som tillhandahåller sådant utrymme åt en användare blir personuppgiftsansvarig för den drift- och säkerhetsrelaterade information som avser användarens ”eget utrymme” och i övrigt för att de personuppgifter som behandlas i utrymmet är omgärdade av adekvata säkerhetsåtgärder. För den nyttoinformation som den enskilde behandlar i sitt utrymme anges emellertid myndigheten inte blir personuppgiftsansvarig. Denna bedömning anges gälla även när utrymmet är utformat som ett konto eller en e-brevlåda.

För att beteckna de ”utrymmen” eller ”förvar” som beskrivits har olika uttryck använts samtidigt som beskrivningarna har varierat beroende på för vilket ändamål de har tillkommit, se vidare den beskrivning som ges i *bilaga 4.*

Delegationen har valt att knyta an till den terminologi som används i gällande rätt. Därför används i det följande begreppet *förvar;* jfr bestämmelsen i 4 kap. 8 § brottsbalken om straffansvar för intrång i förvar. För att tydliggöra att det är fråga om ett virtuellt förvar i it-miljö har delegationen valt att använda uttrycket *elektroniskt förvar.*[15]

3.4 It-drift och andra tjänster

Under arbetet med att kartlägga elektroniskt förvar har även annan hantering som beskrivs med uttryck som utkontraktering, outsourcing eller it-drift visat sig vara i behov av en juridisk översyn. Det är visserligen inget nytt att material överlämnas till en myndighet endast för teknisk bearbetning och teknisk lagring, men omfattningen av denna hantering har blivit en helt annan än vad som förutsågs när reglerna infördes i 2 kap. 10 § TF och 9 kap. 7 § sekretesslagen

[15] Angående elektroniskt förvar hos annan än myndighet, se avsnitt 6.3.6.

(1980:100), numera 40 kap. 5 § offentlighets- och sekretesslagen (2009:400), förkortad OSL. I motiven till dessa bestämmelser nämns sådana exempel som att en myndighet lämnar ljudupptagningar på magnetband för redigering eller pappershandlingar för överföring till maskinläsbart medium.

Utvecklingen har emellertid gått i en annan riktning. Hela it-miljöer tillhandahålls numera av aktörer som har specialiserat sig på sådana tjänster (i det följande *it-drift*). Det har också blivit vanligt att komplexa tekniska och administrativa funktioner tillhandahålls via nät, t.ex. elektroniska brevlådor. Så kallade molntjänster har ytterligare accentuerat behovet av att på ett fungerande sätt inordna it-drift och annan utkontraktering under gällande rätt.

Samtidigt har myndigheter utvecklat sin samverkan på området och i allt högre grad börjat dela med sig av eller tillhandahålla it-baserade funktioner åt myndigheter och enskilda. Statens servicecenter och projektet Verksamt har redan nämnts. Andra exempel är Skatteverkets uppdrag rörande säker elektronisk post och E-legitimationsnämndens uppdrag beträffande säkerhetsinfrastruktur för legitimering och underskrift i elektronisk miljö. Det är alltså inte bara fråga om samverkan rörande it-drift. I praktiken tillhandahålls också specialiserade funktioner och infrastrukturer som regeringen har funnit lämplig att låta myndigheter utveckla och tillhandahålla.

3.5 Behovet av juridisk genomlysning

Vår genomlysning av området har tagit sin utgångspunkt i de frågor som uppkommit till följd av den alltmer spridda användningen av elektroniskt förvar. Det har emellertid visat sig att olika situationer aktualiseras; dels *ren it-drift* när en myndighet tillhandahåller en sådan tjänst åt en *annan myndighet,* dels *specialiserade funktioner* som myndigheter kan behöva tillhandahålla åt *enskilda* för att den elektroniska förvaltningen ska kunna fungera i enlighet med regeringens förvaltningspolitiska strävanden. De specialiserade funktioner delegationen har övervägt utgörs dels av *elektroniskt förvar,* dels av *hjälptjänster och presentationstjänster*.

Myndigheter har vid sin rättstillämpning utgått från att undantaget från handlingsoffentlighet, vid hantering som sker endast som led i teknisk bearbetning eller teknisk lagring för annans räkning, är tillämpligt både vid ren it-drift och i elektroniskt förvar samt att

sekretessregleringen är tillräcklig både vid ren it-drift och för att tillhandahålla elektroniskt förvar. Vid vår genomlysning har det emellertid visat sig

- *dels* att sekretessregleringen, särskilt vid beaktande av behovet av tystnadsplikt, framstår som otillräcklig för
  - ren it-drift,
  - elektroniskt förvar, och
  - hjälptjänster och presentationstjänster,
- *dels* att det har ifrågasatts om tillämpningsområdet för undantaget från handlingsoffentlighet vid endast teknisk bearbetning eller teknisk lagring för annans räkning omfattar en handling i ett elektroniskt förvar,
- *dels* att beskrivna tjänster, om de utkontrakteras till ett enskilt organ[16], kan omfattas av en total tystnadsplikt där genom avtal.

Frågan är därmed om samverkan mellan myndigheter ska kunna äga rum genom utkontraktering eller om privaträttsliga aktörer måste anlitas för att det skydd för uppgifterna som myndigheter och användare av e-tjänster hittills har förutsatt ska kunna upprätthållas.

Vid denna bedömning av beskrivna tjänster blir det av avgörande betydelse om undantaget enligt 2 kap. 10 § första stycket TF från handlingsoffentlighet vid teknisk bearbetning och teknisk lagring för annans räkning kan bli tillämpligt eller om en sekretessreglering behövs, inte bara för att en tystnadsplikt ska gälla för befattningshavare hos den myndighet som tillhandahåller en tjänst för it-drift eller annan utkontraktering utan också för att ett förbud ska gälla mot att lämna ut allmänna handlingar.

[16] Här förutsätts att det är en sådan privaträttslig aktör som vid tillämpningen av offentlighets- och sekretesslagen inte jämställs med en myndighet.

4 Allmän handling

4.1 Regleringen

Enligt 2 kap. 1 § TF ska varje svensk medborgare ha rätt att ta del av allmänna handlingar. Samma rätt har enligt 14 kap. 5 § TF utländska medborgare förutsatt att rätten inte har begränsats i lag. Någon sådan begränsning har inte gjorts.

Förutsättningarna blir vid utkontraktering delvis olika om det är en myndighet eller ett företag som tillhandahåller tjänsten. Reglerna om handlingsoffentlighet gäller endast för myndigheter.[17] En handling kan vidare begäras ut hos en myndighet även om den inte finns tekniskt lagrad där. Det räcker att handlingen är tillgänglig för myndigheten.

Med handling menas enligt 2 kap. 3 § TF dels framställning i skrift eller bild (konventionell handling), dels upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel (här elektronisk handling). De elektroniska handlingarna delas in i färdiga handlingar (här färdig elektronisk handling) respektive sammanställningar av uppgifter ur en upptagning för automatiserad behandling (här potentiell elektronisk handling).

En handling är allmän om den förvaras hos myndighet och enligt 2 kap. 6 eller 7 § TF är att anse som inkommen till eller upprättad hos myndighet. Rekvisitet förvarad regleras särskilt för elektroniska handlingar. En sådan handling anses förvarad 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 (2 kap. 3 §

[17] Jfr dock sådana aktiebolag, handelsbolag, ekonomiska föreningar och stiftelser där kommuner eller landsting utövar visst slag av inflytande samt de organ som upptas i en bilaga till offentlighets- och sekretesslagen, vilka enligt 2 kap. 3 och 4 §§ OSL ska jämställas med myndigheter vid tillämpningen av vad som föreskrivs i tryckfrihetsförordningen om rätt att ta del av handlingar hos myndighet.

andra stycket TF). För sammanställningar av uppgifter ur en upptagning för automatiserad behandling som utgör allmän handling – dvs. potentiella elektroniska handlingar – gäller dessutom ett särskilt tillgänglighetsrekvisit som innebär att en sammanställning anses förvarad (och inkommen) endast om myndigheten kan göra sammanställningen tillgänglig med rutinbetonade åtgärder.

Till detta kommer den s.k. begränsningsregeln i 2 kap. 3 § tredje stycket TF av vilken följer att en sammanställning av uppgifter ur en upptagning för automatiserad behandling inte anses förvarad om sammanställningen innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra sammanställningen tillgänglig. Även begränsningsregeln är alltså tillämplig endast med avseende på potentiella elektroniska handlingar och den har även i övrigt ett smalt tillämpningsområde.

4.2 Särskilt om elektronisk åtkomst

Av 2 kap. 6 § TF följer att en elektronisk handling anses inkommen till myndighet redan när annan har gjort den tillgänglig för myndigheten på sätt som anges i 3 § andra stycket. Rekvisiten förvarad och inkommen har alltså samordnats i it-miljö.

En rättslig komplikation när en myndighet ges elektronisk åtkomst till uppgifter, t.ex. vid utkontraktering eller i en hjälptjänst, är att sådan åtkomst kan leda till att alla elektroniska handlingar som myndigheten kan nå blir att anse som allmänna handlingar hos den myndighet som har möjlighet att nå uppgifterna. Om en myndighet ges tillträde till någon annans it-miljö för att tillhandahålla it-drift eller att kunna ge användare hjälp och stöd vid användning av datorer – så att myndigheten kan ta del av uppgifter eller handlingar i den andres it-miljö och göra dem läsbara – anses de färdiga och potentiella elektroniska handlingar som blir tillgängliga vara allmänna handlingar hos den myndighet som getts sådan åtkomst.[18]

[18] Detta gäller även när myndigheten varken har läst eller på annat sätt hämtat handlingen till sin it-miljö. En beskrivning av dessa frågor ges bl.a. i regeringens proposition 2007/08:160 Utökat elektroniskt informationsutbyte, där regeringen fann att ändamålsbegränsningar inte kan utgöra sådana rättsliga begränsningar som avses i 2 kap. 3 § andra stycket TF; dvs. att de inte omfattas av den s.k. begränsningsregeln. En närmare genomgång av de komplikationer detta kan föra med sig finns i Informationshanteringsutredningens delbetänkande Överskottsinformation vid direktåtkomst (SOU 2012:90).

Färdiga elektroniska handlingar blir därmed vid direkt åtkomst, t.ex. för it-drift eller i en hjälpfunktion hos en myndighet, att anse som inkomna hos den myndighet som tillhandahåller tjänsten, oberoende av om åtgärderna är rutinbetonade. Även potentiella elektroniska handlingar blir att anse som inkomna vid direkt åtkomst hos en myndighet som ges tillgång till dem, om de kan sammanställas med rutinbetonade åtgärder.

Vid denna bedömning blir det alltså utan betydelse om en enskilds begäran om att få en allmän handling utlämnad avser en (färdig eller en potentiell) elektronisk handling som genererats i myndighetens egen verksamhet eller en färdig elektronisk handling som anses inkommen t.ex. till följd av att myndigheten inom ramen för en utkontraktering eller en hjälpfunktion har direkt åtkomst till en annan myndighets, ett företags eller en enskild persons elektroniska information. En (möjlig) sammanställning av uppgifter som någon gör tekniskt tillgänglig för en myndighet genom direkt åtkomst anses således vara förvarad och inkommen hos den myndighet som ges åtkomst, och således allmän handling där.

Detta gäller även om åtkomsten i praktiken ska vara begränsad till t.ex. befattningshavare vid en teknisk funktion för utkontraktering eller en hjälpfunktion och det gäller inte bara för färdiga elektroniska handlingar utan även för t.ex. sammanställningar ur färdiga handlingar som kan göras tillgängliga med rutinbetonade åtgärder och utan användning av förbjudna sökbegrepp. Olika register, t.ex. loggar, omfattas också.

Införs *tekniska begränsningar,* som innebär att den elektroniska handlingen inte är tillgänglig för den myndighet som tillhandahåller it-drift eller en hjälpfunktion, med tekniskt hjälpmedel som myndigheten själv utnyttjar, blir handlingen däremot inte att anse som allmän. I så fall kan hinder emellertid uppkomma i den tekniska hanteringen av tjänsten och handlingen kan inte heller användas av myndigheten i en hjälpfunktion.

Till detta kommer att det – för att undgå handlingsoffentlighet – inte räcker att åtkomsten är teknisk begränsad *för handläggare* vid en hjälpfunktion eller den som administrerar en funktion för utkontraktering. Enligt regeringens proposition 2007/08:160 Utökat elektroniskt informationsutbyte, är det tillräckligt att det finns någon person, t.ex. på teknikavdelningen, som har tekniska möjligheter att överföra uppgifterna till läsbar form (s. 71).

I praktiken torde detta, med dagens it-verktyg, innebära att det är svårt att tänka sig tekniska begränsningar, för befattningshavare,

som inte enkelt kan kringgås av personal som arbetar med driften eller skyddet av berört informationssystem. Skulle det införas en teknisk begränsning hos en myndighet som tillhandahåller t.ex. it-drift eller en hjälpfunktion, så att befattningshavare endast kan söka på uppgifter som rör en viss person som är berörd i det enskilda fallet, gäller denna begränsning inte när en enskild under åberopande av handlingsoffentligheten begär att få ut en elektronisk handling, om någon vid myndigheten, t.ex. en tekniker kan ta fram handlingen i läsbar form med rutinbetonade åtgärder.

4.3 Undantag

Ett sätt att tillgodose en förväntan på att handlingar inte ska bli att anse som allmänna hos den som tillhandahåller en tjänst för teknisk bearbetning och teknisk lagring är att endast låta *privaträttsliga* subjekt tillhandahålla sådana tjänster. Ett annat sätt kan vara att införa en absolut *teknisk begränsning* av den åtkomst till elektroniska handlingar som en myndighet som tillhandahåller en tjänst ges. En sådan teknisk begränsning kan emellertid komplicera administrationen av tjänsten och därmed bli kostnadsdrivande.[19]

För den som endast tar del av lagtexten kan det också förefalla som om en rättslig begränsning enligt 2 kap. 3 § tredje stycket TF skulle kunna bli tillämplig, om begränsningen föreskrivs i lag eller förordning. Detta undantag gäller emellertid bara för potentiella elektroniska handlingar – alltså inte när det är fråga om en färdig elektronisk handling. Undantaget gäller dessutom endast om den potentiella elektroniska handlingen innehåller personuppgifter och

[19] Här bör också noteras att en teknisk begränsning som sätts upp i myndighetens egen it-miljö knappast räcker för att allmänna handlingar inte ska uppkomma. En sådan begränsning är avhängig av att myndigheten inte beslutar att ge sina tekniker i uppdrag att ta bort den; en åtgärd som inom ramen för dagens flexibla it-system kan antas vara möjlig att genomföra med åtgärder som i tryckfrihetsförordningens mening ses som rutinbetonade. Eftersom informationen därvid i princip är tillgänglig för myndigheten när den så önskar är det osannolikt att den tekniska begränsningen får verkan med avseende på tillgänglighetsrekvisitet i 2 kap. 3 § andra stycket TF. – För att en myndighets tillgång till information på ett säkert sätt ska begränsas så att informationen inte anses tillgänglig i 2 kap. TF:s mening kan denna tillgång dock göras beroende av en yttre omständighet som myndigheten inte själv kan påverka, t.ex. att begränsa åtkomsten tekniskt så att den som begär hjälp måste sända över den elektroniska handlingen eller vidta någon annan särskild åtgärd för att materialet ska bli åtkomligt för befattningshavaren vid den myndighet som tillhandahåller tjänsten. I sådana fall blir endast det som i praktiken överförs allmän handling. Detta material kan sannolikt inom kort tas bort i enlighet med ett beslut om gallring.

om undantaget inte gjorts beroende av visst ändamål. Skulle en begränsningsregel utformas så att åtkomst får ske endast när det behövs för att t.ex. rätta tekniska fel eller ge hjälp och stöd – dvs. inte när åtkomst behövs med anledning av en begäran om offentlighetsinsyn – blir undantaget inte grundlagsenligt.

Ett annat alternativ kan vara att begränsa en myndighets roll i enlighet med 2 kap. 10 § första stycket TF så att elektroniska handlingar hanteras endast som led i teknisk bearbetning eller teknisk lagring för annans räkning; jfr 2 kap. 6 § tredje stycket TF där det framgår att en handling inte heller anses inkommen när den återkommer till en myndighet som tillhandahållit den. Denna regel har tillkommit mot bakgrund av att offentlighetsprincipen inte ansetts kräva att allmänheten ska ha tillgång till en upptagning hos myndighet som endast tar teknisk befattning med den. I lagmotiven nämns som exempel på sådan teknisk uppgift att redigera myndighets ljudupptagningar på magnetband, överföra sådana upptagningar till grammofonskiva, framkalla fotografiskt material och lagra information i skivminne eller på magnetband (prop. 1975/76:160 s. 87, 137 och 171).

4.4 Allmän bedömning

4.4.1 Handlingsbegreppet och tillgänglighetsrekvisitet

Begreppet handling i 2 kap. TF är så vidsträckt att alla elektroniskt lagrade uppgifter som aktualiseras i anknytning till it-drift, elektroniskt förvar samt hjälp- och presentationstjänster torde omfattas.

En elektronisk handling blir som framgått att anse som inkommen till myndighet och förvarad där redan genom att den har gjorts tillgänglig av annan för myndigheten – med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas (jfr 2 kap. 3 § andra stycket och 6 § första stycket TF). Detta gäller oberoende av om denna tillgänglighet har sin grund i tillhandahållandet av en tjänst. Tryckfrihetsförordningens grundläggande rekvisit enligt 2 kap. 3 § för allmän handling och enligt 2 kap. 6 § för inkommande i elektronisk miljö är därmed uppfyllda.

Därmed återstår att bedöma om det undantag som föreskrivs i 2 kap. 10 § första stycket TF från allmän handling är tillämpligt på de tjänster som delegationen har genomlyst.

4.4.2 Ren it-drift

När utkontraktering sker så att en myndighet tillhandahåller it-drift åt en annan myndighet kan det vara fråga om hela it-miljöer som den som beställt tjänsten kan bruka utan att behöva ha egna servrar eller egen personal som sköter de tekniska hjälpmedlen. Det är också vanligt med utkontraktering av begränsade enkla tekniska tillämpningar. Oavsett omfattningen av det som tillhandahålls torde det normalt stå klart att den myndighet som tillhandahåller tjänsten varken får eller avses behandla uppgifterna för något annat ändamål än att tillhandahålla teknisk bearbetning och teknisk lagring åt den som har beställt tjänsten.

Vid sådana förhållanden är rekvisiten i 2 kap. 10 § första stycket TF för sådan *endast* teknisk bearbetning och teknisk lagring som omfattas av undantaget uppfyllda. De uppgifter och handlingar som är tekniskt tillgängliga för den tjänstelevererande myndigheten är därmed inte att anse som allmän handling hos den myndighet som levererar tjänsten.

En sekretessreglering för uppgifter hos den tjänstelevererande myndigheten behövs därmed endast som en tystnadsplikt för myndighetens befattningshavare.

4.4.3 Hjälptjänster och presentationstjänster

När uppgifter blir tillgängliga för en myndighet som tillhandahåller en hjälptjänst eller en presentationstjänst är situationen en annan än vid ren it-drift. Tjänsten gå inte ut på att tekniskt bearbeta och lagra uppgifter för någon annan räkning. I stället tillhandahåller myndigheten en tjänst för egen räkning och i eget namn där det centrala är antingen den information som myndigheten ställer samman och visar i en presentationstjänst eller den – ofta muntliga – information som en myndighet ger i en hjälptjänst om hur ett problem kan avhjälpas eller hur vissa uppgifter bör förstås.

När elektroniska handlingar används för dessa ändamål blir det inte fråga om sådan teknisk bearbetning eller teknisk lagring som omfattas av undantaget i 2 kap. 10 § första stycket TF. Även om själva tjänsten gentemot slutanvändaren kan innefatta moment av teknisk bearbetning eller lagring blir det inte fråga om *endast* sådan

verksamhet. En sekretessreglering av uppgifter i en sådan tjänst skulle därmed få verkan både som tystnadsplikt för befattningshavare och förbud mot att lämna ut allmänna handlingar.

4.5 Elektroniskt förvar

Vid bedömningen av behovet av sekretess för elektroniskt förvar[20] är det av betydelse om nyttoinformation[21] i det elektroniska förvaret anses vara allmän handling hos tillhandahållaren av förvaret.

En handling i ett sådant förvar blir visserligen tekniskt tillgänglig för den myndighet som tillhandahåller förvaret – med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas – men frågan är om det undantaget i 2 kap. 10 § första stycket TF blir tillämpligt.

Vid denna bedömning behöver det särskilda syftet med en användares elektroniska förvar beaktas.

4.5.1 Skyddet enligt grundlag

Tanken med att tilldela ett elektroniskt förvar åt en användare av en ärendetjänst är att innehavaren ska kunna använda detta förvar exklusivt och att den myndighet som tekniskt administrerar detta förvar inte ska få ha åtkomst till innehållet – dvs. den nyttoinformation som innehavaren behandlar där.[22] Skulle informationen i en användares elektroniska förvar anses vara offentlig förfelas meningen med den infrastruktur som myndigheterna i denna del byggt upp.

Förutsättningarna liknar delvis det behov av persondataskydd som har redovisats i flera utredningsbetänkanden från senare tid, bl.a. av Informationshanteringsutredningen i delbetänkandet Överskottsinformation vid direktåtkomst.[23] Här är situationen emellertid delvis en annan. Behovet av skydd avser inte de risker för enskildas personliga integritet som kan uppkomma till följd av den

[20] Jfr den närmare beskrivning i avsnitt 3.3 av elektroniskt förvar (även kallat eget utrymme).
[21] Angående detta begrepp, se avsnitt 3.2, och beskrivningen i avsnitt 3.3.
[22] Motsatsen gäller för den drift- och säkerhetsrelaterade information som en myndighet behandlar för att kunna tillhandahålla eget utrymme.
[23] Se SOU 2012:90 s. 39 ff.

handlingsoffentlighet som blir följden av att en myndighet av tekniska skäl ges direkt åtkomst till en *annan myndighets* informationstillgångar. Risken är i stället att uppgifter *i en användares eget förvar* – som den myndighet som tillhandahåller sådant förvar inte avses ta del av – blir allmän handling eller kommer till någon befattningshavares kännedom vid den tekniska hanteringen[24] utan att uppgifterna omfattas av en tystnadsplikt för denne.

Skyddet för elektroniskt förvar knyter här an dels till de undantag från tillämpningsområdet för grundlag som gäller beträffande det *sätt* på vilket en uppgift har anskaffats (se följande redovisning), dels till det privatliv som den *europeiska konventionen* angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) ska värna.

Beträffande sättet för att anskaffa en uppgift har anskaffarfriheten enligt 1 kap. 1 § fjärde stycket TF begränsats så att en anskaffare utan hinder av de fri- och rättigheter som följer av tryckfrihetsförordningen, enligt 1 kap. 9 § 5 TF, kan ställas till svars för de *metoder* han eller hon använder. Är metoden olaglig kan ansvar utkrävas enligt vanlig lag. Anskaffarfriheten medger således inte att uppgifter anskaffas genom inbrott, egenmäktigt förfarande, olovlig avlyssning eller brytande av post- eller telehemlighet.[25] Detsamma följer av 1 kap. 12 § YGL; jfr hur föreskrifter som utan avseende på yttrandens innehåll närmare reglerar ett visst sätt att sprida eller ta emot yttranden, enligt 2 kap. 23 § RF, inte anses som en begränsning av yttrandefriheten och informationsfriheten.

Det skydd som föreskrivs i 4 kap. 9 och 9 c §§ brottsbalken mot intrång i förvar och dataintrång ges visserligen i vanlig lag men det kan omfatta även ett sådant virtuellt elektroniskt förvar som övervägs här. Sådana ”utrymmen” tillhandahålls på motsvarande sätt som när exempelvis Riksarkivet och universitetsbiblioteken tillhandahåller låsbara skåp åt sina besökare. Det blir straffbart även för befattningshavare hos myndigheten att olovligen bereda sig tillgång till ett låst skåp respektive ett skyddat elektroniskt förvar.

En annan parallell av intresse för användares elektroniska förvar är huruvida förvaret, trots att det tekniskt finns i en myndighets it-

[24] Reglerna för befattningshavare som sköter driften av användares elektroniska förvar utformas visserligen så att de inte får bereda sig tillgång till användares elektroniska förvar men det kan undantagsvis vara lovligt om åtgärden krävs för att rätta ett tekniskt fel eller att utföra en åtgärd som krävs från informationssäkerhetssynpunkt.

[25] Däremot skall anstiftan till brott mot tystnadsplikt enligt motiven inte bedömas som ett sätt för uppgiftsanskaffande enligt denna regel (prop. 1975/76:204 s. 98).

miljö, ska anses höra till det privat- eller familjeliv, hem, och den korrespondens som är skyddad enligt Europakonventionen. Elektroniskt förvar inrättas för att vara ett privat ”förvar”. Av artikel 8 Europakonventionen följer ett skydd för privatlivet som inte kan inskränkas annat än genom lag och inte i vidare mån än vad som i ett demokratiskt samhälle är nödvändigt med hänsyn till vissa intressen som anges i artikeln.

Av lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna följer att Europakonventionen gäller som lag i Sverige. Enligt 2 kap. 19 § RF får lag eller annan föreskrift inte meddelas i strid med konventionen. Eftersom offentlighetsprincipen är grundlagsfäst har dock sekretess inte ansetts kunna grundas direkt på Europakonventionen (RÅ 2006 ref 87). Samtidigt har det förutsatts att konventionens innehåll kan påverka tolkningen av svensk lag genom s.k. fördragskonform tolkning (prop. 1993/94:117 s. 37, jfr NJA 1998 s. 838).

Även om det är avsett att bestämmelser i grundlag ska tolkas restriktivt kan det mot denna bakgrund finnas anledning att beakta eventuella möjligheter att tolka bestämmelsen i 2 kap. 10 § TF så att tillämpningen av svensk rätt bringas i överensstämmelse med Europakonventionen även i anknytning till användares elektroniska förvar. De strikta avgränsningar som myndigheter inför tekniskt och administrativt för sådant förvar talar också för att det är fråga om endast led i teknisk bearbetning eller teknisk lagring för innehavarens räkning. Det är bara innehavaren som ska få skriva och förvara handlingar där – i övrigt sker allt helt automatiserat. Så som tjänsterna för elektroniskt förvar utformats kan det inte heller råda någon tvekan om ett utkast till en inlaga eller annan nyttoinformation finns i det elektroniska förvaret eller i myndighetens verksamhetssystem för t.ex. ärendehandläggning. Strikta regler och rutiner tillämpas för elektroniskt mottagningsställe där det tydligt framgår när en handling har lämnat användarens elektroniska förvar och kommit till myndighets ordinarie system. Ett rigoröst säkerhetsarbete bedrivs för att dessa gränser inte ska brytas, vilket i praktiken inte kan förenas med åtkomst för sekretessprövning av uppgifter som finns där.

Härtill kommer att de handlingar som förvaras i en användares elektroniska förvar närsomhelst kan ändras av innehavaren – uppgifter kan läggas till och tas bort. Det är inte ens nödvändigt att den enskilde ger in någon handling till myndigheten. Detta understry-

ker det faktum att den information och de handlingar som finns i en användarens elektroniska förvar inte är något som myndigheten förfogar över. Inte heller är syftet med användares elektroniska förvar att myndigheten ska kunna ta del av t.ex. olika utkast, förlagor eller andra preliminära handlingar som den enskilde kanske senare väljer att i en slutlig version delge myndigheten.

4.5.2 Myndigheternas bedömning

Frågan om hur 2 kap. TF bör tolkas med avseende på en användares elektroniska förvar aktualiserades redan i mitten på 2000-talet inom ramen för ett regeringsuppdrag, det s.k. SAMSET-projektet, och i en E-nämndens vägledning för hantering av inkommande elektroniska handlingar.[26] Där förklarades visserligen att frågor om inkommande enligt tryckfrihetsförordningen och andra frågor om allmänna handlingar inte omfattades av vägledningen, men myndigheterna rekommenderades samtidigt att inte utforma sina system så att handlingar i ett serviceskede, innan de nått myndighetens elektroniska mottagningsställe, blir tillgängliga med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att de kan läsas, avlyssnas eller på annat sätt uppfattas. I vägledningen antogs alltså att användares elektroniska förvar skulle utformas så att en myndighet som tillhandahöll ett sådant var *tekniskt* förhindrad att i uppfattbar form komma åt uppgifter i förvaret.[27]

I praktiken har det emellertid visat sig att i vart fall någon på en myndighets teknikavdelning, som tillhandahåller elektroniskt förvar åt användare, behöver kunna ges åtkomst när det blir nödvändigt för att rätta fel eller att vidta åtgärder som krävs från informationssäkerhetssynpunkt. Det har som berörts visat sig bli alltför administrativt betungande och därmed kostsamt att kryptera innehållet i användares elektroniska förvar så att det inte kan läsas.[28] Denna fråga har uppmärksammats även av E-delegationen redan genom den hänvisning till 2 kap. 10 § TF som delegationen

[26] E-nämnden 05:02; se vidare bilaga 4.

[27] Se vägledningen avsnitt 6.2.5. I den vägledningen förklarades dessutom att en sådan teknisk begränsning var en förutsättning för att kunna upprätthålla en god offentlighetsstruktur.

[28] Jfr avsnitt 4.2 där det framgått att det räcker att det finns en person, t.ex. på teknikavdelning, som har tekniska möjligheter att överföra uppgifter, som myndigheten har teknisk tillgång till hos annan, i sådan form att de kan läsas, avlyssnas eller på annat sätt uppfattas, för att sammanställningar av sådana uppgifter ska utgöra allmänna handlingar (prop. 2007/08:160 s. 71).

gett i en definition av eget utrymme, här kallat elektroniskt förvar.[29] Där beskrivs eget utrymme som ett skyddat förvar hos myndighet som den tillhandahåller ”endast som led i teknisk bearbetning eller teknisk lagring för annans räkning” – dvs. med en formulering som är direkt hämtad från undantaget i 2 kap. 10 § första stycket TF. I den vägledningen har E-delegationen också noterat att uppgifter normalt blir tekniskt tillgängliga för en myndighet som tillhandahåller elektroniskt förvar åt användare (se avsnitt 3.3). E-delegationen har vidare anfört bl.a. följande:

> Tjänster och funktioner för e-förvaltning bygger i övrigt till betydande del på en tillämpning av undantaget för endast teknisk bearbetning eller teknisk lagring för annans räkning och att det i praktiken inte är någon annan än innehavaren som får insyn i den nyttoinformation som finns i användarens eget utrymme.
>
> Lagmotiven till undantagsbestämmelserna är emellertid skrivna med tanke på annat än it-baserade tjänster och det finns inte någon rättspraxis som avser t.ex. ärendetjänster. Den för hela e-förvaltningen avgörande frågan om vad som innefattas i endast teknisk bearbetning eller lagring respektive endast befordran av meddelande är därför delvis svår att bedöma. Om it-arkitekturen och de ändamål för vilka den används utformas felaktigt, och om uppgifterna inte är sekretessbelagda, finns det alltså en risk för att uppgifter och handlingar som användare ser som sina egna, utan att andra ska ha rätt att ta del av dem, blir allmänna och offentliga handlingar.
>
> En myndighet som tillhandahåller en funktion som bygger på något av dessa undantag bör vidta särskilda åtgärder för att säkerställa att handlingarna inte finns tillgängliga vid myndigheten för annat ändamål än vad som anges i berörd undantagsbestämmelse; dvs. att de används endast för teknisk bearbetning eller teknisk lagring för annans räkning eller brukas endast för befordran av meddelande.

Enligt E-delegationens juridiska vägledning för verksamhetsutveckling inom e-förvaltningen bör alltså att särskilda åtgärder vidtas för att säkerställa att handlingar inte finns tillgängliga vid en myndighet för annat än teknisk bearbetning eller teknisk lagring för annans räkning. Vilka dessa åtgärder skulle vara eller på vilket sett hänsyn skulle behöva tas till rekvisitet ”endast” för att det ska gälla anges emellertid inte. I vägledningen sägs också följande:

> Denna rättsliga modellösning för ärendetjänster innebär att utkast och andra handlingar som en användare upprättar eller annars hanterar i sitt eget utrymme inte anses inkomna till den myndighet som till-

[29] Se vidare den E-delegationens juridiska vägledning för verksamhetsutveckling inom e-förvaltningen.

> handahåller ärendetjänsten. Handlingarna blir enligt 10 § FL inte inkomna förrän de har nått myndighetens elektroniska mottagningsställe och it-arkitekturen och de ändamål för vilka den används är utformade i enlighet med 2 kap. 10 § TF så att uppgifter finns i användarens eget utrymme, endast som led i teknisk bearbetning eller teknisk lagring för användarens räkning. En teknisk möjlighet för den myndighet som tillhandahåller utrymmet, att komma åt en handling där, ska därmed inte leda till att handlingar i det egna utrymmet blir allmänna.

Frågan är om E-delegationens tolkning vinner stöd av lagmotiv, rättspraxis eller annars av omständigheter som begränsar den rättsliga risken för enskilda vid användning av elektroniskt förvar.

4.5.3 Undantagsbestämmelsen och dess utformning

När tryckfrihetsförordningen anpassades för elektronisk miljö fanns inte en tanke på att utvecklingen skulle leda till att myndigheter behöver tillhandahålla virtuella ”förvar” för enskilda som utarbetar utkast inför ingivning till en myndighet. Det är emellertid knappast kontroversiellt att en myndighet som tillhandahåller ett elektroniskt förvar åt en användare behandlar de handlingar som finns i sådant förvar som led i teknisk bearbetning eller teknisk lagring för annans räkning. Frågan är i stället om bearbetningen och lagringen ska anses ske ”*endast*” för annans räkning.

En närmast självklar förutsättning för att en enskild ska använda ett sådant förvar är som framgått att de uppgifter som finns där inte röjs – inte ens för myndighetens tekniska personal. Tillhandahåller en myndighet ett sådant förvar ska myndigheten inte kunna veta vilka uppgifter den enskilde behandlar där. Begränsas bedömningen till de ändamål för vilka handlingar behandlas i en användares elektroniska förvar står det klart att hanteringen sker *endast* som led i teknisk bearbetning eller lagring för innehavaren. Det är först när en handling har lämnat detta förvar (i praktiken kommit till myndighetens mottagningsställe för sådana inkommande handlingar – överföringen dit sker sekundsnabbt) som lagring och bearbetning sker för något annat ändamål.

Det kan också hävdas att det redan av ordalydelsen i 2 kap. 10 § första stycket TF följer att en handling som aldrig blir ingiven men finns i en användares elektroniska förvar hanteras där *endast* som led i teknisk bearbetning eller teknisk lagring för annans räkning. Bestämmelsens gäller nämligen för ”*handling*” som förvaras hos myndighet. Olika förstadier och utkast till t.ex. en inlaga utarbetas

stegvis och huvuddelen av dem ges aldrig in till myndigheten i förvaltningslagens mening. Myndigheten får inte heller bereda sig tillgång till de utkast eller den information i övrigt som finns i en användares elektroniska förvar. Myndigheten ska endast handha den tekniska plattformen och den drift- och säkerhetsrelaterade information som krävs för att tjänsten ska fungera smidigt och säkert.

I detta sammanhang kan också ifrågasättas om det är förenligt med ordalydelsen i 2 kap. 6 § första stycket andra meningen TF att hävda att de olika förstadier och utkast som stegvis utarbetas i användares elektroniska förvar, men aldrig sänds till en myndighets elektroniska mottagningsställe, kan anses vara inkomna i tryckfrihetsförordningens mening. En förutsättning för att en elektronisk handling ska anses inkommen enligt 2 kap. 6 § första stycket andra meningen TF är att *annan* har gjort den tillgänglig för myndigheten – på sätt som anges i 3 § andra stycket.

De bedömningar som ligger bakom utformningen av regleringen i tryckfrihetsförordningen av när en elektronisk handling anses inkommen tar sin utgångspunkt i en princip om att allmänhetens tillgång till handlingar ska motsvara den information som myndigheten själv förfogar över. Även om ett sådant förfoganderekvisit inte kommer till direkt uttryck i lagtexten, kan det sägas att myndighetens tillgång till informationen för sin egen information har varit en bärande tanke bakom regleringens utformning (prop. 1975:160 s. 86 f). Utformningen av och ändamålet med användares elektroniska förvar är alltså ett annan än att en myndighet ska göra elektroniska handlingar tillgängliga i läsbar eller annars uppfattbar form. En myndighet avses ta del av en sådan handling först när den har lämnats från användarens elektroniska förvar till myndighetens elektroniska mottagningsställe. Förvaringen avses bara ske som led i bearbetning och lagring för innehavaren av det elektroniska förvaret. Detsamma får anses gälla enligt 2 kap. 6 § första stycket andra meningen TF för handling som ska ges in, till dess den har sänts till angivet mottagningsställe. Först då gör ”annan” – dvs. ingivaren – en handling tillgänglig för myndigheten genom att ge in den till myndigheten.

De funktioner för elektroniskt förvar som myndigheter tillhandahåller syftar till en fungerande elektronisk förvaltning. Om det anses att ”annan” har gjort de handlingar som finns i användares elektroniska förvar tillgängliga för myndighet, på sätt som anges i 2 kap. 3 § andra stycket och 6 § första stycket TF, återstår

att bedöma om undantaget i 2 kap. 10 § första stycket TF är tillämpligt.

4.5.4 Närmare om ”endast” för annans räkning

Frågan är därmed under vilka förutsättningar hanteringen i en användares elektroniska förvar kan anses ske *endast* för annan än myndighetens räkning. Skulle nyttoinformationen där kunna anses vara förvarad för myndighetens räkning, så att undantaget i 2 kap. 10 § första stycket TF inte blir tillämpligt – trots att myndigheten inte avses få ha åtkomst till det elektroniska förvaret och att det inte har avsänts något därifrån?

Eftersom utgångspunkten enligt 2 kap. 10 § första stycket TF är ”handling” som förvaras, får utgångspunkten för bedömningen antas vara om den enskilda handlingen förvaras på sätt som anges i bestämmelsen. Ett annat synsätt skulle kunna vara att se hela myndighetens verksamhet i ett sammanhang och att hävda att undantaget inte kan tillämpas om det finns ett bakomliggande intresse hos myndigheten att hanteringen i användarens elektroniska förvar ska vara till nytta för myndighetens egen verksamhet.

Det senare synsättet skulle få till konsekvens att den omfattande utkontraktering som myndigheter idag ägnar sig åt leder till allmänna handlingar hos myndigheter som utför tjänster för utkontraktering. Från ett slags helhetsperspektiv torde det ytterst alltid kunna hävdas att det fins en koppling till myndighetens egen verksamhet. Som exempel kan nämnas att Skatteverket själv expedierar försändelser elektroniskt via de elektroniska brevlådor – elektroniska förvar – som myndigheten tillhandahåller åt enskilda för meddelanden från myndigheter (se minmyndighetspost.se) och att en utkontraktering till en myndighet av fakturaskanning kan avse även en faktura från den myndighet som utför skanningen.

4.5.5 Lagmotiv och rättspraxis

I regeringens proposition 1975/76:160 om nya grundlagsbestämmelser angående allmänna handlingars offentlighet anfördes att offentlighetsprincipen inte kräver att allmänheten ska ha tillgång till en upptagning hos myndighet som endast tar teknisk befattning med den. Ett undantag föreslogs därför från offentlighet hos en myndighet som endast har en teknisk uppgift i sammanhanget och att detta undantag skulle gälla även om myndigheten som ett led i den tekniska bearbetningen för annans räkning hade lov att

överföra upptagningen i läsbar form. Undantaget föreslogs gälla även om den tekniska bearbetningen utfördes för en enskilds räkning.

Information som kan hämtas från sådana upptagningar kunde enligt lagmotiven inte rimligen sägas ingå i de allmänna organens informationstillgångar. Av författningskommentaren framgick dessutom att förslaget till 10 § hade motiverats av att en myndighet som förvarar en upptagning, endast för teknisk bearbetning eller lagring, inte torde förfoga över upptagningen på sätt som enligt Offentlighets- och sekretesslagstiftningskommitténs (OSK) förslag varit en förutsättning för att en upptagning skulle bli allmän handling.[30] Återgivna uttalanden passar väl in även på de uppgifter som utförs av myndigheter som tillhandahåller elektroniskt förvar åt enskilda.

Därmed återstår vad som kan utgöra sådan teknisk bearbetning eller teknisk lagring för vilken bestämmelsen i 10 § ska gälla. I specialmotiveringen till 10 § hänvisades beträffande innebörden av teknisk bearbetning till vad som anförts i specialmotiveringen till 6 §. Dessa uttalanden var starkt präglade av 1970-talets teknikanvändning. Där nämndes endast datacentral som överför handling till maskinläsbart medium, maskinskrivet manuskript som sänds till datacentral för överföring av texten till magnetband, manuskript som överlämnas för tryckning eller kopiering samt sådana åtgärder som redigering av ljudupptagningar på magnetband, överföringar av sådana upptagningar till grammofonskiva och framkallning av fotografiskt material. Departementschefen hänvisade beträffande vad som avsågs med teknisk lagring till sådana former av lagring som kräver särskilda tekniska anordningar, t.ex. lagring av information i skivminne eller på magnetband.[31] De beskrivningar som gavs i denna del var av en helt annan karaktär än, inte bara vad som tekniskt utförs av myndigheter som tillhandahåller elektroniskt förvar åt användare, utan även av helt annan karaktär än det stöd som myndigheter idag ger i form av ren it-drift eller liknande under åberopande av 2 kap. 10 § första stycket TF.

Att detta undantag numera tillämpas på helt andra former av teknisk bearbetning och teknisk lagring än dem som beskrivits i lagmotiven har också kommit till uttryck i rättspraxis där ekonomi- och redovisningssystem som tillhandahålls av myndighet åt andra

[30] Prop. 1975/76:160 s. 87 och s. 171 och SOU 1975:22.
[31] Prop. 1975/76:160 s. 87, 137 och 171.

myndigheter setts som led i teknisk bearbetning eller teknisk lagring för annans räkning och inte som allmän handling hos den myndighet som tillhandahållit dessa funktioner (RÅ 1994 ref. 64). Ett webbaserat arbetsskadesystem, som har prövats från offentlighetssynpunkt av Högsta förvaltningsdomstolen, ansågs visserligen inte vara omfattat av undantaget i 2 kap. 10 § första stycket TF, men de skäl som angavs var att bearbetning och lagring ägde rum även för myndighetens *egen* räkning eftersom myndigheten också utarbetade statistik och arbetsmiljörapporter med stöd av det tekniskt bearbetade och lagrade materialet (HFD 2011 ref. 52).

Därmed är vi inne på den fråga som är relevant för bedömningen av sådana elektroniska förvar som myndigheter tillhandahåller i anknytning till e-tjänster. Högsta förvaltningsdomstolen undvek att – för de fall där behandlingar skedde endast för annans räkning – bedöma det nämnda webbaserade arbetsskadesystemet, genom att i domskälen ange att *i vart fall* den beskrivna användningen (statistikframställning och arbetsmiljörapportering) inte var hänförlig till sådan teknisk bearbetning eller teknisk lagring som omfattas av undantaget enligt 2 kap. 10 § TF.

Att det ska vara fråga om teknisk bearbetning eller lagring för *annans* räkning har också ansetts utesluta att det aktuella undantaget skulle vara tillämpligt på arkivmyndigheters material. Bakom detta torde ligga att arkivmyndigheten tar hand om och arkiverar materialet för egen räkning (prop. 1979/80:2 s 272).

Frågan om vad som är utmärkande för verksamhet som beskrivs som *endast* teknisk bearbetning eller lagring aktualiseras också i offentlighets- och sekretesslagen (2009:400; förkortad OSL). Enligt 40 kap. 5 § OSL gäller sekretess i verksamhet för *enbart* teknisk bearbetning eller lagring för någon annans räkning. Verksamheten teknisk bearbetning eller teknisk lagring är densamma som beskrivs i 2 kap. 6 § tredje stycket och 10 § första stycket TF. Detta skydd för uppgifter som är föremål för teknisk bearbetning eller lagring har tillkommit mot bakgrund av att offentlighetsprincipen inte ansetts kräva att allmänheten ska ha tillgång till en upptagning hos myndighet som endast tar teknisk befattning med den. Här avses alltså ”endast” teknisk bearbetning eller lagring av handlingen. I motiven till den enligt sekretesslagen tidigare gällande motsvarigheten till 40 kap 5 § OSL har anförts att det inte vore godtagbart att sekretess skulle saknas inom en datacentral med ställning av myndighet för uppgifter som bearbetas eller lagras för en enskild kunds räkning (prop. 1979/80:2 s 272).

Vi återkommer i avsnitt 5 till frågan om gällande bestämmelser ger ett sådant sekretesskydd.

4.5.6 Delegationens bedömning

Delegationens bedömning: Det undantag från allmän handling som föreskrivs i 2 kap. 10 § första stycket TF är tillämpligt även på en handling i ett elektroniskt förvar.

För att bedöma behovet av sekretess för uppgifter i en användares elektroniska förvar är det som framgått av betydelse om den nyttoinformation som finns i ett sådant förvar ska ses som en allmän handling hos den myndighet som tillhandahåller förvaret.

Enligt delegationens bedömning får det undantag som föreskrivs i 2 kap. 10 § första stycket TF anses vara tillämpligt även på handlingar i ett elektroniskt förvar. Det har visserligen invänts att det skulle saknas stöd för en tolkning som innebär att ett tekniskt delmoment, under den tid en handling finns hos en myndighet, skulle kunna ”isoleras” och betraktas separat, t.ex. när en handling först upprättas i en användares elektroniska förvar och därefter ges in och behandlas i myndighetens verksamhetssystem.[32] Denna invändning synes emellertid bygga på tanken att reglerna om handlingsoffentlighet skulle ha kommit till utifrån ett ”processtänkande” – inte utifrån en bedömning av produkter i form av sakligt sammanhängande konstellationer av uppgifter som anses utgöra handling (upptagning) i tryckfrihetsförordningens mening. Ett sådant resonemang byggt på ”processer” framstår inte som naturligt från juridiska utgångspunkter. Om det skulle tillämpas blir det ändå nödvändigt att skilja den process där användaren utarbetar sitt utkast från den process där myndigheten handlägger det ärende som anhängiggörs när handlingen inkommer till myndigheten.

Strukturer av beskrivet slag införs i allt större utsträckning, till följd av de nya förutsättningar som informationstekniken för med sig. Reglerna om handlingsoffentlighet gäller emellertid för produkter – sakligt sammanhängande konstellationer av uppgifter som är att anse som handling.

[32] Beträffande detta begrepp, jfr not 4 i avsnitt 3.2.

Varje ”kopia” av en elektronisk handling har samma kvalitet i en sådan miljö[33] och den kommunikation som sker via nät kan förenklat beskrivas så att data som representerar en handling ”kopieras” gång på gång till dess den når mottagaren. De gränser som införs mellan olika system och aktörer blir därmed virtuella – allt bryts ned till mönster av signaler, även t.ex. brandväggar och andra system för att avgränsa och skydda mot intrång. Till följd av denna s.k. konvergens – dvs. sammansmältning av infrastrukturer, tjänster och apparater[34] – är det inte längre möjligt att bedöma en handlings egenskap att vara allmän eller inte utan att beakta det tekniska och administrativa sammanhang där handlingen figurerar och de virtuella gränser som finns mellan olika aktörers it-miljöer.

Det har därmed blivit en utmaning att juridiskt bedöma om en elektronisk handling är att anse som *förvarad* och *inkommen* hos en myndighet enligt 2 kap. TF. Som regleringen utformats anses så vara fallet redan när handlingen blivit tekniskt tillgänglig för myndigheten; data behöver således inte ens ha överförts. Det undantag för bearbetning och lagring som här övervägs har emellertid inte sin grund i tillgänglighet till handlingar. Avgörande är i stället dels om en myndighet behandlar en viss handling *endast tekniskt,* dels om en handling vid den juridiska bedömningen kan särskiljas från en annan handling, med samma eller annat innehåll, som myndigheten förvarar i en annan teknisk och administrativ kontext. Det kan t.ex. vara fråga om ett elektroniskt exemplar av en handling som användaren har färdigställt och skrivit under i sitt elektroniska förvar hos myndigheten, dels ett exemplar som har överförts till myndighetens elektroniska mottagningsställe och vidare till myndighetens verksamhetssystem; jfr att en sökande har gett in en ansökan på papper till en myndighet men har kvar en kopia hos sig.

Enligt delegationens bedömning är den handling som har nått myndighetens elektroniska mottagningsställe allmän hos myndigheten medan undantaget i 2 kap. 10 § första stycket TF gäller för exemplar i användarens elektroniska förvar. Fråga är om två handlingar som från offentlighetssynpunkt får bedömas var för sig.

[33] Se vidare regeringens proposition 2012/13:74 Förfalsknings- och sanningsbrotten, där det förklaras att man i fråga om elektroniska handlingar inte kan tala om unika exemplar utan snarare om originalinnehåll eftersom det i den elektroniska miljön kan finnas flera exemplar med samma kvalitet.

[34] Se vidare Konvergensutredningens betänkande (SOU 1999:55) Konvergens och förändring – Samordning av lagstiftningen för medie- och telesektorerna.

Särskilt tydligt blir detta om exemplet varieras så att det exemplar som finns i användarens elektroniska förvar endast är ett utkast med annat innehåll.

Behovet av att en handlings status hos en myndighet ska kunna växla över tid har nyligen föranlett en ändring i 2 kap. 10 § TF så att handling inte är att anse som allmän när den förvaras endast i syfte att kunna återskapa information som har gått förlorad i en myndighets ordinarie system för automatiserad behandling av information. Här är det uppenbart en ”kopia” av en och samma handling, den representation som finns på en säkerhetskopia, inte anses vara allmän, till skillnad från det exemplar som finns i myndighetens ordinarie system. Det framgår här såväl av 2 kap. 10 § andra stycket TF som av lagmotiven att en handling som finns i en säkerhetskopia ska bedömas skild från motsvarande handling i myndighetens ordinarie system för automatiserad behandling.

Det är således inte oförenligt med 2 kap. TF – i synnerhet inte med kapitlets 10 § – att betrakta samma information olika beroende på det sammanhang i vilket den förekommer. Vid en tillämpning av motsvarande synsätt när paragrafens första stycke tolkas bör noteras att det i lagmotiven till paragrafens andra stycke har noterats att Högsta förvaltningsdomstolen genom sin praxis har godtagit en ändamålstolkning av offentlighetsprincipen vid tolkning av vad som ska anses ligga i begreppen ”expedierad” respektive ”inkommen” (prop. 2009/10:58 s. 21). Det torde på motsvarande sätt vara förenligt med gällande rätt att – vid bedömning av om uppgifter ingår i en allmän handling eller inte – ta hänsyn till syftet med att viss information finns hos en myndighet. Det för bedömningen av elektroniskt förvar centrala rekvisitet ”endast” förekommer också i paragrafens andra stycke och tar även där sin utgångspunkt i det syfte för vilket en ”handling”, till skillnad från en annan handling, förvaras hos en myndighet. Informationstekniken har utvecklats på ett sätt som knappast kunnat förutses och påverkar nära nog varje samhällsområde och regelverk. Dagens system, strukturer och ansvarsgränser behöver därför kunna förenas med gällande rätt och de synsätt i övrigt som författningsregleringen bygger på. En helt ny rättslig reglering, införd utifrån en snäv tolkning av gällande rätt, kan inte genomföras utan ett omfattande och tidskrävande lagstiftningsarbete som under överskådlig tid skulle stå i vägen för bl.a. de elektroniska tjänster som myndigheterna redan har infört.

Enligt delegationens bedömning är det också naturligt att – i enlighet med det synsätt som redovisats i det nyligen genomförda

lagstiftningsärendet rörande 2 kap. 10 § TF – bedöma handlingar i en användares elektroniska förvar på motsvarande sätt som handlingar på en säkerhetskopia. Det är *andra handlingar* som finns i användarens elektroniska förvar än dem som myndigheten har i sitt ordinarie system. Dessa handlingar förvarar myndigheten *endast* som led i den tekniska bearbetning och tekniska lagring för annans, nämligen för innehavarens räkning.

Härtill kommer att användaren när som helst kan ändra handlingar som han eller hon har i sitt elektroniska förvar så att uppgifter läggs till eller tas bort. Användaren behöver inte ens lämna någon handling som finns i det elektroniska förvaret till myndighetens mottagningsställe. Detta understryker det faktum att myndigheten inte förfogar över de handlingar som finns i användarens elektroniska förvar. Syftet med elektroniskt förvar är inte heller att myndigheten ska kunna ta del av olika utkast, förlagor eller andra preliminära handlingar som den enskilde kanske senare väljer att i en slutlig version ge in till myndigheten. Som framgått har ett bärande skäl bakom undantaget i 2 kap. 10 § första stycket TF varit att den information som myndigheten inte förvarar eller bearbetar för egen del inte kan anses utgöra en del av myndighetens informationstillgångar.

Här bör också nämnas att det knappast finns något offentlighetsintresse som träds förnär genom den tolkning som delegationen hävdar, för det fall att en enskild fyller i en blankett med hjälp av förifyllda uppgifter från en myndighet. De förifyllda uppgifterna är redan en del av allmänna handlingar hos myndigheten i dess ordinarie system och torde få anses bli expedierade när de lämnas till användares elektroniska förvar. På motsvarande sätt blir den information som den enskilde skickar i retur till myndigheten en del i en inkommen handling i myndighetens verksamhetssystem. Offentlighetsintresset kan knappast därutöver anses kräva att de uppgifter som den enskilde har tagit in i ett utkast – som kanske inte ens ges in och som kanske är felaktiga – ska omfattas av offentlighetsinsyn. Sådana uppgifter ska inte läggas till grund för myndighetens ärendehandläggning.

Även de strikta avgränsningar som myndigheter inför tekniskt och administrativt för användares elektroniska förvar talar för att det är fråga om endast led i teknisk bearbetning eller teknisk lagring för en användares räkning. Det är bara innehavaren som får skriva och förvara uppgifter där – i övrigt sker allt automatiserat.

Det kan så som systemen utformas inte heller råda någon tvekan om en handling finns i användares elektroniska förvar eller i myndighetens verksamhetssystem. Strikta regler och rutiner tillämpas för elektroniskt mottagningsställe där det tydligt framgår när en handling har kommit in till myndighets ordinarie system och ett rigoröst säkerhetsarbete bedrivs för att berörda gränser inte ska brytas.

Delegationen vill i sammanhanget betona de negativa konsekvenser för e-förvaltningen och den oklarhet om lämpligt utformade rutiner som skulle bli följden om bestämmelsen i 2 kap. 10 § första stycket TF inte skulle anses kunna tolkas på ett sätt som är förenligt med paragrafens andra stycke; jfr den sekretessreglering som krävts rörande direktåtkomst. Här bör också beaktas att det är av värde om inkommandetidpunkten enligt tryckfrihetsförordningen respektive förvaltningslagen kan bringas i överensstämmelse med varandra. En tolkning av 2 kap. 10 § första stycket TF som innebär att handlingar i elektroniska förvar är allmänna blir därmed mindre lyckad. Sådana handlingar skulle bli allmänna hos en myndighet trots att de inte är inkomna enligt förvaltningslagen förrän de har nått myndighetens elektroniska mottagningsställe. Det är normalt först då som utställaren svarar för handlingens innehåll, bl.a. straffrättsligt.

Slutligen bör nämnas att frågan om tekniska processer måste ses som en helhet eller om en uppdelning är möjlig har behandlats av Högsta domstolen bl.a. i ett beslut den 19 mars 2014 (mål nr Ö 5306-13). Rättsfrågan rörde regleringen i yttrandefrihetsgrundlagen och om den medger att en särskild databas kan uppstå genom att någon annan än den som driver verksamheten tillför information på webbplatsen; dvs. medger regelverket att anslutande information kan betraktas som en annan databas skild från den databas vars innehåll inte kan påverkas av annan (i praktiken genom fiktionen att webbplatsen anses uppdelad i två skilda delar)? Högsta domstolen, som i ett tidigare avgörande (NJA 2007 s. 309) betonat vikten av att det är den som faktiskt råder över informationen i databasen som också betraktas som den som tillhandahåller den, fann att det fick anses vara mest förenligt med de intressen som skyddas av yttrandefrihetsgrundlagen att information, som utan föregående åtgärd av den som driver verksamheten tillförs av en utomstående användare i anslutning till en grundlagsskyddad databas, kan betraktas som *en egen databas* i yttrandefrihetsgrundlagens mening. I båda dessa mål ansågs det avgörande hur förhål-

landena naturligen uppfattas, inte hur informationen i databasen systematiserats eller tekniskt lagrats.

På motsvarande sätt torde det vara mest förenligt med ändamålen bakom regleringen i 2 kap. 10 § TF att betrakta en handling som finns i ett elektroniskt förvar som *användarens egen* – skild från en handling som användaren har gett in och som därmed blivit en del av myndighetens informationstillgångar – eftersom det är så förhållandena naturligen uppfattas. En förutsättning är härvid att det elektroniska förvaret och den nyttoinformation som finns där visas via tydliga användargränssnitt och i övrigt så att det som finns där inte kan förväxlas med myndighetens informationstillgångar.

4.6 Gällande rätt eller ny reglering?

Delegationens bedömning: En helt ny rättslig reglering kan inte införas utan ett omfattande och tidskrävande lagstiftningsarbete. En sådan skulle dessutom skapa en parallell reglering i stället för ett enhetligt och samordnat synsätt. En anpassning bör i stället ske till vedertagna synsätt och gränser i gällande rätt.

Arbetet för att utveckla nya former för elektronisk infrastruktur på myndighetsområdet har varit intensivt. Ett sätt att återskapa tydliga gränser i digital miljö skulle därför kunna vara att se e-förvaltningen som något helt nytt, som följer sina *egna förutsättningar*, och därmed skulle behöva regleras på *ett nytt sätt*. En sådan särskild reglering för elektronisk miljö, parallell med den författningsreglering som gäller för traditionella pappersbaserade förfaranden, skulle följa sin egen logik och sannolikt helt förändra utvecklingen av både organisationer och informationssystem.

Tydliga gränser kan emellertid också återskapas genom att inordna e-förvaltningen under dagens system, strukturer och ansvarsgränser – genom att utforma denna miljö så att den i allt väsentligt kan *förenas med gällande rätt* och de synsätt i övrigt som författningsregleringen bygger på. En helt ny rättslig reglering kan inte införas utan ett omfattande och tidskrävande lagstiftningsarbete. Ett sådant tillvägagångssätt skulle därmed stå i vägen för införandet av moderna e-tjänster under överskådlig tid.

Myndigheter har i stället valt att anpassa sina e-tjänster och tillhörande tekniska och administrativa säkerhetsåtgärder till vedertagna synsätt och gränsdragningar i gällande rätt; bl.a. till digitala motsvarigheter till hus, rum, förvar och brevlådor. Denna anpassning har till betydande del byggt på analogier med motsvarande företeelser i fysisk miljö för att det ska bli möjligt att ta tillvara vedertagna synsätt som gällande rätt bygger på.

I det följande utgår delegationen från att den av sin redovisade tolkning av 2 kap. 10 § första stycket TF är förenlig med gällande rätt. Denna bedömning blir av central betydelse när frågor om sekretess ska bedömas med avseende på information som en myndighet behandlar endast tekniskt.

5 Sekretess i it-baserade tjänster

5.1 Regleringen

5.1.1 Allmänt

Enligt 2 kap. 2 § första stycket TF får rätten att ta del av allmänna handlingar begränsas endast om det är påkallat med hänsyn till vissa angivna intressen, t.ex. skyddet för enskilds personliga och ekonomiska förhållanden eller det allmännas ekonomiska intresse. En sådan begränsning ska enligt 2 kap. 2 § andra stycket TF anges noga i en bestämmelse i en särskild lag eller, om det i visst fall är lämpligare, i en annan lag vartill den särskilda lagen hänvisar. Efter bemyndigande i en sådan bestämmelse får regeringen genom förordning meddela närmare föreskrifter om bestämmelsens tillämplighet. Den särskilda lagen är offentlighets- och sekretesslagen (2009:400), förkortad OSL, och regeringen har meddelat föreskrifter om bestämmelsernas tillämplighet i offentlighets- och sekretessförordningen (2009:641).[35]

Sekretess innebär inte bara en begränsning av rätten att ta del av allmänna handlingar utan även ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av allmän handling eller på något annat sätt (3 kap. 1 § OSL). Sekretess innebär således både *handlingssekretess* och *tystnadsplikt*. Till den del sekretessbestämmelserna innebär tystnadsplikt medför de en begränsning av yttrandefriheten enligt regeringsformen eller enligt den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.[36]

[35] Jfr beträffande den beskrivning som ges här prop. 2012/13:192 s. 7 ff.
[36] Vid konkurrens mellan flera tillämpliga sekretessbestämmelser i ett enskilt fall är huvudregeln att den eller de bestämmelser enligt vilka uppgiften är sekretessbelagd har företräde framför bestämmelser enligt vilka uppgiften ska lämnas ut (7 kap. 3 § OSL).

Sekretess gäller som huvudregel inte bara i förhållande till enskilda utan *också mellan myndigheter* samt inom en myndighet, om där finns olika verksamhetsgrenar som är att betrakta som självständiga i förhållande till varandra (8 kap. 1 och 2 §§ OSL). I vissa fall måste dock myndigheter kunna utbyta information för att kunna utföra sina uppgifter. Sekretessregleringen innehåller därför särskilda sekretessbrytande bestämmelser. Dessa har utformats efter en intresseavvägning mellan myndigheternas behov av att utbyta uppgifter och det intresse som den aktuella sekretessbestämmelsen avser att skydda.

En begäran att få ta del av en allmän handling ska göras hos den myndighet som förvarar handlingen (2 kap. 14 § första stycket TF). Det är också denna myndighet som enligt huvudregeln ska pröva begäran (2 kap. 14 § andra stycket TF och 6 kap. 2 § OSL). Utför en myndighet en teknisk uppgift så att en handling blir förvarad där och är den att anse som allmän kan en begäran om att få ta del av handlingen alltså göras hos den myndigheten.

5.1.2 Sekretessbestämmelsernas uppbyggnad

En sekretessbestämmelses tillämplighet begränsas i regel av tre rekvisit. Dessa tre rekvisit anger sekretessens föremål, dess räckvidd och dess styrka.

Sekretessens *föremål* är den information som kan hemlighållas och anges i lagen genom ordet ”uppgift” tillsammans med en mer eller mindre långtgående precisering av uppgiftens art, t.ex. uppgift om enskilds personliga förhållanden. En sekretessbestämmelses *räckvidd* bestäms normalt genom att det i bestämmelsen preciseras att sekretessen för de angivna uppgifterna bara gäller i en viss typ av ärende, i en viss typ av verksamhet eller hos en viss myndighet. Vissa sekretessbestämmelser har emellertid en obegränsad räckvidd. Uppgiften kan då hemlighållas oavsett var den förekommer. Som exempel kan nämnas de s.k. minimiskyddsbestämmelserna i 21 kap. till skydd för enskildas personliga förhållanden.

Sekretessens *styrka* bestäms i regel med hjälp av s.k. skaderekvisit. Man skiljer mellan raka och omvända skaderekvisit. Vid raka skaderekvisit är utgångspunkten att uppgifterna är offentliga och att sekretess bara gäller om det kan antas att en viss skada uppkommer om uppgiften röjs. När skälen för sekretess väger särskilt tungt i förhållande till insynsintresset används i stället omvända

skaderekvisit. I ett sådant fall är utgångspunkten att uppgifterna omfattas av sekretess och att en uppgift får lämnas ut endast om det står klart att uppgiften kan röjas utan att viss skada uppstår. Sekretessen enligt en bestämmelse kan även vara absolut. I ett sådant fall ska de uppgifter som omfattas av bestämmelsen hemlighållas *utan någon skadeprövning* om uppgifterna begärs ut. Det förekommer också bestämmelser som inte innehåller skaderekvisit, men som i stället innehåller andra typer av rekvisit som beskriver under vilka förutsättningar sekretess gäller.

5.1.3 Rätten att meddela och offentliggöra uppgifter

Som nämns i avsnitt 5.1.1 innebär sekretess såväl handlingssekretess som tystnadsplikt. Den rätt att meddela och offentliggöra uppgifter som följer av 1 kap. 1 § TF och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen (YGL) har som huvudregel företräde framför den tystnadsplikt som följer av en sekretessbestämmelse. Nämnda rätt har dock aldrig företräde framför den handlingssekretess som följer av samma bestämmelse (7 kap. 3 § första stycket 2 och 5 § TF och 5 kap. 1 § första stycket och 3 § 2 YGL). Det kan således vara tillåtet att muntligen lämna en uppgift till en journalist eller att själv publicera uppgiften, men det är aldrig tillåtet att med stöd av rätten att meddela och offentliggöra uppgiften lämna den allmänna handling som den sekretessbelagda uppgiften framgår av till en journalist eller att själv publicera handlingen.

I ett antal fall har emellertid även tystnadsplikten företräde framför rätten att meddela och offentliggöra uppgifter. I dessa fall är således rätten att meddela och offentliggöra uppgifter helt inskränkt. Vissa av dessa situationer är reglerade direkt i tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Av 7 kap. 3 § 3 TF respektive 5 kap. 3 § 3 YGL följer vidare att det inte är tillåtet att med stöd av rätten att meddela och offentliggöra uppgifter uppsåtligen åsidosätta en tystnadsplikt i de fall som anges i en särskild lag. Den särskilda lag som avses är offentlighets- och sekretesslagen (13 kap. OSL, slutet av varje kapitel i lagens fjärde-sjätte avdelningar samt lagens sjunde avdelning).

Varje gång en ny sekretessbestämmelse införs måste lagstiftaren överväga om den tystnadsplikt som följer av den föreslagna sekretessbestämmelsen bör ha företräde framför rätten att meddela och offentliggöra uppgifter. Utgångspunkten är att stor återhållsamhet

ska iakttas vid prövningen av om undantag från rätten att meddela och offentliggöra uppgifter bör göras i ett särskilt fall. Den enskilda sekretessbestämmelsens konstruktion kan ge viss vägledning.

När det är fråga om bestämmelser om absolut sekretess kan det finnas större anledning att överväga undantag från rätten att meddela och offentliggöra uppgifter än i andra fall. Detsamma gäller i viss mån sekretessbestämmelser med ett omvänt skaderekvisit (prop. 1979/80:2 Del A s. 111 f.).

5.2 Tystnadsplikt för vissa tjänster

Delegationens bedömning: Det behövs endast en tystnadsplikt i det allmännas verksamhet för att tillhandahålla it-drift och elektroniska förvar för någon annans räkning.

Det är som framgått av avsnitt 3.3 numera ett vedertaget juridiskt synsätt och en utbredd praxis inom offentlig förvaltning att tillhandahålla elektroniskt förvar åt användare av myndigheters elektroniska tjänster. Användaren utgår närmast självklart från att ingen annan får bereda sig tillgång till den nyttoinformation som finns där och att en myndighet och dess personal inte heller på annat sätt får röja dessa uppgifter. Samtidigt har det som beskrivits i avsnitt 3.4 blivit en utbredd myndighetspraxis att utkontraktera hela eller delar av it-driften. När sådan teknisk bearbetning och lagring utförs av ett privaträttsligt subjekt kan en tystnadsplikt säkerställas genom avtal.

När en myndighet utför teknisk bearbetning och lagring för en annans räkning kan myndighetens personal emellertid inte genom avtal förbjudas att röja uppgifter. Sådana regler för offentliga funktionärer ges i stället i lag genom bestämmelser om sekretess. När det ska bedömas vilket behov som finns av sekretess blir det avgörande om berörda handlingar är att anse som *allmänna* i en myndighets verksamhet, för att tillhandahålla

- it-drift för annans räkning,
- elektroniskt förvar för användare av it-baserade tjänster, och
- hjälptjänster eller presentationstjänster.

Begärs en handling utlämnad med stöd av reglerna om handlingsoffentlighet behöver myndigheten ta ställning till om handlingen är förvarad och inkommen till eller upprättad hos myndigheten samt om något undantag enligt 2 kap. TF från handlingsoffentlighet är tillämpligt.

Skulle en handling vara allmän behöver myndigheten bedöma om den innehåller någon sekretessreglerad uppgift. Kan detta inte slås fast utan en närmare granskning och är inget undantag från allmän handling tillämpligt behöver myndigheten *ta del* av informationen i användarens elektroniska förvar[37], dels för att avgöra huruvida ett påstående om att en begärd handling finns där är riktigt, dels för att bedöma om sekretess gäller för den. En sådan genomgång av information i en användares elektroniska förvar kan emellertid varken förenas med förvarets ändamål eller med skyddet för innehavarens privatliv.

En liknande utmaning uppkommer vid utkontraktering av it-drift till en myndighet, om det inte utan närmare granskning kan slås fast att ett undantag enligt 2 kap. TF är tillämpligt. Begärs en handling utlämnad, under påstående att handlingen är allmän, hos den myndighet som tillhandahåller tjänsten, behöver den tjänstelevererande myndigheten behandla uppgifterna för att bedöma frågan om handlingsoffentlighet. Om sådana åtgärder skulle visa sig bli nödvändiga vid utkontraktering av it-drift till en myndighet torde valet mellan en offentlig respektive en privat leverantör för driften utfalla så att myndigheternas samverkan på området blir begränsad.

Frågan om tillämpningsområdet för 2 kap. 10 § första stycket TF vid utkontraktering av it-drift och tillhandahållande av elektroniskt förvar har redan behandlats i avsnitt 4.4.2 och 4.5.6. Enligt delegationens bedömning får detta undantag från allmän handling anses gälla både för sådan endast teknisk bearbetning och teknisk lagring som utförs vid utkontraktering av it-drift till en myndighet och för handling i ett elektroniskt förvar som en myndighet tillhandahåller åt annan.

En sekretessreglering för utkontrakterad it-drift och för elektroniskt förvar behövs därmed endast i form av en tystnadsplikt i det allmännas verksamhet för att tillhandahålla sådana tjänster.

[37] Se vidare avsnitt 3.2 angående s.k. nyttoinformation.

Som redovisats i avsnitt 4.4.3 är situationen en annan när en myndighet förvarar en handling för att tillhandahålla en presentations- eller en hjälptjänst. Det blir då inte fråga om endast teknisk bearbetning eller lagring för annans räkning utan det centrala är antingen information som myndigheten ställer samman och visar i en presentationstjänst eller den – ofta muntliga – information som myndigheten ger om hur ett problem kan avhjälpas eller hur vissa uppgifter kan förstås.

En sekretessreglering behövs därmed, för uppgifter i hjälptjänster och presentationstjänster, såväl i form av handlingssekretess som tystnadsplikt; se vidare avsnitt 6.

5.3 Tystnadspliktens föremål bör vidgas

Delegationens bedömning: Tystnadspliktens föremål i verksamhet för att tillhandahålla it-drift och elektroniskt förvar ska vidgas så att uppgift om en enskilds personliga eller ekonomiska förhållanden skyddas även om uppgiften inte är en personuppgift.

Det är en förutsättning för att myndigheter ska kunna tillhandahålla elektroniskt förvar – i vart fall på sikt – att innehavaren av förvaret kan veta att de uppgifter som finns där inte får röjas, vare sig det sker muntligen, genom utlämnande av en handling eller på något annat sätt. Detta behov av skydd föreligger även om samma handling, efter att ha getts in, skulle finnas också i myndighetens verksamhetssystem[38] och där anses vara allmän handling. Det är *förvaret* som innehavaren ska ha för sig själv, vilket kan jämföras med att information i en bostad är privat.

På samma sätt behöver ett företag kunna ha ett elektroniskt förvar för sig själv. Detta gäller oberoende av om det är fråga om en arbetsyta på en server eller ett tjänsterum på ett företags kontor. En handling hos ett företag blir inte tillgänglig för utomstående för att den finns på ett kontor i en fastighet som ägs av en myndighet. Dessutom gäller skyddet för handlingen oberoende av om den innehåller någon integritetskänslig uppgift. På motsvarande sätt

[38] Jfr avsnitt 3.2, not 4.

finns ett behov av skydd mot att en myndighet eller dess personal bereder sig tillgång till ett företags elektroniska förvar.

Skulle en befattningshavare ha råka ta del av en uppgift i ett elektroniskt förvar, t.ex. råkat se en uppgift i samband med att han eller hon rättat ett fel i det tekniska systemet eller vidtagit en åtgärd som är nödvändig från informationssäkerhetssynpunkt, behöver det finnas ett förbud mot att röja uppgiften, oavsett om röjandet sker muntligen, genom utlämnande av handling eller på något annat sätt.

På motsvarande sätt behöver det finnas en tystnadsplikt för personalen hos myndighet som sköter it-drift åt någon annan så att de inte får röja de uppgifter som behandlas. Sådan utkontraktering av it-drift till myndighet är numera omfattande; jfr vad som sagts i avsnitt 3.4 om Statens servicecenter och projektet Verksamt.

Enligt 40 kap. 5 § OSL gäller sekretess i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av personuppgifter som avses i personuppgiftslagen (1998:204) för uppgift om en enskilds personliga eller ekonomiska förhållanden.

Denna tystnadsplikt är absolut, vilket innebär att uppgifter som omfattas av sekretessen ska hemlighållas utan någon skadeprövning. Det kan därmed inte råda någon tvekan om att sekretessens *styrka* är tillräcklig för elektroniskt förvar och för utkontraktering av it-drift. Frågan är emellertid om sekretessens *räckvidd* kan anses tillräcklig när den enligt 40 kap. 5 § OSL begränsats till enbart teknisk bearbetning eller lagring för annans räkning.

Vi har i avsnitt 4.4.2 och 4.5.6. gjort den bedömningen att undantaget i 2 kap. 10 § första stycket TF för handling som förvaras hos en myndighet *endast* som led i teknisk bearbetning eller teknisk lagring för annans räkning är tillämpligt även på uppgifter i ett elektroniskt förvar och uppgifter som en myndighet behandlar genom att tillhandahålla tjänster för it-drift. Det för 2 kap. 10 § första stycket TF centrala rekvisitet ”endast” avses ha samma innebörd som begreppet ”enbart” i 40 kap. 5 § OSL. Därmed får även sekretessens räckvidd anses tillräcklig för de behov som elektroniskt förvar och utkontraktering av it-drift aktualiserar.

Sekretessens *föremål* – dvs. den information som kan hemlighållas – har emellertid begränsats, inte bara till uppgifter om enskildas personliga eller ekonomiska förhållanden utan också till *personuppgifter* som avses i personuppgiftslagen (1998:204), förkortad PuL. Den i 40 kap. 5 § OSL föreskrivna tystnadsplikten är därmed alltför begränsad. Ett stort antal elektroniska förvar tillhandahålls redan åt

juridiska personer där de bl.a. upprätta inlagor med uppgifter som inte får komma till utomståendes kännedom, i vart fall inte före det att handlingen har kommit in till myndighet.

Delegationen föreslår därför att tystnadspliktens föremål enligt 40 kap. 5 § OSL utvidgas så att uppgifter om enskildas personliga eller ekonomiska förhållanden skyddas, även om de inte utgör personuppgifter enligt personuppgiftslagen.

5.4 Bestämmelsens utformning

5.4.1 Bakgrund

Bestämmelsen i 40 kap. 5 § OSL hade sin motsvarighet i 9 kap. 7 § sekretesslagen (1980:100). Även där gällde regleringen – efter ändringar i samband med personuppgiftslagens införande – endast för personuppgifter. Dessförinnan gällde bestämmelsen emellertid för *personregister* enligt datalagen. Ett sådant register kunde också innehålla uppgifter om juridiska personer eftersom det med personregister enligt 1 § datalagen menades ”register, förteckning eller andra anteckningar som föres med hjälp av automatisk databehandling och som innehåller personuppgift som kan hänföras till den som avses med uppgiften”. Denna definition träffade alla former av strukturerade behandlingar som *till någon del* innehöll uppgifter om enskilda personer. Eftersom även bolag omfattas av definitionen ”enskild” i sekretesslagen gav sekretessregleringen i sin ursprungliga lydelse alltså ett skydd även för uppgifter om juridiska personer – så snart uppgifterna förekom i ett register tillsammans med personuppgifter.

Den inskränkning i tystnadsplikten som blev följden av vad som i lagmotiven beskrevs endast som en justering med anledning av att personuppgiftslagen skulle ersätta datalagen synes inte ha uppmärksammats. Rena uppgifter om juridiska personer föll därmed utanför sekretessregleringen. När sekretesslagen infördes 1980 utfördes så gott som all behandling med hjälp av ADB hos myndigheter i register som innehöll vissa på förhand definierade faktauppgifter om enskilda. Som exempel kan nämnas ersättningsnivåer, inkomster, adress och fattade beslut. Någon digital behandling av uppgifter i löpande text förekom knappast. I stället skrevs domar och beslut på skrivmaskin. Meddelanden expedierades i brevform med vanlig post. Den som ville kontakta en myndighet

skriftligen sände brev med Postverket. Vid muntlig kommunikation förde tjänstemannen tjänsteanteckningar i pappersjournaler eller direkt på aktkappor. Inom förvaltningsmyndigheter förekom vanligen att enklare beslut sattes upp i form av s.k. tergalresolution, dvs. att beslut tecknades med penna på den handling som innehöll ansökan.

Efter sekretesslagens tillkomst har utvecklingen gått snabbt och idag sker så gått som all behandling av uppgifter om enskilda i digital miljö. Myndigheterna kommunicerar också vanligtvis elektroniskt med enskilda. Information finns på myndigheternas webbplatser och nära nog alla myndigheter som har omfattande kontakter med enskilda tillhandahåller elektroniska tjänster där enskilda kan utföra sina ärenden. Myndigheter använder i betydande omfattning också digitaliserad akthantering där beslut, skrivelser och andra handlingar bevaras digitalt. Detta gäller även för tjänsteanteckningar. Det säger sig själv att behovet av integritetsskydd i denna miljö inte kan begränsas till den information som råkar befinna sig i vad som kan kallas ett register.

När sekretesslagen infördes uttalades bl.a. följande angående sekretess för registerbehandlingar (prop. 1979/80:2 s 272):

> Också i fråga om andra myndigheter än datainspektionen finns behov av sekretessbestämmelser i samband med personregistrering med hjälp av ADB. Någon regel som generellt skulle föreskriva sekretess för personuppgifter i dataregister kan dock naturligen inte införas. En sådan bestämmelse skulle ju på viktiga områden försätta offentlighetsprincipen ur spel.
>
> I 13 § första stycket datalagen föreskrivs att registeransvarig eller annan som har tagit befattning med personregister inte obehörigen får yppa vad han till följd härav har fått veta om enskilds personliga förhållanden. Regeln är i och för sig tillämplig också på myndighet. Den har därvid dock den begränsningen att tystnadsplikten inte kan anses sträcka sig längre än de inskränkningar som gäller i fråga om rätten att skriftligen lämna ut uppgift ur registret. Detta innebär med andra ord att tystnadsplikten inte gäller registeruppgift som ingår i en offentlig ADB-upptagning.
>
> Det finns skäl att på ett begränsat område införa en sekretessbestämmelse i den nya sekretesslagen som kan sägas i viss mån svara mot den berörda bestämmelsen i datalagen. Sålunda är det inte godtagbart att sekretess skulle saknas inom en datacentral med ställning av myndighet, för personuppgifter i sådant personregister som bearbetas eller lagras för enskild kunds räkning. För bearbetning och förvaring av myndighets ADB-register är behovet av särskild sekretess inte lika framträdande, eftersom ofta en för det berörda förvaltningsområdet gällande sekretessbestämmelse skulle bli tillämplig. Tillräcklig anled-

> ning att skilja mellan bearbetning m.m. för enskilds och för myndighets räkning synes dock inte föreligga. Det kan inte heller vara ändamålsenligt att personal som har rent tekniska uppgifter skall behöva tillämpa olika sekretessbestämmelser för skilda delar av sitt arbetsmaterial.
>
> Med hänvisning till det anförda har i promemorian föreslagits att sekretess skall gälla i myndighets verksamhet som endast avser teknisk bearbetning eller teknisk lagring för annans räkning, för uppgift om enskilds personliga eller ekonomiska förhållanden. Sekretessen har föreslagits bli absolut, d.v.s. något skaderekvisit ställs inte upp som villkor för sekretessen. Förslaget har inte mött några invändningar under remissbehandlingen. Bestämmelsen i förevarande paragraf överensstämmer med promemorieförslaget.

Det ansågs alltså finnas behov av ett integritetsskydd för tekniska behandlingar oavsett om de rörde personuppgifter eller en blandning av personuppgifter och uppgifter om juridiska personer. Ett bärande skäl bakom denna sekretess har varit att den personal som biträder vid bearbetningen eller lagringen inte ska behöva tillämpa de skiftande sekretessregler som kan gälla hos de olika myndigheter där uppgifterna hör hemma; jfr hur den sekretess som gäller för personal i en myndighets telefonväxel – se 40 kap. 4 § OSL, tidigare 12 kap. 7 § sekretesslagen (1980:100) – är absolut och att det inte ansetts lämpligt att till växeltelefonisten överlämna att avgöra om en sekretessregel är tillämplig i det enskilda fallet (prop. 1979/80:2 Del A s. 314).

Att sekretessen på datalagens tid inte kom att omfatta annat än personregister torde ha berott på att definitionen av personregister i datalagen omfattade även digitala behandlingar utanför konventionella register. Det bör vidare framhållas att den analys lagstiftaren utförde, i samband med antagande av 1980 års sekretesslag rörande den bestämmelse vilken inflöt som 9 kap. 7 §, avsåg behovet av skydd för *personuppgiftsbehandling* med ADB. Mot bl.a. den bakgrunden får de citerade motivuttalandena förstås, om att det inte var aktuellt att generellt sekretessbelägga personuppgifter i dataregister.

Den avvägning som låg bakom bestämmelsen, mellan behovet av sekretess på den ena sidan och behovet av offentlighet på den andra, framstår därmed inte som heltäckande, i vart fall inte när det beaktas hur it används idag. Något adekvat skydd finns inte för sådan teknisk bearbetning och lagring för annans räkning som numera blivit vanlig på myndighetsområdet. Den utkontraktering av it-drift som numera utgör en central del i myndigheternas sam-

verkan inom förvaltningsområdet präglar exempelvis Statens servicecenters uppdrag enligt förordningen (2012:208) med instruktion för Statens servicecenter. Behov av skydd blir som framgått särskilt tydligt när en myndighet tillhandahåller elektroniskt förvar åt enskilda; jfr vad som redovisats i avsnitt 4.5.1 angående skyddet för privatlivet. Tillhandahålls motsvarande förvar åt enskilda genom ett privaträttsligt subjekt kan emellertid sekretess, innefattande tystnadsplikt, uppnås fullt ut genom avtal.

5.4.2 Andra regler om sekretess

Delegationens bedömning: Andra regler om sekretess ger inte heller ett tillräckligt skydd för uppgifter i elektroniskt förvar eller vid utkontraktering av it-drift till en myndighet.

Även andra bestämmelser i offentlighets- och sekretesslagen kan bli tillämpliga på uppgifter i ett elektroniskt förvar och vid utkontraktering av it-drift till en myndighet. Vanligtvis föreskrivs emellertid begränsningar av sekretessens räckvidd till t.ex. uppgifter i viss verksamhet eller i vissa ärenden. I Skatteverkets ärendetjänster uppkommer frågan om den sekretess som enligt 27 kap. 1 § OSL gäller *i verksamhet* som avser bestämmande av skatt eller fastställande av underlag för bestämmande av skatt, kan anses gälla redan i ett serviceskede när den skattskyldige upprättar ett utkast i ett elektroniskt förvar som verket tillhandahåller. Föreligger verksamhet av där angivet slag när det är fråga endast om uppgifter i utkast till handlingar som inte har getts in i förvaltningsrättslig mening och som verket inte får ta del av – dvs. innan något ärende som rör den handlingen har blivit anhängiggjort hos Skatteverket?

Motsvarande fråga aktualiseras när en ärendetjänst tillhandahålls av Pensionsmyndigheten. Kan sekretess som enligt 28 kap. 1 § OSL gäller för uppgift som förekommer *i ärende* enligt viss närmare angiven lagstiftning anses gälla innan något sådant ärende har anhängiggjorts? En sådan tolkning framstår som extensiv.

Det finns vidare regler om sekretess för uppgifter som hanteras inom ramen för *uppdrag som bygger* på *förutsättningen att uppgifterna inte röjs*. I 29 kap. OSL ges regler om sekretess för allmän samfärdsel,

- för postförsändelse (1 §), hos bl.a. myndighet som bedriver postverksamhet för uppgift om en särskild postförsändelse,

- elektroniskt meddelande (2 §), hos en myndighet som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst för uppgift om innehållet i ett elektroniskt meddelande eller annan uppgift som angår ett särskilt elektroniskt meddelande, och
- annan samfärdsel (3 §), hos myndighet som handhar allmän samfärdsel för sådan uppgift om en enskilds förbindelse med samfärdselverksamheten.

Sekretessen för postförsändelse gäller dock endast för traditionell papperspost och skyddet för elektroniskt meddelande gäller endast hos en myndighet som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. En myndighet som tillhandahåller ett elektroniskt förvar eller genom utkontraktering hanterar en annan myndighets uppgifter tillhandahåller emellertid inte därigenom en sådan elektronisk kommunikationstjänst som omfattas av sekretessregleringen för elektroniskt meddelande.

I detta sammanhang bör också nämnas att sekretess gäller enligt 40 kap. 2 § OSL i notarius publicus verksamhet, som följer av lag eller annan författning för uppgift som det *kan antas att den rättssökande har förutsatt ska bli behandlad förtroligt,* och att det enligt 40 kap. 4 § OSL gäller sekretess för personal i en myndighets *telefonväxel,* för uppgift som har inhämtats vid tjänstgöringen och som avser telefonsamtal till eller från någon annan person hos myndigheten, oberoende av om uppgiften är offentlig i myndighetens verksamhet i övrigt. Avsikten är i dessa fall, liksom vid användningen av ett elektroniskt förvar, att material som avsändare och mottagare har utgått från ska behandlas förtroligt inte får röjas, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. Enskilda lämnar uppdragen och använder tjänsterna under den förutsättningen.

Vad som utmärker elektroniskt förvar hos en myndighet är att innehavaren uppfattar det som sitt – som om det var en del av hans eller hennes egen it-miljö, kanske till och med som om det fanns i användarens egen dator. Detta förvar hade tekniskt lika gärna kunnat tillhandahållas av ett företag eller en annan myndighet än den som tillhandahåller den ärendetjänst där det förvaret används, t.ex. av Statens servicecenter.

Information i en användares elektroniska förvar är vidare som framgått av privat natur. Innehavaren av förvaret har uppgifter och

handlingar där för sin egen räkning och utgår från att ingen annan ska få bereda sig tillgång till förvaret och läsa eller annars använda det som finns där. Syfte med förvaret är att det ska fungera för användaren på samma sätt som om personen hade haft handlingarna i sin bostad eller på sitt kontor. De handlingar som finns där ska alltså vara skyddade från insyn oberoende av om de innehåller skyddsvärda uppgifter; se vidare avsnitt 4.5.1 angående skyddet för privatlivet.

Det förhållandet att utkast, som tas fram i ett sådant förvar, kan komma att ges in till en myndighet, förändrar inte ändamålet med det elektroniska förvaret. Syftet är att ge de uppgifter som den enskilde mottar, förvarar och bearbetar där samt lämnar vidare därifrån ett tillräckligt skydd.

På liknande sätt brukar tanken finnas, när en myndighet överväger att utkontraktera t.ex. sin it-drift, att förutsättningarna ska kunna vara desamma oberoende av om uppdraget ges till en myndighet eller till ett privaträttsligt subjekt. När en myndighet anlitar en annan myndighet som underleverantör eller när en enskild har ett elektroniskt förvar i en myndighets e-tjänst förutsätts emellertid som framgått också att den personal som sköter de tekniska systemen inte röjer de uppgifter som behandlas där.

I privaträttslig miljö är en tystnadsplikt grundad på avtal det normala. För myndigheter gäller i stället de förbud mot att röja eller utnyttja en uppgift som föreskrivs i offentlighets- och sekretesslagen eller enligt lag eller förordning som offentlighets- och sekretesslagen hänvisar till. Den personkrets för vilken regleringen i offentlighets- och sekretesslagen gäller utgörs inte bara av myndighetens anställda. Den gäller även för personer som har uppdrag där, t.ex. för it-drift, och som har en sådan anknytning till myndigheten att de kan sägas delta i dennas verksamhet (2 kap. 1 § OSL). För denna kategori av personer finns bestämmelser om yttrandefrihet som inte medger att tystnadsplikt införs genom avtal.

5.4.3 Särskilt om uppdragssekretess

Delegationens bedömning: Uppdragssekretess kan inte heller ge det skydd som behövs vid teknisk bearbetning eller lagring för annan.

Enligt 31 kap 12 § OSL gäller sekretess i samband med uppdragsverksamhet som myndigheter bedriver för enskildas räkning. Bestämmelsen föreskriver sekretess för uppgift som avser provning, bestämning av egenskaper eller myckenhet, värdering, vetenskaplig, teknisk, ekonomisk eller statistisk undersökning eller annat sådant *uppdrag* som myndighet utför för en enskilds räkning om det kan antas att uppdraget lämnats under förutsättning att uppgiften inte röjs. Sekretessen är absolut och meddelarfrihet gäller inte.

Att det är en myndighet som utför uppdraget och att det lämnats under förutsättning att uppgifterna inte röjs stämmer väl överens med de utgångspunkter från vilka elektroniskt förvar tillhandahålls och utkontraktering sker till myndighet av it-drift. En begränsning gäller emellertid till s.k. uppdragsverksamhet. Typiska myndigheter att tillämpa bestämmelsen har angetts vara universitet och högskolor, SCB, Konsumentverk eller Boverket.

Myndigheter som tillhandahåller elektroniskt förvar behandlar visserligen de uppgifter som finns där inom ramen för ett uppdrag, men ett uppdrag att utföra sådan teknisk lagring och bearbetning av information synes inte vara att jämställa med undersökning av vetenskaplig, teknisk eller statistisk karaktär eller utgöra ”… annat sådant uppdrag”, som det uttrycks i lagtexten. Någon vägledning ges inte i motiven till OSL eller sekretesslagen (1980:100), från vilken bestämmelsen (då i 8 kap 9 §) överförts utan ändring i sak.

Högsta Förvaltningsdomstolen har övervägt begreppet uppdrag i HFD 2011 not. 28 och konstaterat att det i begreppet måste ligga att det är fråga om en uppgift som kräver vissa arbetsinsatser av inte alltför obetydligt slag. Domstolen uttalade vidare att resultatet skulle redovisas i en rapport eller liknande. Eftersom det är fråga om ett notismål kan knappast några långtgående slutsatser dras. Avgörande torde vara, inte själva formatet för redovisning av uppdraget utan snarare omfattningen av redovisningen och av uppdraget, detta eftersom domstolen från tillämpningsområdet uteslöt fall där det bara är fråga om att svara på en enstaka faktafråga eller att upplysa om innehållet i en rättsregel.

I motiven till sekretesslagen (prop. 1979/80:2 s 238) angavs att paragrafen avsågs omfatta situationer där sekretessen var närmast av förtroendekaraktär, där det i situationen ligger att enskilda knappast skulle anlita myndigheten, om de inte kunde vara säkra på att få samma skydd som hos ett privat företag. I denna del är överensstämmelsen sannolikt fullständig med användares förväntningar på skyddet för de uppgifter som finns i ett elektroniskt förvar.

Den aktuella regelns angivna syfte och Högsta Förvaltningsdomstolens ovan nämnda avgörande talar för att man vid tolkning av denna bestämmelse som avgörande bör se snarare omfattningen och den förtroendefulla karaktären av de uppgifter en enskild låter en myndighet sköta än att det måste vara fråga om vissa analyser och undersökningar som ska rapporteras. Det kan mot denna bakgrund inte helt uteslutas att bestämmelsen i något fall skulle kunna bli tillämplig även på uppgifter som behandlas inom ramen för varaktiga elektroniska förvar. Det synes inte heller vara någon direkt förutsättning för tillämpning av bestämmelsen att varje enskild uppgift har lämnats till myndigheten av den enskilde. I den äldre motsvarigheten till bestämmelsen (27 § i 1937 års sekretesslag) fanns en formulering som gjorde att bestämmelsen omfattade även ”införskaffande eller meddelande av upplysningar till enskildas tjänst”. Någon saklig ändring har inte avsetts vare sig i sekretesslagen eller OSL. Men detta uttryck har tagits bort och ersatts av uttrycket ”annat sådant uppdrag” (se prop. 1979/80:2 s. 237 f., Ds Ju 1977:11 s. 507 f. och SOU 1975:22 s. 216 ff.).

Någon säker slutsats om huruvida bestämmelsen kan bli tillämplig i anknytning till elektroniskt förvar kan inte dras. Uppdragssekretessen kan därmed inte – utan en ändring i lag eller ett klarläggande genom rättspraxis – läggas till grund för skyddet av uppgifter i elektroniskt förvar. Något stöd för att tillämpa denna bestämmelse vid t.ex. it-drift och liknande för annan myndighet finns inte heller. De praktiska förutsättningarna påminner emellertid om dagens förhållanden vid utkontraktering där det kan ingå i uppdraget att lämna vissa rapporter, t.ex. vid it-incidenter.

5.4.4 Sekretessen bör inte begränsas till personuppgifter

Delegationens förslag: Sekretess ska gälla i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning för uppgift om en enskilds personliga eller ekonomiska förhållanden.

Utkontraktering av it-drift har som framgått blivit en central del i myndigheters samverkan för en fungerande elektronisk förvaltning. Regeringen har gett vissa myndigheter i uppdrag att ge sådant stöd och för många myndigheter är utkontraktering en central del i

hanteringen eftersom it-baserade funktioner kräver specialistkompetens och avancerade tekniska hjälpmedel som med hänsyn till utvecklingstakten knappast kan hanteras av varje myndighet för sig. Regeringen har också i olika sammanhang betonat vikten av att myndigheter samverkar kring gemensamma funktioner och tjänster och delar på resurser och investeringar över myndighetsgränser.

Enligt sin instruktion har flera myndigheter också i uppdrag att tillhandahålla it-baserade funktioner och tjänster åt andra; se t.ex. förordningen (2012:208) med instruktion för Statens servicecenter, förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte, förordningen (2010:1497) med instruktion för E-legitimationsnämnden och förordningen (2009:1078) om tjänster på den inre marknaden.[39]

Det har vidare blivit en allmänt spridd myndighetspraxis att utforma e-tjänster så att myndigheter tillhandahåller elektroniskt förvar åt dem som använder tjänsten. Inte förrän innehavaren av ett sådant förvar har avsänt en handling därifrån så att den nått ett anvisat mottagningsställe avses handlingen finnas hos myndigheten för annat än teknisk bearbetning eller teknisk lagring.

Vid sådana förhållanden finns, som framgått av avsnitt 5.2 och 5.3, ett behov av att vidga föremålet för tystnadsplikten. Regeringens mål för it-politiken är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. För att uppnå detta krävs dels en ökad specialisering och samverkan mellan myndigheter så att den tekniska kompetens som finns hos en myndighet kan nyttjas av flera, dels en ökad digital delaktighet i samhället så att fler vill och vågar använda digitala tjänster.

En nödvändig del i denna utveckling är att myndigheter inför fler elektroniska tjänster som vanliga användare upplever att de har

[39] Här bör också nämnas att det enligt 4 § första stycket 4 förordningen (2007:937) med instruktion för Försvarets radioanstalt är en uppgift för myndigheten att genom it-säkerhetsanalyser, efter begäran, ge stöd åt statliga myndigheter som hanterar viss information. Ett sådant uppdrag innebär en utkontraktering till Försvarets radioanstalt av den drabbade myndighetens granskning av sin informationssäkerhet. Det kan knappast förutses vad tillhörande insamling och överlämning av data inom ramen för uppdraget kan komma att innefatta för uppgifter. På motsvarande sätt föreskrivs i 11 a § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap (MSB) att myndigheten ska svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera IT-incidenter och att MSB i detta arbete ska agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade. Även här aktualiseras analyser och annan hjälp genom utkontraktering till en myndighet.

nytta av. Sådana tjänster måste vara enkla att bruka och göra det möjligt att påbörja arbetet med t.ex. en ansökan till en myndighet vid en tidpunkt som passar den enskilde. Det behöver också gå att spara underlaget när användaren så önskar för att kunna fortsätta arbetet vid en lämplig tidpunkt utan att behöva börja om från början. Arbetsmaterial och andra handlingar som en enskild förvarar hos en myndighet endast för sin egen räkning måste härvid ges ett skydd som gör att användaren kan känna trygghet och säkerhet.

Detta skyddsbehov är starkt uttalat för såväl uppgifter i användares elektroniska förvar som uppgifter vilka en myndighet behandlar för en annan myndighets räkning vid utkontraktering av it-drift. Delegationen föreslår därför att den år 1998 gjorda inskränkningen i sekretessen, som blivit följden av vad som i lagmotiven (prop. 1997/98:44 s. 147) beskrivits som endast en justering med anledning av att personuppgiftslagen ersatte datalagen, tas bort. Ett sådant återinförande av sekretess, och därmed av tystnadsplikt för befattningshavare, kan ske genom att sekretessen enligt till 40 kap. 5 § OSL, anges avse även uppgifter som inte är personuppgifter.

Med hänsyn till den vida tolkning begreppet personregister gavs i praxis rörande datalagen kan delegationens förslag knappast innebära annat än en marginell utvidgning i förhållande till området för 9 kap. 7 § sekretesslagen (1980:100) vid tiden före ikraftträdandet av personuppgiftslagen (1998:204). Det är, och var, ovanligt att uppgifter om juridiska personer blev behandlade utan anknytning till någon personuppgift, t.ex. en uppgift om företrädare för en juridisk person. Ett sådant skydd behövs både för den myndighetssamverkan som i stor omfattning bedrivs genom utkontraktering av it-drift mellan myndigheter och för elektroniskt förvar som myndigheter erbjuder användare.

Sekretess bör därmed gälla i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning för uppgift om en enskilds personliga eller ekonomiska förhållanden.

När en myndighet utkontrakterar sin it-drift till en annan myndighet framstår det med dagens infrastruktur för kommunikation som rimligt att den som vill begära ut en uppgift får vända sig till den myndighet som svarar för den verksamhet där uppgiften hör hemma – inte till den som endast har en teknisk uppgift. Utför en myndighet teknisk bearbetning eller lagring av uppgifter för ett organ som inte omfattas av reglerna om handlingsoffentlighet (se

2 kap. 3-5 §§ OSL) gör sig kraven på insyn enligt reglerna om handlingsoffentlighet inte gällande beträffande de uppgifterna.

5.5 Överföring av sekretess

Delegationens förslag: Får en myndighet i sin verksamhet för enbart teknisk bearbetning eller teknisk lagring för en annan myndighets räkning en uppgift som av hänsyn till ett allmänt intresse är sekretessreglerad där, blir sekretessbestämmelsen tillämplig på uppgiften även hos den mottagande myndigheten.

5.5.1 Mer än personliga eller ekonomiska förhållanden

I en myndighets verksamhet för enbart teknisk bearbetning eller lagring för en annan myndighets räkning kan uppgifter komma att behandlas hos den myndighet till vilken utkontraktering skett (i det följande ”tjänstelevererande myndighet”), som visserligen omfattas av tystnadsplikt hos den myndighet som utkontrakterat sin it-drift (i det följande ”beställande myndighet”), men där *sekretessens föremål är ett annat* än enskilds personliga eller ekonomiska förhållanden. Någon tystnadsplikt för befattningshavare hos den tjänstelevererande myndigheten kan under sådana förhållanden inte följa av 40 kap. 5 § OSL och det är som framgått inte möjligt att införa tystnadsplikt genom avtal.

Frågan blir därmed om den tystnadsplikt som gäller för uppgiften hos den beställande myndigheten kan bli tillämplig även hos den tjänstelevererande myndigheten eller om utkontrakteringen för med sig ett försämrat skydd för uppgifterna, om en myndighet ska leverera tjänsten. Normalt finns det ett behov av en tystnadsplikt för befattningshavare hos tjänstelevererande myndighet när en uppgift är sekretessreglerad hos den myndighet som har beställt tjänsten.

Detta kan åskådliggöras med den sekretessreglering som gäller hos regeringen, Riksbanken och Riksgäldskontoret för uppgift som rör rikets centrala finanspolitik, penningpolitik eller valutapolitik. Skulle utkontraktering ske av teknisk bearbetning eller teknisk lagring av sådan uppgift till en annan myndighet, hos vilken sekretessen enligt 16 kap. 1 § OSL inte gäller, hade en lucka uppstått i sekretessen, om föreskriften i 16 kap. 2 § OSL inte hade funnits.

Där föreskrivs att 1 § blir tillämplig även hos den myndighet som får en uppgift som är sekretessreglerad i 1 §. Det finns emellertid andra bestämmelser om sekretess som har begränsats till t.ex. viss verksamhet hos viss myndighet utan att det har föreskrivits att denna sekretess gäller även hos annan myndighet. Som exempel kan nämnas när sekretess, som gäller hos en myndighet inte skulle gälla hos annan myndighet, som fått uppgiften till sig endast till följd av en utkontraktering av it-driften.

Utkontraktering till en privaträttslig aktör sker regelmässigt under förutsättning att de uppgifter som behandlas inom ramen för uppdraget inte röjs eller annars utnyttjas för något annat ändamål. Detsamma avses gälla vid utkontraktering av it-drift till en myndighet.

Undantaget i 2 kap. 10 § första stycket TF är konstruerat så att resultatet blir detsamma som vid utkontraktering till en privaträttslig aktör: *Handlingar* som förvaras hos den tjänstelevererande myndigheten endast för teknisk bearbetning och lagring blir inte allmän handling där. Någon sådan likställighet mellan utkontraktering till privaträttsliga respektive offentliga aktörer följer emellertid inte av reglerna om *tystnadsplikt* för tjänstelevererande myndigheters personal. Föremålet för sekretessen enligt 40 kap. 5 § OSL – i praktiken tystnadsplikten – är begränsad till personuppgifter som avses i personuppgiftslagen (1998:204) för uppgift om en enskilds personliga eller ekonomiska förhållanden. Även om delegationens förslag till ändring av 40 kap. 5 § OSL genomförs kvarstår en begränsning till uppgifter om enskildas personliga eller ekonomiska förhållanden.

Sekretessregleringen för uppgifter hos en myndighet som beställer en outsourcingtjänst kan avse även annat än uppgift om enskilds personliga eller ekonomiska förhållanden. För sådana fall finns risk för att sekretessen – och därmed tystnadsplikten – inte kommer att gälla om en uppgift blir förvarad hos den tjänstelevererande myndigheten. En och samma uppgift kan därmed omfattas av tystnadsplikt hos beställande myndighet men sakna sådant skydd med avseende på personal hos den myndighet som tillhandahåller tjänsten. Det kan också vara så att uppgiften är sekretessreglerad hos båda myndigheterna men att olika skyddsnivåer kommer att gälla hos dem, t.ex. att sekretessen är absolut hos den ena myndigheten medan ett skaderekvisit gäller hos den andra myndigheten.

5.5.2 Sekretess kan följa med till annan myndighet

Skälet för att sekretessen – och därmed tystnadsplikten – som huvudregel inte följer med en uppgift när den lämnas mellan myndigheter är att behovet av och styrkan i en sekretess inte kan bestämmas enbart med hänsyn till sekretessintresset. Detta intresse måste vägas mot intresset av insyn i myndigheternas verksamhet. Offentlighetsintresset kan således kräva att de uppgifter som behandlas som hemliga hos en myndighet är offentliga hos en annan myndighet som har inhämtat dem hos den förstnämnda myndigheten (prop.1979/80:2 Del A s. 75 f.).

Någon generell bestämmelse om överföring av sekretess från en myndighet till en annan finns därför inte utan har införts endast för särskilda fall. Det finns således primära och sekundära sekretessbestämmelser. Med en primär sekretessbestämmelse menas en bestämmelse om sekretess som en myndighet ska tillämpa på grund av att bestämmelsen riktar sig direkt till myndigheten eller omfattar en viss verksamhetstyp eller en viss ärendetyp som hanteras hos myndigheten eller omfattar vissa uppgifter som finns hos myndigheten. Med en bestämmelse om överföring av sekretess avses en bestämmelse som innebär att en primär sekretessbestämmelse som är tillämplig på en uppgift hos en myndighet ska tillämpas på uppgiften även av en myndighet som uppgiften lämnas till eller som har elektronisk tillgång till uppgiften hos den förstnämnda myndigheten. En sekundär sekretessbestämmelse är därmed en bestämmelse om sekretess som en myndighet ska tillämpa på grund av en bestämmelse om överföring av sekretess (3 kap. 1 § OSL).

Till följd av denna reglering kan en bestämmelse om sekretess vara primär hos beställande myndighet men sekundär hos tjänstelevererande myndighet. Frågan blir därmed om en tystnadsplikt som gäller för beställande myndighet, men där föremålet för sekretessen är begränsat till den beställande myndighetens verksamhetsområde eller liknande, kan överföras till den tjänstelevererande myndigheten.[40] För att en sådan regel om sekretess ska gälla hos en tjänstelevererande myndighet behövs en särskild regel om sekundär sekretess. I 11 kap. OSL ges visserligen generella regler om sekundär sekretess, men de gäller endast för verksamhet som avser tillsyn eller revision, disciplinansvar, forskningsverksamhet, fackliga förhandlingar, direktåtkomst och viss arkivering och förvaring av all-

[40] Denna fråga aktualiseras oavsett om vårt förslag till ändring av 40 kap. 5 OSL genomförs.

männa handlingar. Inte heller i 40 kap. OSL finns någon bestämmelse om överföring av sekretess som har anknytning till sekretess i verksamhet för enbart teknisk bearbetning eller teknisk lagring för annans räkning; jfr däremot hur överföring av sekretess föreskrivs i 40 kap. 7 § för verksamhet som avser skadereglering.

5.5.3 Myndighetssamverkan förutsätter överförd sekretess

Vid de redovisade bestämmelsernas tillkomst torde det inte ha funnits en tanke på att utvecklingen skulle kunna leda till den myndighetssamverkan på it-området som ses som närmast självklar idag. Utvecklingen har gått snabbt. En liknande gränsdragningsfråga vid myndighetssamverkan har redan föranlett en bestämmelse i 11 kap. 4 § OSL enligt vilken sekretess som gäller hos en myndighet överförs till en mottagande myndighet, om den mottagande myndigheten ges elektronisk tillgång till en upptagning för automatiserad behandling hos en utlämnande myndighet och denna upptagning är sekretessreglerad hos den utlämnande myndigheten. Genom denna sekundära sekretess hindras att uppgifter i en upptagning som är sekretessreglerad hos värdmyndigheten (den myndighet hos vilken uppgifterna blir tillgängliga) blir offentliga hos den mottagande myndigheten (den myndighet som ges direktåtkomst). Bestämmelsen syftar till att uppgifter som är tekniskt tillgängliga för en mottagande myndighet, men inte omfattas av någon sekretessreglering där, ska behålla sekretesskyddet genom den överförda sekretessen.

Både för de nu beskrivna fallen (direktåtkomst) och för sådan utkontraktering av it-drift till en myndighet som delegationen överväger uppkommer oväntade, icke avsedda effekter, som en följd av myndigheternas behov av att kunna använda i samhället allmänt spridda tekniska och administrativa lösningar för informationsbehandling. Medan frågan om överföring av sekretess vid direktåtkomst har sin grund i den överskottsinformation som oavsiktligt blir tillgänglig för en annan myndighet[41] rör frågan om överföring av sekretess vid outsourcing den information som lämnas av en myndighet till en annan endast av tekniska skäl.

Vid utkontraktering av it-drift förvarar en myndighet data bara för att sköta en teknisk uppgift. Personalen hos den beställande

[41] Se vidare Informationshanteringsutredningens delbetänkande Överskottsinformation vid direktåtkomst (SOU 2012:90).

myndigheten avses utföra sitt arbete på samma sätt som om den beställande myndigheten hade haft egna datorer och egen personal för att utföra uppgiften. Den tjänstelevererande myndighetens personal tar därmed normalt del endast av drift- och säkerhetsrelaterad information. Inslag kan emellertid förekomma i hanteringen som innebär att den tjänstelevererande myndighetens personal får se eller annars får tillgång till nyttoinformation som den beställande myndigheten använder för t.ex. sin ärendehandläggning. Kan en tystnadsplikt, som hade gällt om personalen i stället arbetat direkt för den beställande myndigheten, inte överföras, behöver verksamheten sannolikt organiseras på annat sätt. Vid utkontraktering är det en förutsättning att uppgifter som är sekretessreglerade hos den beställande myndigheten inte röjs. Alternativet blir därmed att utkontraktera it-driften till ett privaträttsligt subjekt. Något hinder för en myndighet att i avtal om leverans från en privat leverantör ta in en klausul om tystnadsplikt finns inte och ett utlämnande till den som tillhandahåller tjänsten kan vanligtvis ske med stöd av 10 kap. 2 § OSL.

5.5.4 Delegationens förslag

Regeringen har i olika sammanhang betonat vikten av myndighetssamverkan bl.a. genom att myndigheter ansluter sig till tjänster som en annan myndighet tillhandahåller.[42] När utkontraktering av it-drift sker till en myndighet behöver den tystnadsplikt som gäller för personal hos beställande myndighet gälla också för personal hos den tjänstelevererande myndigheten.

En sådan regel om överföring av sekretess bör kunna formuleras efter förebild av den överföring av sekretess vid direktåtkomst som följer av 11 kap. 4 § OSL och införas som en ny 4 a §, i förening med en ny rubrik, som anger att den nya paragrafen avser teknisk bearbetning och teknisk lagring för annan. Bestämmelsen föreslås gälla endast till skydd för allmänna intressen eftersom primär

[42] Se bl.a. 4 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte, uttalanden i regeringens proposition 2012/13:116 En mer samlad myndighetsstruktur inom folkhälsoområdet om att en föreslagen ny myndighet bör anslutas till Statens servicecenter och de administrativa tjänster som servicecentret erbjuder (s. 35) samt regeringens proposition 2012/13:128 Ny myndighet för hälso- och vårdinfrastruktur där regeringen också har uttalat att den nya myndigheten bör använda de administrativa tjänster som Statens servicecenter erbjuder (s. 32).

sekretess avses gälla enligt 40 kap. 5 § OSL för enskildas personliga eller ekonomiska förhållanden.

Den bestämmelse om överföring av sekretess som delegationen föreslår bör därmed kunna ges följande lydelse. Om en myndighet i sin verksamhet för enbart teknisk bearbetning eller teknisk lagring för en annan myndighets räkning får en uppgift som av hänsyn till ett allmänt intresse är sekretessreglerad där, blir sekretessbestämmelsen tillämplig på uppgiften även hos den mottagande myndigheten.

5.6 Alternativa bedömningar

5.6.1 Ett längre gående skydd

Delegationen har även övervägt andra mera långtgående förslag om sekretess för uppgifter vid utkontraktering av it-drift och tillhandahållande av elektroniskt förvar, *dels* för det fall att en annan tolkning än den vi redovisat i avsnitt 4.5.6 skulle göras av rekvisiten ”endast” (2 kap. 10 § TF) och ”enbart” (40 kap. 5 § OSL), *dels* för att kunna undgå de tolkningsfrågor som en överföring av sekretess kan föra med sig (förslaget till 11 kap. 4 a § OSL).

Gemensamt för dessa alternativ är i vilken mån det kan vara möjligt att vidga *föremålet* för sekretessen så att uppgifter av alla slag innefattas.

5.6.2 Närmare om elektroniskt förvar

En utmärkande egenskap hos ett elektroniskt förvar är att bara innehavaren får ha åtkomst till den nyttoinformation som finns där; jfr att var och en anser att information i den egna bostaden är privat. På samma sätt behöver ett företag ha ett elektroniskt förvar för sig själv. Handlingar blir inte att anse som allmänna för att de finns i en lokal som företaget hyr av en myndighet. Myndigheten saknar rätt att bereda sig tillträde dit utan att en sådan rätt följer av t.ex. ett straffprocessuellt tvångsmedel. Detta skydd för handlingar i bostäder och på kontor gäller oberoende av om handlingarna innehåller integritetskänsliga uppgifter. Det ska på samma sätt vara förbjudet för en myndighet att bereda sig tillgång till den information som finns i en enskilds elektroniska förvar.

När behovet av skydd för ett sådant förvar ska beskrivas närmare bör det noteras att det inte får förekomma någon teknisk bearbetning eller teknisk lagring där, för den tjänstelevererande myndighetens egen räkning, och att det i ett sådant förvar inte heller får förekomma bearbetning eller lagring av uppgifter som den myndighet som tillhandahåller förvaret tar del av. Det är alltså inte fråga om en utkontraktering där uppdraget innebär t.ex. att pappersdokument ska skannas eller att en annan myndighets it-drift ska skötas på ett sådant sätt att hanteringen inrymmer manuella moment där personalen behöver bereda sig tillgång till nyttoinformation för att utföra uppdraget.

Den teknisk lagring och bearbetning som en myndighet utför för att tillhandahålla ett elektroniskt förvar ska således vara begränsad, dels så att behandling får äga rum endast för innehavarens räkning, dels så att den tillhandahållande myndighetens personal inte får ta del av nyttoinformation – inte ens för att utföra tekniskt arbete med förvaret. Skulle en befattningshavare råka upptäcka att han eller hon tar del av nyttoinformation i ett elektroniskt förvar ska åtgärden omedelbart avbrytas.[43]

Innehavaren ser således innehållet i sitt elektroniska förvar som en del av sitt privatliv. Myndighetens personal ska endast hantera den drift- och säkerhetsrelaterade informationen, så att ingen obehörig tar sig in och att funktionerna fungerar för att lagra, skriva och på annat sätt bearbeta informationen; jfr skalskyddet för en fysisk lokal och den utrustning som finns där.

Regler som förbjuder personal hos den myndighet som tillhandahåller det elektroniska förvaret att bereda sig tillgång till en användares förvar eller att annars ta del av information som finns där är därmed en viktig del i skyddet för den enskilde.[44] Som undantag bör anges endast sådan åtkomst som är nödvändig för att rätta tekniska fel eller att tillgodose informationssäkerheten.

Det blir därmed vid straffansvar förbjudet för myndigheten och dess personal att bereda sig tillgång till en användares elektroniska förvar eller att annars ta del av information som finns där; jfr intrång i förvar enligt 4 kap. 9 § brottsbalken (BrB) och dataintrång

[43] Jfr hur straffprocessuella tvångsmedel ofta har utformats så att en åtgärd genast ska avbrytas när det upptäcks att informationen inte får granskas inom ramen för den enligt lag och beslut medgivna granskningen. Detta är särskilt relevant för it-området där det ofta inte går att se vad vissa data representerar förrän innehållet har gjorts läsbart.

[44] Detsamma gäller för personal hos en myndighet till vilken driften av ett elektroniskt förvar har utkontrakterats.

enligt 4 kap. 9 c § BrB. Straffansvar för dataintrång gäller oberoende av om samma uppgift eller handling finns tillgänglig för befattningshavaren någon annanstans, t.ex. i en myndighets system för ärendehandläggning. Här kan det exemplet nämnas att en uppgift i ett utkast till en deklaration som finns i ett elektroniskt förvar också kan finnas i en handling som nått myndighetens system för ärendehandläggning, där uppgiften får läsas av myndigheten.

Trots tekniska begränsningar och förbud för befattningshavare att bereda sig tillgång till nyttoinformation som en användare har i sitt elektroniska förvar kan en befattningshavare råka få se en uppgift där eller i en säkerhetskopia. Som ett resultat av digitaliseringen bryts allt ned till mönster av signaler, även t.ex. brandväggar och andra system för skydd mot intrång. Denna s.k. konvergens[45] – dvs. sammansmältning av infrastrukturer, tjänster och apparater – leder till att det inte går att separera elektroniska förvar för användare till egna fysiska enheter. Även data i elektroniska förvar behandlas i myndighetens it-miljö och i många fall blir det inte klarlagt vad vissa data representerar förrän de har behandlats med ett datorprogram. En uppgift i ett elektroniskt förvar kan då bli läsbar för en människa; jfr vad en fastighetsskötare kan få syn på när en lokal öppnas med huvudnyckel för att det har uppstått ett vattenläckage.

5.6.3 Ett fungerande skydd

Nyttoinformation i ett elektroniskt förvar hör till innehavarens egen kontrollsfär, dvs. vad denne med rimliga krav kan uppfatta som privat och där uppgifter inte får röjas; jfr avsnitt 4.5.1.

Ett exempel på en regel om sekretess som ger ett sådant skydd är sekretessen enligt 40 kap. 4 § OSL för växeltelefonister. Det har enligt lagmotiven inte ansetts lämpligt att överlämna till växeltelefonisten att avgöra om en sekretessregel är tillämplig i det enskilda fallet. Sekretessregleringen har inte heller avgränsats till vissa slag av uppgifter eller liknande. Växeltelefonistens tystnadsplikt kan därmed omfatta i och för sig offentliga uppgifter hos myndigheten i vars verksamhet växeltelefonisten deltar.

Förutsättningarna påminner om dem som gäller för personalen i en myndighets funktion för elektroniskt förvar. Eftersom perso-

[45] Se vidare Konvergensutredningens betänkande (SOU 1999:55) Konvergens och förändring – Samordning av lagstiftningen för medie- och telesektorerna.

nalen inte ska få ha åtkomst till en användares förvar och att förvaret avses vara skyddat oberoende av uppgifternas innehåll bör det övervägas om en tystnadsplikt kan införas som inte är avgränsad till vissa slag av uppgifter eller liknande. En befattningshavare skulle annars, när det är tveksamt om t.ex. ett skaderekvisit är uppfyllt, kunna ställas inför frågan om han eller hon, i syfte att kunna göra en skadedömning, ska sätta sig ytterligare in i uppgifter som egentligen inte ska läsas av denne. Även andra liknande situationer kan uppkomma där det inte är lämpligt att överlämna bedömningen av om en sekretessregel är tillämplig till någon som varken ska få ta del av uppgifterna eller, så länge undantaget enligt 2 kap. 10 § TF är tillämpligt, behöver göra det vid en begäran enligt 2 kap. TF.

Här kan en jämförelse också göras med den sekretess som enligt 45 kap. 2 § OSL gäller i notarius publicus verksamhet som följer av lag eller annan författning, för uppgift som det kan antas att den rättssökande har förutsatt ska bli behandlad förtroligt. En absolut sekretess har införts för uppgift som det kan antas att den rättssökande har förutsatt ska bli behandlad förtroligt. Sekretessen är i denna del inte heller begränsad till visst föremål såsom enskilds personliga eller ekonomiska förhållanden.

Det är ett sådant skydd som innehavare av elektroniskt förvar i praktiken förväntar sig. En sekretessreglering som inte är begränsad till uppgifter av viss art skulle också behövas om vår tolkning av 2 kap. 10 § första stycket TF och 40 kap. 5 § OSL skulle visa sig felaktig. I så fall skulle sekretess behövas inte bara för att en tystnadsplikt ska gälla i det allmännas verksamhet för att tillhandahålla elektroniskt förvar utan även för att utlämnande av en allmän handling som finns där ska vara förbjudet. En myndighet som tillhandahåller ett elektroniskt förvar, där det finns uppgifter som inte är sekretessreglerade hos myndigheten, skulle bli skyldig att lämna ut en handling som finns där till var och en som begär det.

En tystnadsplikt av det slag som gäller för växeltelefonisten och för notarius publicus, när uppgiften förutsätts bli förtroligt behandlad, skulle ge erforderligt skydd. Rätten till skydd för privatlivet kan sägas kräva detta (jfr avsnitt 4.5.1).

5.6.4 En alternativ sekretessreglering

En alternativ regel om sekretess har övervägts som en ny paragraf enligt vilken sekretess skulle gälla för en uppgift *i ett elektroniskt förvar* som en myndighet tillhandahåller åt en enskild som led i teknisk bearbetning eller teknisk lagring för dennes räkning.

Tystnadsplikt enligt offentlighets- och sekretesslagen gäller för uppgifter – inte för platser. Det finns emellertid exempel på en sekretessreglering som har avgränsats till elektroniskt registrerade uppgifter som har blivit lagrade på vissa datamedier; jfr en viss plats. Enligt 18 kap. 14 § OSL gäller sekretess för uppgift i kopior som i säkerhetssyfte har genererats i Regeringskansliets datasystem och som har bevarats med anledning av naturkatastrofen i Asien 2004, om det inte står klart att uppgiften kan röjas utan fara för att Regeringskansliets verksamhet skadas. Här avses de uppgifter som fanns på de s.k. tsunamibanden, dvs. vissa magnetband som år 2006 uppmärksammades i Regeringskansliet.

Till detta kommer, som framgått av avsnitt 4.5.6, att det sedan den 1 januari 2011 finns en föreskrift i 2 kap. 10 § andra stycket TF enligt vilken en handling som en myndighet förvarar endast i syfte att kunna återskapa information som har gått förlorad i en myndighets ordinarie system för automatiserad behandling av information (säkerhetskopia) inte utgör en allmän handling; jfr hur en myndighet tillhandahåller ett eget utrymme i myndighetens system så att innehavaren ska kunna förvara och behandla information där – skild från annan information. Sådana logiska gränser skapar myndigheter genom behörighetskontrollsystem (BKS), brandväggar, intrångsdetekteringssystem, kryptografiska skydd och liknande. Innehavaren av ett elektroniskt förvar behöver därför inte tveka om vilka handlingar som är registrerade i dennes förvar. Det han eller hon når där, efter att ha berett sig tillträde med e-legitimation, finns där. Dessa gränser, mellan elektroniska förvar och i förhållande till myndighetens it-miljö i övrigt, är tydliga också för myndighetens tekniska personal. Gränserna finns redan och de fungerar väl.

För en sekretessreglering av elektroniskt förvar räcker denna beskrivning, förutsatt att det är den nyttoinformation som användaren har i sitt logiskt avgränsade förvar som ska skyddas och inget

annat. En sådan reglering skulle kunna utformas så att sekretess ska gälla för en uppgift i ett elektroniskt förvar som en myndighet tillhandahåller åt en enskild. I begreppet elektroniskt förvar skulle ligga att det endast är den information innehavaren ser och förfogar över som omfattas av skyddet; dvs. den nyttoinformation som han eller hon har där i form av olika utkast, mottagna uppgifter eller handlingar, avsända handlingar eller egna registreringar.

För att tydliggöra att de behandlingar som myndigheten får utföra endast är tekniska skulle den avgränsningen också kunna göras att bestämmelsen gäller bara för elektroniskt förvar som myndigheten tillhandahåller åt en enskild *som led i teknisk bearbetning eller teknisk lagring* för dennes räkning. Genom denna formulering – hämtad från 2 kap. 10 § TF och 40 kap. 5 § OSL – skulle det bli tydligt att tystnadsplikten inte skulle gäller för uppgifter i myndighetens ordinarie system för verksamheten, t.ex. i en elektronisk akt för ett ärende som myndigheten handlägger. Genom en sådan begränsning, till bearbetning eller lagring för en *enskilds* räkning, skulle den föreslagna regeln inte heller kunna leda till kringgåenden av offentlighetsinsynen vid informationsutbyte mellan myndigheter. När teknisk bearbetning och teknisk lagring sker i elektroniskt förvar ska myndigheten, som framgått, inte få ta del av uppgifterna.

För uppgifter som inte finns i förvaret – den drift- och säkerhetsrelaterade informationen – skulle gällande regler om sekretess vara tillräckliga; se bl.a. 18 kap. 8 och 9 §§ OSL om säkerhets- eller bevakningsåtgärd rörande system för automatiserad behandling av information och om chiffer och kod m.m. Dessa drift- och säkerhetsrelaterade uppgifter kan förenklat beskrivas som ett slags ”skalskydd” kring användarens elektroniska förvar. ”Innanför” detta skal har innehavaren sin nyttoinformation.

För att tillgodose behovet av sekretess för den händelse vår tolkning av 2 kap. 10 § TF och 40 kap. 5 § OSL inte skulle anses riktig skulle rekvisitet ”endast” resp. ”enbart” kunna utelämnas. Sekretessens tillämpningsområde skulle därmed inte beröras av denna tolkningsfråga. En alternativ regel om sekretess skulle därmed kunna utformas så att sekretess ska gälla för en uppgift i ett elektroniskt förvar som en myndighet tillhandahåller åt en enskild som led i teknisk bearbetning eller teknisk lagring för dennes räkning.

5.6.5 Tolkningssvårigheter för befattningshavare

En alternativ regel om sekretess har övervägts genom en sådan ändring i 40 kap. 5 § OSL att sekretess skulle gälla för uppgift i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning.

Den i föregående avsnitt redovisade alternativa regeln skulle kunna ge ett fullgott skydd för elektroniskt förvar. De rättsliga bedömningar rörande överföring av sekretess, som kan komma att behöva göras med anledning av delegationens förslag till 11 kap. 4 a § OSL om överföring av sekretess, skulle emellertid kvarstå.

När en myndighet sköter sin egen it-drift gäller inte någon generell tystnadsplikt för den personal som utför arbetet. Befattningshavare får i stället i det enskilda fallet, innan en uppgift lämnas eller annars används, bedöma om sekretess och därmed en tystnadsplikt föreligger. Detsamma gäller för personalen hos en tjänstelevererande myndighet till vilken någon annans it-drift har utkontrakterats, om någon får del av en uppgift vid skötseln av en annan myndighets it-miljö. Förutsättningarna liknar dem som gäller för personalen i en myndighets telefonväxel; jfr avsnitt 5.4.1. För dem gäller emellertid absolut sekretess för uppgift som inhämtats vid tjänstgöringen och som avser telefonsamtal till eller från någon annan person hos myndigheten; jfr uppgifter som inhämtas av personal vid en tjänstelevererande myndighet.

Ett alternativt förslag till ändring av 40 kap. 5 § OSL har därför övervägts. Enligt detta skull inte bara begränsningen till personuppgifter utmönstras. Sekretessens föremål skulle vidgas ytterligare så att varje uppgift i sådan verksamhet omfattades av sekretessen.

En sådan regel om sekretess för uppgift i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning skulle bli enkel att tillämpa eftersom varje uppgift som behandlas inom ramen för den typen av verksamhet skulle omfattas. Samtidigt hade delegationens förslag att införa en regel om överföring av sekretess (förslaget till 11 kap. 4 a § OSL) inte längre behövts – alla uppgifter skulle bli skyddade såväl vid utkontraktering av it-drift som tillhandahållande av elektroniskt utrymme.

En befattningshavare som får del av en uppgift som myndigheten bearbetar eller lagrar tekniskt endast för annans räkning kan därvid behöva göra tolkningar av delvis svårtillgängliga regler om

huruvida andra regler om sekretess och möjligen en bestämmelse om överföring av sekretess blir tillämpliga eller om uppgiften är offentlig. Delegationen har visserligen föreslagit en bestämmelse enligt vilken sekretess som gäller hos den uppdragsgivande myndigheten överförs till den tjänstelevererande myndigheten när det är fråga om enbart teknisk bearbetning eller teknisk lagring för den andra myndighetens räkning (11 kap. 4 a § OSL). En sådan reglering medför emellertid som framgått att befattningshavaren måste göra en bedömning av om den endast tekniskt behandlade uppgiften är av sådan art att den är sekretessreglerad och om t.ex. ett skaderekvisit är uppfyllt i det enskilda fallet.

När sekretessen i verksamhet för teknisk bearbetning och lagring infördes var de uppdrag som lämnades vanligtvis begränsade jämfört med dagens utkontraktering av hela it-miljöer och materialet var oftast av enkel, överblickbar beskaffenhet. De bearbetningar som skulle och kunde utföras var också enkla att beskriva. Förutsättningarna har helt förändrats. I vissa delar kan de påminna om de risker för nya uppgiftskonstellationer som föranlett att säkerhetskopior undantagits från begreppet allmän handling och att en särskild bestämmelse om sekretess har införts för uppgifter som fanns på de s.k. tsunamibanden (jfr avsnitt 5.6.4). Undantaget enligt 2 kap. 10 § TF från handlingsoffentlighet gäller visserligen. Hur en befattningshavare ska kunna bedöma vilken tystnadsplikt som gäller när helt nya uppgiftskonstellation kan råka uppkomma inom ramen för en rent teknisk hantering har emellertid inte uppmärksammats. En sådan bedömning – i enlighet med våra förslag i 11 kap. 4 a § och 40 kap. 5 § OSL om tystnadsplikt vid outsourcing – kan visa sig bli betydligt mer komplex än de svårigheter att göra juridiska bedömningar som har föranlett en absolut sekretess för personal i en myndighets telefonväxel, som omfattar alla uppgift som de har inhämtat vid tjänstgöringen.

Frågan är om dessa nya förutsättningar kan beaktas fullt ut så att myndigheter från offentlighets- och sekretessynpunkt kan samverka på lika villkor som privaträttsliga subjekt.

5.6.6 Insynsintresset

Delegationens bedömning: Med dagens nätbaserade, sekundsnabba informationshantering kan ett särskilt insynsintresse knappast hävdas hos en myndighet som endast har en teknisk uppgift.

Frågan blir om en så långtgående sekretessreglering som i de alternativ delegationen presenterat i avsnitt 5.6.4 och 5.6.5 kan förenas med grundlag och den avvägning som måste göras mellan offentlighet och sekretess.

En grundläggande princip vid bedömningen av om en ny sekretessreglering ska införas är att behovet av och styrkan i en sekretess inte kan bestämmas enbart med hänsyn till sekretessintresset. Det behov som finns av sekretess måste i varje sammanhang vägas mot intresset av insyn i myndigheternas verksamhet. Denna avvägning kan mycket väl tänkas utfalla på annat sätt utanför det område där den primära sekretessen gäller än innanför detta område. Offentlighetsintresset kan alltså kräva att uppgifter som behandlas som hemliga hos den ena myndigheten är offentliga hos en annan som har inhämtat dem hos den förstnämnda (prop. 1979/80:2 Del A s. 76).

Här aktualiseras den omvända situationen – att uppgifter i vissa fall bör betraktas som offentliga eller vara skyddade endast genom svag sekretess hos en beställande myndighet, som lämnar ut uppgiften, medan samma uppgifter kan behöva omfattas av stark sekretess hos en den mottagande, tjänstelevererande myndigheten. Ett sådant behov kan finnas i tekniska sammanhang när en beställande myndighet har kommit överens med en tjänstelevererande myndighet om att den senare myndigheten ska sköta it-driften för den beställande myndighetens räkning eller biträda tekniskt på annat liknande sätt.

Utöver ren utkontraktering av en myndighets it-drift kan som exempel på mera avgränsade insatser nämnas att tillhandahålla tjänster för fakturahantering, redovisning, e-beställning, diarium, arkivering tekniska säkerhetsfunktioner av olika slag liksom analyser av uppgiftssamlingar i samband med intrång eller andra angrepp mot en myndighets informationssystem. Sådan samverkan mellan myndigheter är av en helt annan karaktär än de begränsade, delvis manuella insatser som var föremål för bedömning när bestämmelsen om sekretess vid teknisk lagring och bearbetning kom

till; numera 40 kap. 5 § OSL. I det lagstiftningsärendet nämndes som exempel att sända maskinskrivet manuskript till en datacentral för överföring av texten till magnetband, att överlämna manuskript för tryckning eller kopiering samt redigering av ljudupptagningar på magnetband, överföringar av sådana upptagningar till grammofonskiva, framkallning av fotografiskt material och liknande.

Sådan hantering är – i den mån den ens förekommer – helt väsensskild från den tekniska bearbetning och tekniska lagring som en tjänstelevererande myndighet numera utför vid utkontraktering av it-drift eller tillhandahållande av elektroniskt förvar. Höghastighetsnät kan användas så att en myndighets hela it-miljö, utöver tangentbord, skärmar och liknande, finns och sköts på en annan plats av en tjänsteleverantör. I verksamhet för sådan it-drift, hos en myndighet som utför behandlingar för en annan myndighets räkning förekommer inte någon handläggning av de ärenden som uppgifterna rör. Uppgifterna hanteras helt automatiserad i komplexa informationssystem så att materialet normalt är direkt tillgängligt via nät hos den beställande myndigheten.

Hos den beställande myndigheten finns kompetens och rutiner för att bedöma de frågor om offentlighet och sekretess som aktualiseras till följd behandlingen. Den tjänstelevererande myndigheten har i stället byggt upp teknisk kompetens för att hantera informationssystem. Kostnaderna blir betydande om motsvarande juridiska kompetens måste etableras även hos tjänsteleverantören; jfr att frågan enkelt kan lösas genom avtal när en privaträttslig aktör anlitas för tjänsten.

På samma sätt som en växeltelefonist svårligen kan bedöma olika sekretessfrågor i det flöde av uppgifter och samtal som växelfunktionen aktualiserar framstår det som främmande för servicetekniker och experter på tekniska frågor att göra komplexa bedömningar av om tystnadsplikt gäller för vissa uppgifter. Detta gäller särskilt som berörda tekniker inte avses ta del av det flöde av uppgifter som it-driften genererar. De skäl som åberopats för att en enskild ska kunna vända sig till vilken som helst av flera myndigheter där en uppgift förekommer är knappast heller lika relevanta när uppgifterna finns sekundsnabbt åtkomliga via nät hos den beställande myndighet som helt eller i vissa delar har utkontrakterat sin it-drift.

Med dagens nätbaserade, sekundsnabba informationshantering kan ett särskilt insynsintresse knappast hävdas hos en myndighet som endast har en teknisk uppgift. Vad som kan återstå att efter-

fråga hos en tjänstelevererande myndighet, som i dagens it-miljö utför teknisk bearbetning eller teknisk lagring för en annan myndighets räkning, kan vara vissa tekniska data, exempelvis säkerhetsloggar eller uppgifter i brandväggar och liknande. Sådana uppgifter omfattas emellertid vanligtvis av sekretess.

5.6.7 Kan en alternativ regel förenas med grundlag?

Delegationens bedömning: Det bör närmare genomlysas om den alternativa sekretessreglering som övervägts kan förenas med grundlag.

I 2 kap. 2 § TF ges en uttömmande uppräkning av de intressen som får skyddas genom att handlingar hålls hemliga. Om vår tolkning av 2 kap. 10 § TF och 40 kap. 5 § OSL är riktig blir 2 kap. 2 § TF dock inte tillämplig eftersom bestämmelsen endast gäller vilka begränsningar som får göras i rätten att ta del av *allmänna* handlingar. Vid utkontraktering blir det endast fråga om en tystnadsplikt för personal hos en tjänstelevererande myndighet. Till den del en bestämmelse i offentlighets- och sekretesslagen innebär en tystnadsplikt för befattningshavare vid en myndighet för regeln emellertid också med sig en begränsning av befattningshavarens yttrandefrihet enligt regeringsformen eller enligt den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen).

Även i regeringsformen föreskrivs att yttrandefriheten får begränsas endast om vissa förutsättningar är uppfyllda. Enligt 2 kap. 21 § RF får begränsningar göras endast 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 § RF 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. Uppräkning är emellertid

inte uttömmande. Berörda fri- och rättigheter får *i övrigt* begränsas om särskilt viktiga skäl föranleder det. Vid bedömandet av vilka begränsningar som får göras ska emellertid vikten av vidaste möjliga yttrandefrihet och informationsfrihet i politiska, religiösa, fackliga, vetenskapliga och kulturella angelägenheter beaktas.

Regleringen i regeringsformen syftar alltså till att nödvändiga begränsningar inte ska träffa yttrande- och informationsfriheternas ”kärna”. En regel som medför att teknisk personal, efter förebild av den som gäller för växeltelefonister, omfattas av en generell tystnadsplikt synes inte träffa kärnan i yttrande- eller informationsfriheten. Hanteringen är endast teknisk. Dessutom omfattas berörda uppgifter normalt av handlingsoffentlighet hos den beställande myndighet som utkontrakterat sin it-drift. Är det i stället fråga om elektroniskt förvar är det enskildas handlingar som berörs. För sådan privat information kan det inte rimligen hävdas att det finns ett intresse av offentlighetsinsyn.

Av lagmotiven (prop. 1979/80:2 Del A s. 66 f.) framgår att regeringsformens föreskrifter om begränsningar i yttrandefriheten i vart fall inte ger mindre utrymme för tystnadsplikt än tryckfrihetsförordningens regler om handlingssekretess. Det kan därmed – förutsatt att vår tolkning av 2 kap. 10 § TF och 40 kap. 5 § OSL är riktig – inte uteslutas att regleringen i grundlag skulle kunna ge utrymme för ett mera vidsträckt föremål för sekretessen än delegationen föreslagit. Härvid bör särskilt beaktas de utmaningar som en befattningshavare med tekniska arbetsuppgifter hos en tjänstelevererande myndighet kan ställas inför om han eller hon måste sätta sig in i den komplexa regleringen av tystnadsplikt. Detta gäller särskilt när regler om överföring av sekretess, så som föreslagits, behöver tillämpas vid en sekretessprövning hos en tjänstelevererande myndighet.

Behovet av tystnadsplikt för personal som endast sköter informationssystem – dvs. endast hanterar ren teknik – framstår inte som mera begränsat för att en myndighet i stället för ett privaträttsligt subjekt ges i uppdrag att sköta it-driften. Vid sådana förhållanden finns det skäl att närmare överväga om en alternativ sekretessreglering kan införas, i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning, där föremålet vidgas så att sekretess gäller oberoende av vilken typ av uppgift det är fråga om.

Enligt 40 kap. 8 § OSL gäller redan att den tystnadsplikt som följer av 5 § samma kapitel inskränker rätten enligt 1 kap. 1 § TF och 1 kap. 1 och 2 §§ YGL att meddela och offentliggöra uppgifter.

6 Hjälptjänster och presentationstjänster

6.1 Funktioner för att avhjälpa fel

6.1.1 De tjänster som erbjuds

Nya metoder har utvecklats för att hjälpa enskilda i deras kontakter med myndigheter. Ett exempel är de *svar på vanliga frågor* (s.k. FAQ) som ges på myndigheters webbplatser. Filmer förekommer också där det visas hur e-tjänster kan användas eller annars förklaras hur en användare bör gå tillväga. Att information görs allmänt tillgänglig på detta sätt för normalt inte med sig några nya frågor om offentlighet och sekretess.

Andra funktioner för att ge hjälp och stöd till enskilda bygger på *helt automatiserade* tjänster som utan legitimering av användaren interagerar med denne, t.ex. så att den enskilde fyller i vissa uppgifter och därigenom kan få automatiserat svar på vad som gäller i en viss fråga eller få veta vilket belopp som kan räknas fram enligt ett visst regelverk. Som exempel kan nämnas hur Transportstyrelsen via en webbsida, som var och en kan nå utan inloggning, låter användare fylla i registreringsnummer för viss bil och viss släpvagn, varefter tjänsten hämtar uppgifter ur myndighetens register, bearbetar uppgifterna och visar om angivet släp får dras av angiven bil samt vilken körkortsbehörighet ekipaget kräver. Ett annat exempel är en tjänst som Skatteverket tillhandahåller där användare utan inloggning kan beräkna reavinst vid försäljning av fastighet. Försök har dessutom gjorts med robotar som ”tolkar” vad en användare säger eller skriver och därefter ger svar helt automatiserat, försök som hittills inte torde ha utfallit särskilt väl.

Att information behandlas på beskrivet sätt, för vanligtvis inte med sig några komplikationer från offentlighets- eller sekretessynpunkt. Den enskilde fyller manuellt i vissa uppgifter eller säger

något. Svar genereras automatiserat och visas elektroniskt eller förs över som tal till användarens telefon eller dator.

Vissa frågor kan emellertid behöva klargöras när interaktionen drivs längre, t.ex. så att en tjänst kopplas upp mot användarens dator, inte bara för att användaren ska kunna skriva en fråga eller mata in ett värde, utan så att *tjänstens it-miljö kommunicerar helt automatiserat med användarens*. En fråga är om sådan tillgång för en myndighet till en användares dator medför att uppgifter i datorn blir att anse som allmän handling hos myndigheten. Skulle så vara fallet uppkommer frågan om uppgifterna är sekretessreglerade. Det är vidare av betydelse – oberoende av om allmänna handlingar föreligger – om en tystnadsplikt finns för befattningshavare som sköter det informationssystem som myndigheten brukar för sådana behandlingar.

Tänkbara exempel skulle kunna vara en tjänst för automatiserad felsökning om en myndighets e-tjänst inte fungerar för en användare och orsaken antas vara fel i användarens it-miljö (jfr hur virusprogram, efter att ett virus detekterats, i många fall har inbyggda funktioner för att återställa så att ingen skada sker). Tjänster av denna art torde dock för närvarande inte tillhandahållas av myndigheter utan endast av företag som kommersiella tjänster.

Däremot har det i anknytning till e-tjänster blivit allt vanligare med s.k. hjälptjänster (eng. helpdesk) där en användare *samtalar med en person* hos en myndighet, via telefon eller någon annan liknande kanal för att i realtid överföra tal. Liknande kommunikation förekommer också i form av text (s.k. ”chat”).

Så länge muntliga samtal inte spelas in och det inte är fråga om ”chat” uppkommer inga allmänna handlingar hos den myndighet som tillhandahåller tjänsten. Här återstår endast att bedöma om den person som ger hjälp har tystnadsplikt för det han eller hon får veta vid tjänstgöringen; jfr den tystnadsplikt som enligt 40 kap. 4 § OSL gäller för växeltelefonister.

Till detta kommer emellertid att hjälptjänster där användare kommunicerar, muntligen eller i form av ”chat”, med personal i en myndighets hjälptjänst allt oftare har kommit att förenas med funktioner för att den som söker hjälp ska kunna *lämna uppgifter elektroniskt* så att ett effektivare stöd kan ges. Användaren skulle visserligen kunna lämna ut uppgifterna via vanlig papperspost men denna kanal är i praktiken för långsam. I stället kan den hjälpsökande skicka *e-post* som genast når befattningshavaren. Då sänds meddelandet till myndighetens elektroniska mottagningsställe för

e-post och torde därigenom bli att anse som en inkommen handling enligt såväl förvaltningslagen som tryckfrihetsförordningen.[46] Här aktualiseras både frågor om tystnadsplikt och om förbud mot att lämna ut allmänna handlingar.

Vad som främst behöver övervägas är emellertid en ny form för kommunikation där den hjälpsökande *”delar skärm”* med personal vid en hjälpfunktion.[47] Frågan är om en sådan teknisk funktion ska anses innebära att myndigheten *går in* i användarens dator eller om den ska förstås så att den hjälpsökande *lämnar ut* vissa uppgifter till myndigheten. – Är funktionen utformad så att användarens it-miljö omedelbart blir tekniskt tillgänglig enligt tryckfrihetsförordningen, så att information som finns där ska ses som allmän handling, eller blir information som finns i användarens it-miljö allmän handling först när den hjälpsökande har vidtagit en åtgärd för att *lämna ut* en uppgift till myndigheten och uppgiften har överförts till myndighetens it-miljö?[48] – En långsiktigt hållbar rättslig bedömning av ”skärmdelning” i hjälptjänster förutsätter att det klarläggs hur berörda tjänster är utformade.

I anknytning till beskrivna tjänster uppkommer också komplicerade frågor om bl.a. informationssäkerhet och fördelning av ansvar enligt olika regelverk. Vår genomlysning har emellertid i denna fas av E-delegationens arbete begränsats till frågor om tillämpningsområdet för 2 kap. TF och huruvida gällande regler om sekretess är tillräckliga för berörda myndighetstjänster.

6.1.2 Närmare om ”skärmdelning”

Som ett exempel på ”skärmdelning” kan nämnas att en myndighet inför en programvara som är förenad med en tjänst som leverantören av programvaran tillhandahåller så att en krypterad tunnel kan skapas mellan hjälptjänsten och den hjälpsökandes dator. Den hjälpsökande uppmanas att besöka program- och tjänsteleverantörens webbplats, ladda ned en programvara samt installera den på sin dator. Med hjälp av programvaruleverantörens tjänst sker därefter

[46] Se vidare avsnitt 6.3.3 om gallringsbeslut och omedelbar gallring av vissa handlingsslag.
[47] Att ”dela skärm” får inte förväxlas med det som brukar kallas ”handläggaringång”. Det senare begreppet avser endast ingångar till handlingar som har kommit in *i ett ärende*.
[48] Jfr direktåtkomst med utlämnande på medium för automatiserad behandling (se E-delegationens rapport om direktåtkomst och utlämnande på medium för automatiserad behandling).

ett utbyte av kryptografiska nycklar för att den hjälpsökande ska kunna kommunicera skyddat med myndigheten. På den hjälpsökandes skärm visas vissa engångskoder som denne behöver uppge för myndigheten. En session upprättas endast om den hjälpsökande uppger koderna så att myndigheten skriver in dem på sin dator.

När detta förlopp är klart ser befattningshavaren i hjälptjänsten vad användaren har på sin bildskärm. Befattningshavaren kan däremot inte söka, skriva eller ge kommando till den hjälpsökandes dator. Den tekniska lösningen innebär alltså att den hjälpsökande lämnar ut de uppgifter som denne har på sin skärm; jfr om den hjälpsökande i stället hade besökt myndighetens lokaler, tagit fram en handling och visat den för en befattningshavare för att få hjälp. Personal i hjälptjänsten kan som framgått inte själv söka uppgifter eller handlingar i den hjälpsökandes dator eller annars skaffa sig åtkomst till något. Det är den hjälpsökande som gör en viss av den hjälpsökande bestämd skärmbild tillgänglig, genom att ta fram vissa uppgifter på sin skärm, ladda programvara och uppge koder, som skrivs in hos myndigheten så skärmbilden blir överförd. Något annat än vad användaren väljer att visa på sin skärm kan myndigheten inte ta fram; jfr att myndigheten, om den hjälpsökande i stället hade besökt myndighetens lokaler, inte haft rätt att öppna den hjälpsökandes portfölj och ta del av det som finns där.

Att den hjälpsökande på detta sätt t.ex. kan låta en befattningshavare i en hjälptjänst guida sig genom en e-tjänst, bör inte leda till någon annan bedömning eftersom det är den hjälpsökande som, så länge den kryptografiska tunneln är aktiv, väljer vilka skärmbilder som visas och därigenom lämnas ut. Myndigheten kan inte använda lämnade koder för att på nytt ta del av vad som visas på användarens skärm – koderna gäller bara en gång – och det sparas inte någon information hos myndigheten som kan knytas till den hjälpsökande. Allt försvinner när hjälpsessionen är över.

Programvaror som en myndighet använder kan visserligen konfigureras så att en dator kan fjärrstyras, men så får inte ske. Skulle det ändå äga rum är åtgärden sannolikt att anse som ett dataintrång. Ett annat exempel som bör nämnas är när en myndighet, efter att användaren har loggat in i en e-tjänst, erbjuder denne att ”chatta” med en befattningshavare vid myndighetens hjälptjänst. I hjälptjänsten kan en funktion ha byggts in så att den som användaren ”chattar” med kan se den hjälpsökandes blankett i dennes elektroniska förvar. Även här bör det finnas en tydlig punkt där an-

vändaren tar ställning till om befattningshavaren i hjälptjänsten ska få ut de uppgifter som användaren har på sin skärm.

Det får inte heller finnas någon möjlighet för befattningshavare vid en hjälptjänst att föra in eller ta bort uppgifter i en användares elektroniska förvar.

6.2 Handlingsoffentlighet i hjälptjänster

6.2.1 Regleringen

Reglerna om handlingsoffentlighet har redovisats i avsnitt 4.1–4.3.

Av avsnitt 4.4 har framgått att handlingsbegreppet fått en sådan utformning i 2 kap. TF att även sådana uppgifter som behandlas i anknytning till hjälptjänster blir att anse som handling i tryckfrihetsförordningens mening. Detta gäller även för samtal som spelas in elektroniskt. Dessutom anses en elektronisk handling, som framgått, bli inkommen till och förvarad hos myndighet redan genom att den har gjorts tillgänglig av annan för myndigheten, med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas (2 kap. 3 § andra stycket och 6 § första stycket TF).

Som redovisats i avsnitt 4.4.3 torde det undantag från allmän handling som föreskrivs i 2 kap. 10 § första stycket TF, för teknisk bearbetning och lagring, inte gälla handlingar i hjälptjänster eftersom sådana handlingar inte förvaras endast som led i teknisk bearbetning eller teknisk lagring för annans räkning. En myndighet tillhandahåller normalt en hjälptjänst för egen räkning och det centrala är den – ofta muntliga – information som myndigheten ger om hur ett visst problem kan avhjälpas. Även om en hjälptjänst gentemot slutanvändaren kan innefatta moment av teknisk bearbetning eller lagring synes det inte bli fråga om *endast* sådan verksamhet.

6.2.2 Vad som blir allmän handling vid hjälptjänster

De olika slag av hjälptjänster som berörts kan något förenklat redovisas genom följande figur.

Figur 6.1 Hjälptjänster

Med utgångspunkt från denna uppdelning i olika slags hjälptjänster kan noteras att handlingar med *svar på vanliga frågor* (FAQ), som tillhandahålls t.ex. via en myndighets webbtjänst, är att anse som förvarade och expedierade, och därmed allmänna handlingar.

På liknande sätt är uppgifter som görs tillgängliga för en myndighets hjälptjänst inom ramen för ett *helt automatiserat it-stöd*, och de svar användaren får genom tjänsten, att anse som förvarade och inkomna respektive expedierade allmänna handlingar.

Tillhandahålls en hjälptjänst *endast muntligen* av en myndighet – utan att samtalen spelas in eller annars dokumenteras och utan att den som begär hjälp gör handlingar tillgängliga – uppkommer inte allmänna handlingar. Motsatsen gäller vid s.k. chat. Det en hjälpsökande skriver blir en inkommen handling och svar från en hjälptjänst blir en expedierad och därmed allmän handling. Detsamma gäller när den hjälpsökande genom e-post och liknande ger in uppgifter till en myndighets hjälptjänst som i övrigt är baserad endast på muntliga samtal eller ”chat”. Meddelandena blir allmänna handlingar.

6.2.3 Särskilt om ”skärmdelning”

När en muntlig hjälptjänst eller en hjälptjänst baserad på ”chat” ska kombineras med ”skärmdelning” måste den funktionalitet som införs göras förenlig med reglerna om offentlighet och sekretess.

Den hjälpsökande upprättar vanligtvis ett utkast till en handling i ett sådant elektroniskt förvar som beskrivits och övervägts i avsnitt 4.5. Sådana handlingar är visserligen normalt tekniskt tillgängliga för någon hos den myndighet som tillhandahåller förvaret (t.ex. på teknikavdelningen) men enligt den bedömning delegationen redovisat i avsnitt 4.5.6 kan undantaget i 2 kap. 10 § första stycket TF från allmän handling tillämpas om lösningen utformas rätt.

Här uppkommer frågan om samma bedömning kan göras när en hjälptjänst kombineras med ”skärmdelning” eller om denna funktion för med sig att alla handlingar i en användares elektroniska förvar blir allmänna och ska lämnas ut på begäran om de inte omfattas av sekretess. Som framgått av avsnitt 4.5.6 är det knappast möjligt att bedöma en handlings egenskap av allmän eller inte utan att beakta det tekniska och administrativa sammanhang där handlingen figurerar och de virtuella gränser som finns mellan olika aktörers it-miljöer. Avgörande blir dels om myndigheten behandlar en viss handling endast tekniskt, dels om handlingen kan särskiljas från en annan handling, med samma eller annat innehåll, som myndigheten har tillgång till i en annan teknisk och administrativ kontext.

Vid bedömningen i avsnitt 4.5.6 av elektroniskt förvar utan ”skärmdelning” har som exempel nämnts dels en elektronisk handling som användaren har färdigställt och skrivit under i sitt förvar, dels ytterligare ett exemplar av den underskrivna handlingen som efter en aktiv handling av användaren har sänts från förvaret till myndighetens elektroniska mottagningsställe och förts vidare in i myndighetens verksamhetssystem. Vid bedömningen av en hjälptjänst där ”skärmdelning” förekommer blir det i stället fråga om ett utkast som användaren *har i sitt elektroniska förvar* och en elektronisk skärmbild som överförs via den upprättade tunneln till *myndighetens elektroniska hjälpfunktion* där data som representerar skärmbilder från elektroniskt förvar tas emot och visas. Medan det endast är innehavaren av det elektroniska förvaret som förfogar över de handlingar som finns där och innehavaren genom en aktiv handling bestämmer om någon handling ska lämnas till myndigheten, är det myndigheten som förfogar över de skärmbilder som

har mottagits. Det blir särskilt tydligt att olika exemplar föreligger om handlingen i användarens elektroniska förvar har xml-format och innehåller mer än skärmbilden visar för ögonblicket, medan det som överförs till myndighetens hjälpfunktion via tunneln endast är en rastrerad bild (jfr ett foto).

Avgörande för bedömningen av om 2 kap. 10 § första stycket TF blir tillämpligt är huruvida myndigheten behandlar en viss handling *endast tekniskt.* Eftersom den beskrivna lösningen innebär att skärmbilder, efter en aktiv handling av innehavaren av förvaret, *lämnas ut* till en särskild funktion hos den myndighet som ger hjälp och att myndigheten inte ges någon rätt att gå in i utrymmet eller att annars förfoga över de handlingar som finns där, får den nytto-information som finns i det elektroniska förvaret alltjämt anses omfattad av undantaget enligt 2 kap. 10 § första stycket TF. Den handling som når myndighetens tekniska funktion för att ta emot skärmbilder blir således allmän hos den myndighet som ger hjälp medan undantaget i 2 kap. 10 § första stycket TF alltjämt gäller för exemplar i användarens elektroniska förvar. Det är fråga om olika handlingar som från offentlighetssynpunkt får bedömas var för sig.

Skulle däremot den som ger hjälp se den blankett innehavaren av förvaret arbetar med, utan någon föregående åtgärd av innehavaren för att lämna ut handlingen, blir risken påtaglig att myndigheten anses vara inne i det elektroniska förvaret, för annat än endast teknisk bearbetning och lagring, och att de handlingar som finns i förvaret därmed inte längre omfattas av undantaget i 2 kap. 10 § första stycket TF.

Enkelt uttryckt bör det alltså upprätthållas en klar rågång mellan, på ena sidan sådana tekniska och administrativa lösningar för att ge hjälp som får anses innebära att en myndighet går in i det elektroniska förvaret, på den andra sidan sådana där den enskilde måste vidta en aktiv åtgärd för att uppgifter ska lämnas ut ur det elektroniska förvaret, så att det blir tydligt att dessa uppgifter överförs till en teknisk funktion där myndigheten mottar utlämnade handlingar.

Denna tolkning innebär att en myndighet som tillhandahåller elektroniskt förvar inte kan hjälpa innehavare att fylla i t.ex. en ansökan som finns i ett elektroniskt förvar utan att undantaget enligt 2 kap. 10 § första stycket TF upphör att bli tillämpligt. – Ska hjälp ges ”i utrymmet” och de handlingar eller uppgifter som finns där vara skyddade från insyn behöver särskilda regler om sekretess införas.

6.3 Sekretess och tystnadsplikt i hjälptjänster

6.3.1 Regleringen och allmän bedömning

Sekretess innebär som framgått (avsnitt 5.1) både handlingssekretess och tystnadsplikt. Till den del en sekretessbestämmelse innebär tystnadsplikt medför den en begränsning av yttrandefriheten enligt regeringsformen eller Europakonventionen.

Någon allmän regel om sekretess, så som gäller för växeltelefonister, finns inte för befattningshavare i en hjälptjänst. Det kan inte heller införas någon tystnadsplikt för dem genom avtal.[49]

Med utgångspunkt från de olika slag av hjälptjänster som beskrivits kan därmed följande bedömning göras.

De *svar på vanliga frågor* (s.k. FAQ) som ges på myndigheters webbplatser och filmer som visar t.ex. hur en e-tjänst kan användas innehåller endast publikt tillgänglig information för vilken det inte finns något behov av sekretess.

Beträffande sådant it-stöd där *hjälptjänstens it-miljö* kommunicerar *helt automatiserat med användarens* för felsökning eller för ”chat” och liknande har det inte vuxit fram några tydliga konturer ännu. I den mån sådana funktioner för felsökning överhuvudtaget finns hos myndigheter torde innehållet antingen vara harmlöst eller ta sikte på sådana säkerhets- eller bevakningsåtgärder för vilka sekretess gäller enligt 18 kap. 8 § OSL. En kategori som hör hit och som blivit allt vanligare är emellertid hjälptjänster där en användare anger vissa uppgifter för att få svar utifrån en datoriserad tillämpning av ett visst regelverk; t.ex. den tjänst som efter att registreringsnummer angetts visar om viss bil får dra visst släp och vilken körkortsbehörighet som krävs. Eftersom sådana tjänster används anonymt, utan inloggning, finns det knappast något behöv av handlingssekretess eller tystnadsplikt för myndighetens personal.

Därmed återstår *hjälptjänster som tillhandahålls muntligt* eller skriftligt genom ”chat”. Så länge sådana tjänster inte kombineras med ”skärmdelning” kan behovet av en särskild sekretessreglering framstå som begränsat, i vart fall vid en jämförelse med traditionell

[49] Med annan än myndighet kan avtal om tystnadsplikt träffas med rättslig verkan. Sådana avtal används regelmässigt när myndigheter sluter outsourcingavtal med privaträttsliga aktörer och det är en vedertagen uppfattning att avtalsgrundad tystnadsplikt bryter meddelarfriheten; se vidare prop. 1990/91:64 s. 34, prop. 1993/94:48 s. 85 och prop. 2005/06:162 s. 14. Hos de privaträttsliga organ som avses i 2 kap. 3 och 4 §§ OSL har anställda och uppdragstagare däremot samma meddelarfrihet m.m. som offentliganställda.

miljö. Enskilda synes inte hittills ha brukat hävda att en avsaknad av tystnadsplikt eller handlingssekretess skulle utgöra ett hinder mot att ringa och fråga en befattningshavare vid en myndighet. Möjligen kan det bero på att frågan inte har uppmärksammats eller att den sekretessreglering som finns har ansetts tillräcklig när servicen är begränsad till vanliga telefonsamtal.

Enligt delegationens bedömning har det inte framkommit skäl för att det skulle behövas nya bestämmelser om *tystnadsplikt* för hjälptjänster där endast samtal eller ”chat” sker med en befattningshavare hos en myndighet som ger hjälp, så länge de regler om sekretess som gäller för berörda ärendekategorier etc. blir tillämpliga även inom ramen för hjälptjänsten.

6.3.2 Delvis nya situationer

Situationen har emellertid delvis förändrats i takt med att *särskilda avdelningar* byggs upp inom myndigheter – kanske till och med som en egen verksamhetsgren – för att ge hjälp åt användare. I vissa fall kombineras sådan verksamhet med en för personal i hjälptjänsten särskilt anpassad tillgång till information hos den hjälpsökande. Utkontraktering har också börjat förekomma där en myndighet tillhandahåller ett annat organs hjälptjänst. För en myndighet som utför sådana uppgifter för annans räkning gäller vanliga regler om offentlighet och sekretess, till skillnad från när utkontrakteringen sker till ett företag, där tystnadsplikt som framgått (not 49) kan införas genom avtal.

Organisatoriska förändringar av denna art kan föra med sig luckor i sekretessen. Som exempel på situationer där det kan ifrågasättas om så blir fallet kan nämnas de bestämmelser som redovisats i avsnitt 5.4.2 rörande sekretess enligt 27 kap. 1 § OSL, *i verksamhet* som avser bestämmande av skatt eller fastställande av underlag för bestämmande av skatt, och enligt 28 kap. 1 § OSL, *i ärende* enligt viss närmare angiven lagstiftning. Föreligger sådan verksamhet eller sådant ärende när hjälpen sker på ett stadium där endast utkast övervägs, dvs. avser handlingar som inte har getts in i förvaltningsrättslig mening och gäller uppgifter som myndigheten inte ska få ta del av eftersom de behandlas i en användares elektroniska förvar? På detta stadium har något ärende oftast inte anhängiggjorts. I praktiken har myndighets verksamhet som avser bestämmande av skatt eller fastställande av underlag för att bestämma

skatt inte heller inletts. Myndigheten ger endast tekniskt och administrativt stöd som en service i *enskildas verksamhet* för att ge in underlag så att myndigheten kan inleda sin verksamhet i ett ärende, t.ex. för att bestämma skatt eller att fastställa beskattningsunderlag.

Beskrivna förändringar, i myndigheters verksamhet för att ge hjälp som en service, kan leda till att gällande regler om sekretess inte blir tillämpliga, när en hjälptjänst

- organiseras så att den utförs vid en myndighet utanför den verksamhet som omfattas av sekretess, eller
- utkontrakteras till en myndighet till vilken aktuell sekretess inte överförs.

Till detta kommer tekniska förändringar genom ”skärmdelning”, som utöver handlingsoffentlighet kan föra med sig att

- uppgifter samlas in hos den myndighet som ger hjälp, och
- befattningshavare får se ovidkommande, kanske känsliga uppgifter vid en hjälpsession.

”Skärmdelning” med en myndighets hjälptjänst innebär också att data som representerar vad en hjälpsökande ser på sin skärm kommer in till myndigheten. Valet mellan att bevara eller att kasta dessa data handlar tekniskt endast om att slå av eller på vissa inställningar i programvaror. För att ge en fullständig bild av dessa nya förutsättningar bör även frågor om gallring beröras.

6.3.3 Omedelbar gallring

Av arkivlagen (1990:782) följer att myndigheternas arkiv ska bevaras, hållas ordnade och vårdas så att de tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen, och forskningens behov. Enligt arkivförfattningarna ska myndigheterna vidare bevara allmänna handlingar i ursprungligt skick. Alla åtgärder som innebär förstöring av allmänna handlingar och uppgifter i allmänna handlingar eller annan informationsförlust utgör gallring. Även skärmbilder som ges in till en myndighets hjälptjänst omfattas av denna reglering.

Från det att en handling blivit allmän gäller att gallring får ske endast om åtgärden är tillåten enligt särskilda gallringsföreskrifter i

lag eller förordning eller i enlighet med föreskrifter eller beslut av Riksarkivet; se 10 § arkivlagen och 14 § arkivförordningen. Riksarkivet har utfärdat bl.a. generella gallringsföreskrifter för handlingar av tillfällig eller ringa betydelse för myndighetens verksamhet. Enligt 7 § Riksarkivets föreskrifter och allmänna råd om gallring av handlingar av tillfällig eller ringa betydelse (RA-FS 1991:6; ändrad genom RA-FS 1997:6) får sådan gallring dock ske endast under förutsättning att allmänhetens rätt till insyn inte åsidosätts och att handlingarna bedöms sakna värde för rättskipning, förvaltning och forskning.

Till föreskrifterna hör en bilaga med exempel på bl.a. handlingar som genom sitt informationsinnehåll eller sin funktion är av tillfällig eller ringa betydelse. Bland dessa exempel kan nämnas inkomna eller expedierade framställningar, förfrågningar och meddelanden av tillfällig betydelse eller rutinmässig karaktär samt loggar för e-post och fax under förutsättning att de inte längre behövs för kontroll av överföringen, och att de inte heller behövs för återsökning av de handlingar som har inkommit till eller utgått från myndigheten och som ska bevaras.

De handlingar som inkommer i en myndighets hjälptjänst blir av betydelse för myndighetens verksamhet endast under den aktuella hjälpsessionen och endast för den person som söker hjälp. Myndigheten avses inte – så som vid kommunikation i ett förvaltningsärende – ha insyn i dessa uppgifter. De mister sin betydelse för myndighetens verksamhet så snart hjälpsessionen har avslutats. Uppgifterna bör därmed kunna gallras utan att allmänhetens insyn i myndighetens verksamhet försvåras och utan att andra myndigheters eller forskningens behov sätts åt sidan.

I detta sammanhang bör också noteras att en allmän handling, enligt 5 kap. 1 § OSL, varken behöver registreras eller hållas ordnad om det är uppenbart att den är av ringa betydelse för myndighetens verksamhet.

E-delegationen har i en den 8 juli 2013 beslutad Juridisk vägledning för verksamhetsutveckling inom e-förvaltningen[50] beskrivit *omedelbar gallring* som ett juridiskt koncept. Vidare har E-delegationen, för att tillgodose enskildas befogade förväntningar på att andra inte ska ges tillgång till information som den enskilde ser som sin egen och att enskild inte ska kunna spåras eller övervakas

[50] Se bl.a. avsnitt 3.2 och avsnitt 3.3.

utifrån en tjänsts användning, i nämnda vägledning förordat att det beslutas om *omedelbar gallring.* De uppgifter som registrerats ska därmed enligt vägledningen tas bort genast efter att de brukats för att ge den enskilde hjälp. På motsvarande sätt ska enligt vägledningen uppgifter – om myndigheten getts åtkomst till dem – göras oåtkomliga för myndigheten så snart de inte längre behövs i hjälptjänsten (vägledningen avsnitt 2.3.5).

6.3.4 Ett praktiskt utformat skydd

Av Riksarkivets föreskrifter följer att en myndighet själv får fatta beslut om gallring av handlingar som är av tillfällig eller ringa betydelse för myndighetens verksamhet. E-delegationen har dessutom i sin vägledning fört in omedelbar gallring av sådana handlingar som ett juridiskt koncept. Enligt 5 kap. 1 § OSL behöver handlingar som uppenbarligen är av ringa betydelse för myndighetens verksamhet inte heller registreras eller hållas ordnade.[51]

Uppgifter som en befattningshavare i en hjälptjänst får del av eller som registreras eller blir tillgängliga i en sådan tjänst *saknar* normalt *betydelse från offentlighetssynpunkt*. Sådana uppgifter är vidare av *endast tillfällig betydelse* för myndighetens verksamhet eftersom de används endast för att som en ren service hjälpa den enskilde. Vid sådana förhållanden torde förutsättningar föreligga för en myndighet som tillhandahåller en hjälptjänst att besluta om omedelbar gallring av handlingar som blivit allmänna vid användning av hjälptjänsten.

Ett sådant beslut kan fattas på förhand och verkställas så snart den hjälpsession avslutats där berörd handling förekommer. För en sådan ordning talar även – utöver att handlingarna saknar betydelse från offentlighetssynpunkt och är av endast tillfällig betydelse för myndighetens verksamhet – att användare av hjälptjänster förväntar

[51] Av lagkommentaren framgår bl.a. följande: Från huvudregeln i första stycket görs ett generellt undantag i fråga om allmänna handlingar som uppenbarligen är av ringa betydelse för myndighetens verksamhet. Handlingar av detta slag behöver alltså inte registreras och därmed heller inte på annat sätt hållas lättillgängliga på sätt som annars medges för handlingar som inte är hemliga. Det är handlingens betydelse för myndighetens verksamhet som ska tas till utgångspunkt när det gäller att bedöma huruvida huvudregeln ska tillämpas eller inte. Att en handling som saknar betydelse för myndighetens verksamhet ändå har ett intresse från offentlighetssynpunkt medför alltså inte att handlingen måste registreras eller på annat sätt hållas lättillgänglig. Vilka handlingar som kan sägas vara av ringa betydelse måste givetvis avgöras från fall till fall (Lenberg, Geijer, Tansjö, Offentlighets- och sekretesslagen, kommentaren till 5 kap. 1 § tredje stycket OSL).

sig att de uppgifter som presenteras där inte röjs. Skulle personal i hjälptjänster lämna ut sådant material som allmän handling eller annars sprida det tas hjälptjänster knappast i bruk av enskilda.

Samtidigt synes utrymmet för att begära ut uppgifter i en hjälptjänst som allmän handling bli ytterst begränsat om ett gallringsbeslut finns och systematiskt verkställs när en session i hjälptjänsten har avslutats. En förutsättning är emellertid att den myndighet som ger hjälp inte får åtkomst till uppgifter på förhand utan först efter en aktiv handling vid hjälptillfället av den hjälpsökande så att det aktuella materialet blir tekniskt tillgängligt för myndigheten endast en kort tid.[52]

Upprätthålls sådana tekniska spärrar – utom under den korta tid som en hjälpsession är aktuell – blir utrymmet för att begära ut en handling med stöd av 2 kap. TF ytterst begränsat. En förutsättning torde i praktiken vara att den som ska använda tjänsten själv berättar om sin åtgärd och att begäran om att få ut handlingen framställs just vid tiden för brukandet av tjänsten. Som exempel kan nämnas en tjänst där samtycke för åtkomst ges för tre dagar respektive en tjänst där samtycket lämnas endast för en session som pågår några minuter. Endast i det första fallet torde en begäran om utlämnande enligt 2 kap. TF kunna förväntas resultera i att myndigheten finner att en handling alltjämt är förvarad där. Tidsfaktorn medför emellertid att även denna möjlighet till åtkomst framstår som delvis teoretisk. Antalet förvarade handlingar blir samtidigt begränsat så att sökningar eller sammanställningar som innefattar uppgifter från en mängd hjälpsökande knappast kan göras.

Här torde inte heller kunna hävdas att reglerna om god offentlighetsstruktur skulle innebära att effektiva sökningar måste kunna göras i sådant material. Berörda handlingar behöver som framgått inte ens hållas ordnade (5 kap. 1 § OSL). Däremot får en handling inte gallras när en begäran om att få ut den föreligger. JO har riktat skarp kritik mot ett sådant förfarande och förklarat att det är en självklarhet att en handling inte får förstöras (gallras) under sådana förhållanden.[53]

Sammantaget blir utrymmet ytterst begränsat för att under åberopande av reglerna om handlingsoffentlighet få ut uppgifter som har getts in eller gjorts tillgängliga vid en hjälpsession, om

[52] Jfr om överskottsinformation, bl.a. avsnitt 5.5.3 och not 41.
[53] Se JO beslut i Dnr 2265-2012.

omedelbar gallring beslutats och verkställs genast när en hjälpsession är över. Befattningshavare kan under sådana förhållanden inte heller, i syfte att utöva sin meddelarfrihet, söka i och sammanställa uppgifter ur omfattande material eftersom det inte finns något sådant material bevarat.

6.3.5 Tystnadsplikt i hjälptjänster

Delegationens förslag: Sekretess ska gälla i myndighets verksamhet för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar för uppgift om en enskilds personliga eller ekonomiska förhållanden.

Utgångspunkter

Behovet av sekretess blir under beskrivna förhållanden begränsat. Har det beslutats om omedelbar gallring och verkställs sådan genast kan en begäran om att få ut en handling – i myndighets verksamhet för att tillhandahålla service genom en hjälptjänst – endast i mycket speciella undantagsfall leda till ett utlämnande. I praktiken återstår därmed frågan om tystnadsplikt för personal i hjälptjänster.

Uppgifter och handlingar som lämnas till eller görs tillgängliga i en hjälptjänst rör vanligtvis en enskilds personliga eller ekonomiska förhållanden. Det behöver emellertid inte vara fråga om personuppgifter enligt personuppgiftslagen. Delegationens förslag till ändring i 40 kap. 5 § OSL och om överföring av sekretess enligt 11 kap. 4 a § OSL kan visserligen ge ett skydd även för sådana uppgifter. En förutsättning för att denna reglering ska bli tillämplig är emellertid att behandlingen sker *enbart* för teknisk bearbetning eller teknisk lagring för annan; jfr 2 kap. 10 § första stycket TF. I en hjälptjänst behandlas uppgifter normalt för myndighetens räkning, så att myndigheten kan ge service.

Någon allmän regel om tystnadsplikt för befattningshavare, så som gäller för växeltelefonister (jfr avsnitt 5.4.2), finns inte för personal i en hjälptjänst. Sekretessen för uppgift som avser uppdrag som en myndighet utför för en enskilds räkning, när det kan antas att uppdraget har lämnats under förutsättning att uppgiften inte röjs, omfattar inte heller här aktuell hjälpverksamhet (jfr avsnitt

5.4.3). Däremot kan andra bestämmelser om sekretess, för särskilda behov av skydd, gälla i en hjälptjänst, t.ex. sekretessen för uppgifter om säkerhets- eller bevakningsåtgärder (se 18 kap. 8 § OSL).

Vad som är speciellt, i verksamhet för att tillhandahålla en hjälptjänst, vid en avvägning mellan offentlighet och sekretess, är att såväl intresset av offentlighet som behovet av tystnadsplikt framstår som begränsat. Användare av hjälptjänster ser det visserligen ofta som naturligt att ingen utomstående ska få del av de personliga uppgifter eller företagsuppgifter som lämnats vid en hjälpsession. Uppgifterna uppfattas som privata. Vid en närmare granskning förefaller emellertid intresset av tystnadsplikt inte vara särskilt starkt uttalat. Undantaget är vissa uppgifter som är sekretessreglerade när de förekommer i ärende hos myndighet; t.ex. uppgifter om skatt, pension, hälsa o.dyl. Som berörts i avsnitt 6.3.2 kan det visa sig oklart om en sådan sekretessbestämmelse är tillämplig redan när uppgifter behandlas i en hjälptjänst, utan att något ärende har anhängiggjorts.

En ny sekretessbestämmelse

Som framgått av avsnitt 5.6.6 kan behovet av sekretess och styrkan i en sekretessreglering inte bestämmas enbart med hänsyn till sekretessintresset. Det måste i varje sammanhang vägas mot intresset av insyn i myndigheternas verksamhet. I en hjälptjänst är det emellertid inte myndighetens verksamhet och uppgifter om den som väcker frågor om sekretess – för sådana uppgifter finns redan en fungerande sekretessreglering. Frågan rör i stället användarens förväntning att uppgifter inte ska röjas om de blir tillgängliga i en hjälptjänst. Syftet med en hjälptjänst är inte att ge in uppgifter eller handlingar till myndighet utan att göra det möjligt att få *tekniska och administrativa funktioner* att fungera så att uppgifter kan hanteras elektroniskt och handlingar därefter kan upprättas och ges in. Med administrativa funktioner menas här t.ex. hjälp om innebörden av relevanta begrepp, i vilka fält olika uppgifter ska fyllas i och liknande stöd som en myndighet kan bidra med inom ramen för sin serviceverksamhet.

I detta hjälpskede är intresset av offentlighet svagt, för att inte säga obefintligt, vilket framgår redan av vad som gäller enligt bestämmelserna om registrering och gallring. När endast hjälp ges ska uppgifterna dessutom göras tillgängliga endast under det korta

moment när enskilda ges service, t.ex. för att få sin dator att fungera tillsammans med en myndighets e-tjänst eller att få beskrivet hur uppgifter fylls i och i övrigt hanteras för att e-tjänsten ska fungera. De uppgifter som i en hjälpsession utbyts mellan den som ger och den som tar emot hjälp saknar normalt betydelse för såväl myndighetens verksamhet som från offentlighetssynpunkt. Statistiska uppgifter och information för planering, utveckling och förbättring av sådan verksamhet hör inte hit utan endast vad användare av en hjälptjänst berättar och visar för att myndigheten ska kunna se och förstå användarens problem och hjälpa till rätta. Uppgifter som en myndighet som tillhandahåller en hjälptjänst använder för annat än att hjälpa en användare torde ges ett tillräckligt skydd genom befintliga regler om sekretess.

Behovet av skydd kan således begränsas till uppgift om enskilds ekonomiska eller personliga förhållanden i myndighets verksamhet för att tillhandahålla service. Samtidigt finns det emellertid knappast skäl att införa en tystnadsplikt för sådana uppgifter vid varje samtal eller skriftväxling – t.ex. ”chat” – mellan en hjälpsökande och en befattningshavare i en myndighets funktion för att ge hjälp. Muntlig hjälp har sedan länge getts av myndigheter via telefon, utan att något särskilt behov av sekretess motsvarande det för en växeltelefonist ansetts föreligga. Detsamma gäller för hjälp via e-post.

Vad som är nytt och kan anses ge den hjälpsökande en befogad förväntning att uppgifter inte röjs är de elektroniska förvar som myndigheter inför på bred front och som präglas av att ingen annan än innehavaren ska få ta del av den nyttoinformation[54] som finns där. När uppgifter som en användare har i sitt elektroniska förvar överförs till en hjälptjänst – t.ex. i form av skärmbilder – ger en avvägning mellan skälen för respektive mot en sekretessreglering vid handen att det inte finns hinder mot sekretess om det krävs för att användare av elektroniskt förvar ska känna sig trygga och ta emot den hjälp som myndigheter erbjuder via hjälptjänster.

En sådan sekretessreglering för uppgift om enskilds ekonomiska eller personliga förhållanden bör begränsas till myndighets verksamhet för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar. Bara sådan hjälp som avser uppgifter i ett elektroniskt förvar, som lämnas genom överföring från elektroniskt

[54] Se angående detta begrepp, avsnitt 3.2.

förvar till en hjälptjänst samt andra uppgifter som lämnas i samband med en sådan överföring, omfattas därmed av förslaget. Med hänsyn till att det normalt saknas insynsintresse beträffande sådana uppgifter, till skillnad från statistiska uppgifter och information om planering, utveckling och förbättring av sådana verksamheter, bör en absolut sekretess kunna föreskrivas. Redan risken för att en sådan uppgift skulle kunna komma att lämnas ut efter en sekretessprövning skulle kunna förmå enskilda att avstå från att använda tjänsten. Finns ingen tystnadsplikt föreskriven genom sekretess kan verksamhet av detta slag antas bli utkontrakterad till privaträttsliga subjekt för att kunna införa en tystnadsplikt genom avtal, vilket kan ske utan någon begränsning till vissa uppgifter.

Den reglering delegationen föreslår innebär således i allt väsentligt en tystnadsplikt för personal i hjälptjänster som är till för elektroniskt förvar. Förslaget medför emellertid också att en handling som alltjämt finns kvar, i en myndighets verksamhet för att tillhandahålla service genom en sådan hjälptjänst, inte behöver lämnas ut som allmän handling om den endast innehåller uppgifter om enskilds ekonomiska eller personliga förhållanden. En sådan bestämmelse om sekretess för uppgift om en enskilds personliga eller ekonomiska förhållanden, i myndighets verksamhet för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar, föreslås, som en ny 5 a § i 40 kap. OSL. Någon generell sekretess för uppgifter i hjälptjänster föreslås alltså inte utan endast ett kompletterande skydd för elektroniskt förvar i verksamhet för att tillhandahålla hjälptjänster som har till syfte att underlätta användningen av sådant förvar.

Uppgifter som den myndighet som tillhandahåller hjälptjänsten använder även för annat än att på den enskildes begäran tillhandahålla service, som avser en hjälptjänst för elektroniskt förvar, omfattas inte av sekretessen. För sådana uppgifter torde ett tillräckligt skydd ges genom befintliga regler om sekretess. Denna begränsning avses framgå genom att sekretessen föreslås gälla endast *i verksamhet* för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar.

6.3.6 Förvar utanför myndighet

Delegationens bedömning: Sekretess för uppgift om en enskilds personliga eller ekonomiska förhållanden i myndighets verksamhet för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar, bör kunna tillämpas även om förvaret finns hos den hjälpsökande eller tillhandahålls av ett privaträttsligt subjekt.

Som framgått av avsnitt 3.3 har delegationen valt att använda uttrycket *elektroniskt förvar*, i stället för ”eget utrymme”, i syfte att knyta an till bestämmelsen i 4 kap. 8 § brottsbalken, där ansvar för intrång i förvar föreskrivs för den som olovligen bryter brev eller telegram eller eljest bereder sig tillgång till *något som förvaras förseglat eller under lås eller eljest tillslutet*. I motiven till den numera upphävda datalagen förklarade departementschefen att den som gör sig skyldig till obehörigt förfarande med ADB-material ibland kan straffas enligt brottsbalken, bl. a. för intrång i förvar. Samtidigt påpekade departementschefen att obehöriga förfaranden var möjliga utan att förfarandet blev åtkomligt enligt då gällande bestämmelser.[55] Frågan om data kan ses som något ”tillslutet” i paragrafens mening har övervägts av Datastraffrättsutredningen, som förklarade att data får anses vara fysiskt inneslutna om en diskett förvaras i ett förslutet kuvert eller om *dator och terminaler är inlåsta*. Däremot fann utredningen att det fick anses mer tvivelaktigt om *elektroniska ”förslutningar”* såsom lösenord eller kryptering kan anses medföra att förvaringen sker tillslutet.[56]

Vår avsikt med denna genomgång av bestämmelsen om intrång i förvar har inte varit att söka klarlägga straffansvarets gränser utan att undersöka möjligheten att knyta an till vad som numera får anses vara en allmän uppfattning om gränser i it-miljö: Enskilda kan ha ett ”förvar” som andra inte obehörigen får tränga in i såväl

[55] Se vidare prop. 1973:33 s. 104. Straffansvar för dataintrång infördes därvid, först i den då gällande datalagen och sedermera i 4 kap. 9 c § brottsbalken. Visserligen skulle 9 c § tillämpas endast när 9 § inte var tillämplig. I praktiken synes det emellertid inte ha prövats i vilken mån ett intrång i förvar kan föreligga i it-miljö.

[56] SOU 1992:110. En annan uppfattning än den i prop. 1973:33 redovisade har också kommit till uttryck i SOU 2013:39 s. 339, nämligen att bestämmelsen om intrång i förvar skulle ta sikte på att bereda sig tillgång till något fysiskt eller materiellt som förvaras förseglat eller under lås eller på annat sätt tillslutet, exempelvis att bereda sig tillgång till ett brev, dokument eller en annan handling genom att bryta upp en låst skrivbordslåda.

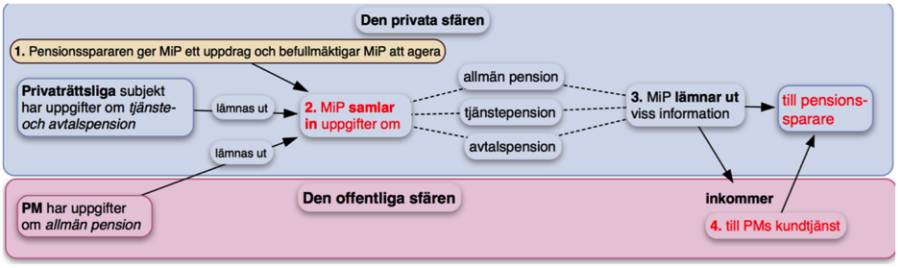
fysiskt, genom att användaren har sin dator inlåst i ett rum och förvarar sina uppgifter där, som *logiskt skyddat* genom att data i användarens via nät uppkopplade dator omgärdas av brandväggar och skydd genom lösenord, krav på e-legitimation eller annat liknande som ska hindra olovlig åtkomst till användarens dator och det som finns i detta förvar. Utvecklingen har dessutom, som beskrivits beträffande elektroniskt förvar som myndigheter tillhandahåller, gått dithän att virtuella utrymmen tillhandahålls åt enskilda så att de kan logga in där på ett säkert sätt, samtidigt som andra inte får och inte heller ska kunna bereda sig tillgång till det som finns där; jfr s.k. molntjänster.

Det redovisade synsättet bör kunna läggas till grund för delegationens förslag till sekretessreglering för uppgift om en enskilds personliga eller ekonomiska förhållanden, i myndighets verksamhet för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar. När uppgifter hanteras hos myndighet i dess verksamhet för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar bör ett skydd finnas även om förvaret finns hos den hjälpsökande, i dennes dator i form av t.ex. en elektronisk blankett.

Som exempel kan nämnas Pensionsmyndighetens samverkan med Min Pension i Sverige Aktiebolag. Uppgifter om vilken pension en individ (pensionssparare) kan förvänta sig finns hos olika aktörer. Uppgifterna omfattar såväl allmän pension som tjänstepension och privat pension. Pensionssparare utgår från att utomstående inte får del av dessa uppgifter. Samlad information om pension tillhandahålls därför av det privaträttsliga subjektet Min Pension i Sverige Aktiebolag, i det följande ”Bolaget”. De olika pensionsinstituten lämnar således information till en aktör som inte omfattas av reglerna om handlingsoffentlighet.

På en punkt bryts denna struktur emellertid igenom. Bolaget har gett Pensionsmyndigheten i uppdrag att tillhandahålla Bolagets funktion för kundservice (Bolagets Hjälpfunktion). Inom ramen för denna funktion ges Pensionsmyndigheten tillgång till uppgifter, som Bolaget har hämtat in enligt avtal med pensionssparare och förvarar åt dem, för att de via en webbtjänst ska kunna ta del av samlad information om sin pension. En pensionssparare som behöver tala med en befattningshavare för att få teknisk hjälp eller för att kunna förstå de uppgifter som finns där hamnar alltså i en hjälpfunktion som till följd av utkontraktering från Bolaget sköts av en myndighet; se följande figur som visar flödet av uppgifter.

Figur 6.2 E-tjänsten Min pension



Uppgifter som på detta sätt lämnas ut av Bolaget (punkterna 3 och 4 i figuren) kommer alltså in till Pensionsmyndigheten och blir allmän handling där. Det torde inte finnas tillräckliga regler om sekretess för att berörda handlingar ska kunna hållas hemliga om de begärs utlämnade med stöd av offentlighetsprincipen.

Som framgått kan en handling dessutom bli att anse som allmän redan till följd av att en myndighet ges tillgång till den. Detta gäller oberoende av om tillgången utnyttjats så att uppgifterna har hämtats till Pensionsmyndigheten. Bolaget har därför, för att information ska tillgängliggöras för Pensionsmyndigheten bara enligt avtal med pensionssparare, infört en särskild funktion på sin webbplats; ”Medgivande för supportåtkomst”. Befattningshavare vid Bolagets Hjälpfunktion, som finns hos Pensionsmyndigheten, får tillgång till uppgifter hos Bolaget endast via webbläsare och sökning kan bara ske genom att myndighetens befattningshavare manuellt anger en viss pensionssparares personnummer – ett nummer åt gången. Dessutom krävs att den aktuella pensionsspararen via www.minpension.se *tillfälligt* (för en tid av en eller tre dagar) har godkänt att kundtjänst får tillgång till pensionsspararens uppgifter.

Dessa särskilda begränsningar har införts för att säkerställa pensionsspararens berättigade förväntningar att uppgifter om hans eller hennes pension inte lämnas som allmän handling till utomstående.[57]

Den bestämmelse delegationen föreslår, om sekretess för uppgift om en enskilds personliga eller ekonomiska förhållanden i

[57] Det finns inte några uppgifter *hos Pensionsmyndigheten* om vilka pensionssparare som har lämnat ett tillfälligt samtycke vid en viss tidpunkt. I praktiken behöver pensionsspararen sannolikt ha upplyst någon om att han eller hon lämnat ett i tiden aktuellt samtycke för att en begäran om att få ut en viss pensionssparares uppgifter inte ska bygga på en ren gissning om att samtycke finns.

myndighets verksamhet för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar, bör kunna tillämpas även här. Avgörande för att ett elektroniskt förvar ska anses föreligga har beträffande myndighet ansetts vara att uppgifterna förvaras endast för teknisk bearbetning eller lagring, på sätt som anges i 2 kap. 10 § första stycket TF. Ett förvar av en enskilds uppgifter hos ett privaträttsligt subjekt kan emellertid utformas något friare eftersom allmänheten oberoende därav inte har någon rätt att begära ut uppgifter som finns där.

Avgörande vid tillämpning av den föreslagna sekretessbestämmelsen – för att ett elektroniskt förvar ska anses föreligga hos ett privaträttsligt subjekt – bör alltså vara att uppgifter som finns i ett elektroniskt förvar inte avses komma till någon utomståendes kännedom; jfr redovisningen av bestämmelsen om straffansvar för intrång i förvar.

Även uppgifter som lämnas till en myndighet, i verksamhet för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar, som lämnas från användarens förvar *i dennes egen dator* till den myndighet som tillhandahåller hjälpen bör omfattas av den föreslagna sekretessen. Det kan t.ex. vara fråga om en blankett med ett utkast till en handling som användaren håller på att färdigställa i sin dator för att ges in till en myndighet.

Eftersom sekretessen föreslås vara avgränsad till *myndighets verksamhet för* att tillhandahålla service genom en hjälptjänst för elektroniskt förvar, kommer även uppgifter som lämnas muntligen i sådan verksamhet att omfattas av skyddet, förutsatt att det är fråga om uppgift om enskilds personliga eller ekonomiska förhållanden.

6.3.7 Rätten att meddela och offentliggöra uppgifter

Delegationens förslag: Den tystnadsplikt som följer av den föreslagna sekretessbestämmelsen ska ha företräde framför rätten att meddela och offentliggöra uppgifter.

I offentlighets- och sekretesslagen finns också bestämmelser som begränsar den rätt att meddela och offentliggöra uppgifter som följer av 1 kap. 1 § TF och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen (YGL). Den rätt att meddela och offentliggöra uppgifter som följer av TF och YGL har som huvudregel företräde framför

tystnadsplikten. Nämnda rätt har dock aldrig företräde framför handlingssekretessen (7 kap. 3 § första stycket 2 och 5 § 1 TF samt 5 kap. 1 § första stycket och 3 § första stycket 2 YGL). Det kan således vara tillåtet att t.ex. muntligen lämna en sekretessbelagd uppgift till en journalist eller att själv publicera uppgiften, men det är aldrig tillåtet att med stöd av rätten att meddela och offentliggöra uppgifter lämna en handling som den sekretessbelagda uppgiften framgår av till en journalist eller att själv publicera handlingen.

I ett antal fall har emellertid även tystnadsplikten företräde framför rätten att meddela och offentliggöra uppgifter. Denna rätt är då helt inskränkt. Som exempel kan nämnas att rätten, enligt tryckfrihetsförordningen och yttrandefrihetslagen att meddela och offentliggöra uppgifter, har inskränkts i 40 kap. 8 § OSL såvitt avser bl.a. notarius publicus och växeltelefonister samt för teknisk bearbetning och lagring av personuppgifter.

I förarbetena till sekretesslagen (1980:100) angavs att det inte är möjligt att dra upp några fasta regler för när en begränsning av rätten att meddela och offentliggöra uppgifter bör göras. Varje gång en sådan fråga uppkommer måste flera faktorer beaktas. Det bör bl.a. beaktas om en uppgift har lämnats i en förtroendesituation eller om uppgiften hänför sig till ett ärende om myndighetsutövning. I det förra fallet bör rätten att meddela och offentliggöra uppgifter normalt vara utesluten. När det gäller uppgifter av det senare slaget bör däremot meddelarfrihet oftast föreligga. Vidare kan den enskilda sekretessbestämmelsens utformning ge viss ledning. I fråga om sekretessbestämmelser utan skaderekvisit kan det finnas större anledning att överväga undantag från rätten att meddela och offentliggöra uppgifter än i andra fall. Detsamma gäller i någon mån sekretessbestämmelser med ett omvänt skaderekvisit (prop. 1979/80:2 Del A s. 111).

Den föreslagna sekretessbestämmelsen avser uppgifter som lämnas i en slags förtroendesituation där en myndighet ger hjälp, utan att uppgifterna hänför sig till något ärende om myndighetsutövning. Sekretessen föreslås dessutom vara absolut. Den tystnadsplikt som följer av den föreslagna sekretessbestämmelsen bör därmed ha företräde framför rätten att meddela och offentliggöra uppgifter. Delegationen föreslår därför att 40 kap. 8 § OSL ändras så att 5 a § förs in i den uppräkning som ges av bestämmelser där tystnadsplikten inskränker rätten att meddela och offentliggöra uppgifter.

6.4 Funktioner för att sammanställa och presentera uppgifter

6.4.1 Utgångspunkter för hanteringen

Till de metoder som har utvecklats för att hjälpa enskilda – bland annat i deras kontakter med myndigheter – hör tjänster för att få uppgifter eller handlingar från olika organ presenterade efter att den aktuella informationen har samlats in till och blivit allmän handling hos en myndighet som tillhandahåller tjänsten. Dessa presentationstjänster, som översiktligt beskrivits i avsnitt 3.2, har definierats i E-delegationens Juridiska vägledning för verksamhetsutveckling inom e-förvaltningen, som en e-tjänst där en enskild kan få uppgifter eller handlingar från flera organ visade, efter att uppgifterna eller handlingarna har kommit in till den som tillhandahåller tjänsten, utan att det som visas blir tillgängligt för annan.

Syftet med dessa tjänster är att överbrygga de gränser mellan olika myndigheter som har tillkommit för traditionell miljö och som i vissa delar är svåra att förena med dagens nätverkssamhälle, där det är viktigt för enskilda att de inte upplever sig ”bollade” mellan olika organ och att de kan få överblick över sina engagemang. E-delegationen har därför verkat för att presentationstjänster ska utvecklas. Lösningar har exempelvis tagits fram för att en enskild ska kunna få en översikt över sina mottagna och lämnade fullmakter (Mina fullmakter) och över sina ärenden hos myndigheter (Min ärendeöversikt). En myndighet som tillhandahåller en sådan tjänst kan på olika sätt hämta in material, som finns hos ett eller flera andra organ, efter en visningsbegäran från en användare av en tjänst för att presentera uppgifterna. Sådan insamling kan ske momentant, direkt från organ som har det begärda underlaget, men insamlingen kan också ske på förhand, antingen till den myndighet som tillhandahåller presentationstjänsten eller till en annan myndighet som ges i uppdrag att förvara dessa handlingar.[58]

Den insamling som sker leder till att handlingar kommer in till myndigheten och därmed blir allmänna handlingar. Eftersom enskilda inte vill använda en presentationstjänst om den för med sig

[58] En insamling till en annan myndighet än den som tillhandahåller presentationstjänsten kan aktualiseras t.ex. för att det under den tid förvaringen sker ska kunna säkerställas att handlingarna förvaras endast som led i teknisk bearbetning eller teknisk lagring för annans räkning (2 kap. 10 § första stycket TF).

att var och en kan få ut uppgifterna under åberopande av reglerna om handlingsoffentlighet, gallrar myndigheten – när så får ske – de insamlade uppgifterna snarast efter att de har presenterats för användaren. Sker sådan gallringen genast är sannolikheten liten för att uppgifterna lämnas ut som allmän handling; jfr avsnitt 6.3.3. En myndighets verksamhet för att presentera en sammanställning för en enskild av uppgifter som helt eller delvis har hämtats in från annan kan emellertid i vissa fall också ha en funktion över tid så att vissa uppgifter behöver bevaras av den myndighet som tillhandahåller tjänsten.

Eftersom enskildas behov av samlad information rörande vissa förhållanden bryter igenom de myndighetsgränser utifrån vilka den offentliga förvaltningen är organiserad behöver det övervägas hur sådana tjänster ska kunna förenas med bl.a. reglerna om offentlighet och sekretess. I detta sammanhang aktualiseras också 2010 års ändringar i regeringsformen (RF), av vilka följer att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (2 kap. 6 § RF). Det är visserligen frivilligt för en enskild att använda en sådan tjänst och hanteringen av personuppgifter kan därmed utformas så att den äger rum endast om den enskilde har lämnat sitt samtycke. Tjänsterna syftar emellertid regelmässigt till någon form av *kartläggning* av den enskildes förhållanden, så att en sammanställning av dem skapas. Sannolikt skulle användare uppleva sig bli kartlagda på det område där en presentationstjänst används, om materialet hade blivit tillgängligt för var och en som allmän handling. Att den eller de fullmakter som finns för en person hos *en enda* myndighet kan begäras ut som allmän handling är knappast känsligt, i vart fall inte i traditionell miljö där handlingarna måste sökas fram manuellt. Skulle det däremot gå att begära ut alla fullmakter hos *olika* myndigheter som en person lämnat eller fått blir situationen en annan. På motsvarande sätt kan en enskilds kontakter med många myndigheter – kanske med t.ex. Polisen och Kronofogden – framstå som känsliga. En enskild, som i och för sig har behov av att enkelt få en överblick över sina ärenden, kan därmed antas avstå från att använda en tjänst för sådan presentation om det är nödvändigt för att undgå att var och en kan begära att få del av sammanställningen.

I andra fall kan det vara fråga om uppgifter som omfattas av sekretess men där det är oklart om sekretessen skulle gälla för upp-

gifterna även i en presentationstjänst; jfr avsnitt 5.4.2. Hit hör också att *särskilda avdelningar* byggs upp inom myndigheter – kanske till och med som en egen verksamhetsgren – för att presentera viss information för användare av e-tjänster eller att ge annan hjälp. I vissa fall kombineras sådan verksamhet med en särskilt anpassad tillgång till uppgifter för personal. Utkontraktering har också börjat förekomma så att en myndighet kan tillhandahålla ett annat organs presentationstjänst. För en myndighet som utför sådana uppgifter gäller vanliga regler om offentlighet och sekretess, till skillnad från när utkontraktering sker till ett företag, där tystnadsplikt som framgått kan införas genom avtal (se not 49).

Till detta kommer ett nytt kanalalternativ som Pensionsmyndigheten tillhandahåller för att fullgöra sitt uppdrag att ge så många pensionssparare som möjligt helhetsinformation om sin pension, oberoende av om pensionsspararen vill använda dator. Myndigheten erbjuder en presentationstjänst där Min Pension i Sverige Aktiebolag (Bolaget), på samma sätt som vid användning av den webbtjänst för pensionsprognos som finns på www.minpension.se, samlar in individens pensionsinformation. Informationen lämnas emellertid med stöd av fullmakt och särskilt samtycke ut till Pensionsmyndigheten, som presenterar den *muntligen* via telefon för de pensionssparare som väljer att använda tjänsten. Även här bryts den i avsnitt 6.3.6 beskrivna strukturen med utlämnande endast till ett privaträttsligt subjekt igenom, så att uppgifter som Min Pension samlat in till den privata sfären, görs tillgängliga för Pensionsmyndigheten; dvs. för ett organ där reglerna i 2 kap. TF gäller.

6.4.2 Handlingsoffentlighet

Som framgått av avsnitt 4.1–4.3 och avsnitt 6.2.1 har handlingsbegreppet fått en sådan utformning i 2 kap. TF att även uppgifter som behandlas i anknytning till presentationstjänster blir att anse som handling i tryckfrihetsförordningens mening. En handling anses dessutom bli inkommen till och förvarad hos myndigheten redan genom att den har gjorts tillgänglig med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas (2 kap. 3 § andra stycket och 6 § första stycket TF).

Som redovisats i avsnitt 4.4.3 torde det undantag från allmän handling som följer av 2 kap. 10 § första stycket TF, för teknisk bearbetning och lagring, inte gälla handlingar som förvaras i en presentationstjänst eftersom de inte förvaras där endast som led i teknisk bearbetning eller teknisk lagring för annans räkning. Myndigheter tillhandahåller vanligtvis presentationstjänster för egen räkning. Uppgifter som samlas in och sammanställs av myndigheter i presentationstjänster kan alltså bli allmän handling där.

Även de uppgifter som presenteras blir att anse som allmän handling, i vart fall när presentationen inte sker muntligt. Skulle handlingarna expedieras, t.ex. som e-post till Mina meddelanden – dvs. ett elektroniskt förvar som är användarens – är det som finns kvar hos den myndighet som gjort och expedierat sammanställningen alltjämt allmän handling hos myndigheten.

6.4.3 Omedelbar gallring

Som framgått av avsnitt 6.3.3 får en myndighet, i enlighet med generella gallringsföreskrifter, gallra handlingar som är av tillfällig eller ringa betydelse för myndighetens verksamhet, under förutsättning att allmänhetens rätt till insyn inte åsidosätts och att handlingarna bedöms sakna värde för rättskipning, förvaltning och forskning. De uppgifter som samlas in av en myndighet för en presentationstjänst blir normalt av betydelse för myndighetens verksamhet endast under den aktuella sessionen för visning. Myndigheten avses inte – så som vid kommunikation i ett förvaltningsärende – ha insyn i dessa uppgifter och behöver dem inte för annat än visning. Allmänna handlingar som härvid uppkommer mister således normalt sin betydelse för myndighetens verksamhet så snart sessionen för presentation har avslutats. Handlingarna bör därmed kunna gallras utan att allmänhetens insyn i myndighetens verksamhet försvåras och utan att andra myndigheters eller forskningens behov åsidosätts.

En myndighet som tillhandahåller en presentationstjänst bör därmed, så som för hjälptjänster, kunna besluta om omedelbar gallring och verkställa denna underhand, så snart respektive presentationssession har avslutats. Sådana uppgifter är av endast tillfällig betydelse för myndighetens verksamhet. De används endast för att som en ren service hjälpa den enskilde vid det aktuella tillfället. Om en ny begäran om sammanställning görs måste uppgifterna normalt

samlas in på nytt eftersom de kan bli inaktuella. Därmed saknas skäl att ha kvar insamlade uppgifter. För en sådan ordning talar också att användare av presentationstjänster förväntar sig att de uppgifter som samlas in och presenteras inte röjs. Skulle allmänheten kunna begära ut sådana sammanställningar kan det antas att tjänsterna inte tas i bruk av enskilda.

Samtidigt synes utrymmet för att som allmän handling begära ut uppgifter om sammanställningar i en sådan tjänst bli ytterst begränsat när ett gallringsbeslut finns och systematiskt verkställs så snart en presentationssession har avslutats. En förutsättning är emellertid att den myndighet som presenterar uppgifter inte får åtkomst till dem på förhand utan först efter en aktiv handling vid presentationstillfället av den registrerade så att det materialet blir tekniskt tillgängligt för myndigheten endast en kort tid; jfr dock vad som anförts i avsnitt 6.3.3 om att gallring inte får ske av en handling när en begäran om att få ut den föreligger. Befattningshavare i en presentationstjänst kommer inte heller att kunna söka och sammanställa omfattande material eftersom gallring sker.

Undantagsvis kan en presentationstjänst emellertid behöva vara utformad så att insamlade handlingar bevaras, för att kunna presenteras på nytt för samma användare av tjänsten. Omedelbar gallring kan härvid inte ske om tjänsten ska fungera.

6.4.4 Sekretess i presentationstjänster

Delegationens förslag: Sekretess ska gälla för uppgift om en enskilds personliga eller ekonomiska förhållanden i verksamhet för att presentera en sammanställning för en enskild av uppgifter som helt eller delvis har hämtats in från annan, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs.

Den information som behandlas inom ramen för en presentationstjänst kan normalt antas röra en enskilds personliga eller ekonomiska förhållanden. Det behöver emellertid inte vara fråga om en personuppgift enligt personuppgiftslagen.

En användare av en presentationstjänst ser det normalt som en självklarhet att ingen utomstående ska få del av uppgifterna. Detta tillgodoses i huvudsak redan genom beslut om omedelbar gallring.

Verkställs ett sådant beslut så snart presentationen har skett blir utrymmet för att begära ut en allmän handling ytterst begränsat. En sådan möjlighet kan emellertid inte helt uteslutas.

Användare av sådana tjänster förvänta sig att uppgifterna inte heller röjs på annat sätt, t.ex. muntligen av personalen.

Som framgått av avsnitt 5.6.6 kan behovet av sekretess och styrkan i en sekretessreglering inte bestämmas enbart med hänsyn till sekretessintresset. Detta intresse måste i varje sammanhang vägas mot intresset av insyn i myndigheternas verksamhet. Särskilda sammanställningar av uppgifter, som tas fram endast som en service för den registrerade, är som framgått av sådan ringa betydelse för myndighetens verksamhet att de enligt 5 kap. 1 § OSL varken behöver registreras eller hållas ordnade. Sammanställningarna behövs inte för rättskipningen eller förvaltningen och i den mån uppgifterna skulle bli av intresse för forskningen eller för offentlighetsinsynen finnas de sannolikt bevarade där de hämtades för att sammanställningen skulle kunna göras. Den kartläggning en sådan sammanställning kan innebära, genom att den tas fram för att underlätta för en enskild att få en överblick över egna förhållanden, medför att den enskilde har ett befogat intresse av sekretess, även om uppgifterna inte är sekretessreglerade var för sig.

Vid sådana förhållanden ger enligt delegationens bedömning en avvägning mellan skälen för respektive mot en sekretessreglering vid handen att det inte finns hinder mot sekretess. Delegationen föreslår därför en sådan bestämmelse, som en ny 5 b § i 40 kap. OSL, enligt vilken sekretess ska gälla för uppgift om en enskilds personliga eller ekonomiska förhållanden i verksamhet för att presentera en sammanställning för en enskild av uppgifter som helt eller delvis har hämtats in från annan. Som bestämmelsen formulerats ges skydd för såväl helt elektroniska tjänster som muntlig presentation av sammanställningar, så som i den beskrivna tjänsten för pensionsinformation, och för kombinationer härav. Delegations förslag, att sekretessen ska gälla för uppgifter som *helt eller delvis* hämtats in från annan, innebär att sekretess gäller även för en uppgift som hämtats in från den egna myndigheten, när uppgiften förekommer i myndighetens verksamhet för att presentera en sammanställning för en enskild.

Undantagsvis kan en presentationstjänst vara utformad så att en uppgift om en enskilds personliga eller ekonomiska förhållanden, som har hämtats in i myndighetens verksamhet för att presentera en sammanställning, behöver bevaras för att kunna visas på nytt

efter en förnyad visningsbegäran. Delegationen föreslår därför att sekretessregleringen utformas så att den omfattar även uppgifter som blir bevarade i verksamhet för att presentera sammanställningar.

6.4.5 Sekretessens styrka och rätten att meddela och offentliggöra uppgifter

Delegationens bedömning: Sekretessen ska gälla endast om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs. Rätten att meddela och offentliggöra uppgifter bör inte inskränkas.

Den information som behandlas inom ramen för en presentationstjänst kan, i den verksamhet där den hämtats, vara omfattad av alltifrån absolut sekretess till ingen sekretess alls. Vid en avvägning mellan behovet av sekretess och styrkan i en sekretessreglering har delegationen stannat vid att sekretessen bör gälla endast om det kan antas att den enskilde eller någon närstående till denne skulle lida skada eller men om en uppgift röjs.

För tjänster där uppgifter som inte är sekretessreglerade samlas in för att presenteras – t.ex. om en central tjänst införs för fullmakter – saknas ofta tillräckliga skäl för en starkare sekretess. Innefattar tjänsten i stället uppgifter om t.ex. skatt, för vilka absolut sekretess gäller, torde behovet av skydd för uppgifterna vara större. Under arbetets gång har därför övervägts att föreslå ett omvänt skaderekvisit. Det är emellertid för närvarande – med den snabba utveckling som äger rum på området – delvis oklart hur långt behovet av sekretess kommer att sträcka sig. Utgångspunkten vid utformningen av en ny sekretessbestämmelse är att det inte ska gälla mer sekretess än vad som är oundgängligen nödvändigt för att skydda det intresse som har föranlett bestämmelsen. Skulle det visa sig att presentationstjänster växer fram med så känsligt innehåll att ett rakt skaderekvisit inte kan anses tillräckligt bör den föreslagna sekretessens styrka övervägas på nytt.

Som exempel på situationer där det bör kunna antas att den enskilde eller någon närstående till denne skulle lida skada eller men om uppgifter röjs kan nämnas den kartläggning som blir följden om en persons ombudskrets eller anhängiggjorda mål eller ärenden

som berör en person kan begäras ut i sammanställd form så att en bild ges av personens rättsliga engagemang eller tvister.

Reglerna om rätt att meddela och offentliggöra uppgifter har berörts i avsnitt 6.3.7. Genom att den bestämmelse delegationen föreslår som en ny 5 b § i 40 kap. OSL är försedd med ett rakt skaderekvisit gäller en presumtion för att uppgifterna är offentliga. Denna omständighet talar för att den tystnadsplikt som följer av bestämmelsen inte bör ha företräde framför rätten att meddela och offentliggöra uppgifter (jfr prop. 1979/80:2 Del A s. 111 f.).

7 Konsekvenser av förslagen

I avsnittet behandlas konsekvenserna av delegationens förslag i den mån dessa konsekvenser inte tydligt framgår av betänkandet i övrigt. Redovisningen sker i enlighet med 14, 15 och 15 a §§ kommittéförordningen (1998:1474). Sålunda har också 6–7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning beaktats.

Delegationens förslag begränsar det allmännas kostnader. Dessutom ökar enskildas integritetsskydd liksom deras möjlighet att få service av myndigheterna. Det gäller inte minst småföretagen. Generellt sett medför delegationens förslag inte några kostnadsökningar för stat, kommuner eller landsting.

De förslag som möjliggör utkontraktering till en annan myndighet kan förväntas föra med sig betydande besparingar för det allmänna eftersom dagens avancerade it-miljöer förutsätter komplexa it-system och i vissa delar behöver skötas av tekniker som har spetskompetens. Det säger sig självt att varje myndighet inte kan ha egna sådana resurser, åtminstone inte om hanteringen ska bli ekonomiskt försvarbar. Detta kan jämföras med näringslivets inriktning att begränsa sina kostnader med hjälp av tjänster som tillhandahålls av specialiserade företag.

På motsvarande sätt kan möjligheten att skydda uppgifter i elektroniskt förvar och hjälptjänster som är knutna till sådana förvar, leda till en effektiviserad service åt enskilda, även vid tekniskt krångel. Enskilda kan samtidigt erbjudas en ökad trygghet och säkerhet. Därigenom åstadkoms betydande vinster för såväl enskilda och samhälle. Myndigheterna ges förutsättningar att få in ansökningar m.m. på ett strukturerat och effektivt sätt där uppgifterna i högre grad än annars blir korrekta till följd av det stöd som kan ges.

Arbetet med att ta fram presentationstjänster har utgått ifrån enskildas behov, nämligen att få en överblick i elektroniskt miljö

över sina mellanhavanden i olika avseenden. Presentationstjänster kan emellertid leda till att utomstående kartlägger de registrerade på ett integritetskänsligt eller kommersiellt sätt. Med de förslag som här lämnas kan enskilda erbjudas presentationstjänster som ger dem tillräckligt skydd för att tjänsterna ska komma till användning.

Storleken av vinsterna för enskilda och besparingarna för det allmänna kan knappast anges i siffror. Omfattningen av myndighetssamverkan för att kunna ta tillvara bl.a. expertkompetens på it-området är emellertid betydande. Skulle myndigheterna nödgas att begränsa sin samverkan i form av utkontraktering blir konsekvenserna omfattande, särskilt om privata leverantörer inte kan tillgodose dessa behov.

För integritetsskyddet medför föreslagna författningsändringar konsekvenser på så sätt att skyddet för den enskilde inte försvagas som en följd av den tekniska och administrativa utvecklingen på området. Den alternativa lösningen – att myndigheterna avstår från att samverka genom utkontraktering och att tillhandahålla elektroniska förvar, hjälptjänster och presentationstjänster – framstår inte som en reell möjlighet. Detta framgår bl.a. av att det allmänna har inrättat en rad organ för ändamålet såsom exempelvis Statens servicecenter.

Berörda frågor om bl.a. upphandling, konkurrens, informationssäkerhet och satsningar på infrastruktur hör inte hemma i ett lagstiftningsärende om sekretessreglering utan i de ärenden där det övervägs och beslutas om en tjänst ska införas.

I övrigt bedömer delegationen inte att förslagen får några sådana konsekvenser som sägs i 14, 15 och 15 a §§ kommittéförordningen.

8 Författningskommentar

8.1 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

11 kap.

Teknisk bearbetning och teknisk lagring för annan

4 a § *Får en myndighet i sin verksamhet för enbart teknisk bearbetning eller teknisk lagring för en annan myndighets räkning en uppgift som av hänsyn till ett allmänt intresse är sekretessreglerad där, blir sekretessbestämmelsen tillämplig på uppgiften även hos den mottagande myndigheten.*

Genom paragrafen, som är ny, införs en bestämmelse om överföring av sekretess i verksamhet för enbart teknisk bearbetning eller teknisk lagring som en myndighet utför för en annan myndighets räkning. Den överförda sekretessen gäller för uppgift som av hänsyn till ett allmänt intresse är sekretessreglerad hos den myndighet som lämnat ut uppgiften. Övervägandena finns i avsnitt 5.5.

För att en mottagande myndighet ska anses ”få” en uppgift i sin verksamhet för enbart teknisk bearbetning eller teknisk lagring, krävs inte alltid en överföring av data i teknisk mening. Åtgärder kan utföras för en beställande myndighets räkning så att uppgifter omfattas av överförd sekretess även om den mottagande myndigheten har behandlat dem så att nya uppgiftskonstellationer uppkommit.

Av 11 kap. 8 § följer att bestämmelsen inte gäller om en sekretessbestämmelse till skydd för samma intresse redan är tillämplig på uppgifterna hos den mottagande myndigheten. Finns det en sekretessbestämmelse som är primärt tillämplig hos den mottagande myndigheten är det således den bestämmelsen som ska tillämpas i stället för den överförda sekretessen oavsett om den primära sekretessen är starkare eller svagare än den sekundära sekretessen.

Genom att sekretessen kommer att gälla i verksamhet för *enbart* teknisk bearbetning eller teknisk lagring för någon annans räkning, ges bestämmelsen samma tillämpningsområde som det undantag från allmän handling som föreskrivs i 2 kap. 10 § första stycket TF, se vidare avsnitten 4.4.2 och 4.5.6. Det innebär att bestämmelsen blir tillämplig när myndighet utkontrakterar sin it-drift till en annan myndighet. Den kan emellertid också aktualiseras om en myndighet tillhandahåller ett elektroniskt förvar åt en annan myndighet.

40 kap.

5 § Sekretess gäller i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning för uppgift om en enskilds personliga eller ekonomiska förhållanden.

I paragrafen föreskrivs sekretess i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning. Övervägandena finns i avsnitt 5.2-5.4. Genom förslaget vidgas tystnadsplikten i verksamhet för att tillhandahålla it-drift och elektroniska förvar så att uppgift om en enskilds personliga eller ekonomiska förhållanden skyddas även om uppgiften inte är en personuppgift i personuppgiftslagens mening.

Genom att sekretessen kommer att gälla i verksamhet för *enbart* teknisk bearbetning eller teknisk lagring för någon annans räkning, ges bestämmelsen samma tillämpningsområde som det undantag från allmän handling som föreskrivs i 2 kap. 10 § första stycket TF, se vidare avsnitten 4.4.2 och 4.5.6. Det innebär att bestämmelsen blir tillämplig både vid utkontraktering av it-drift och vid tillhandahållande av sådant elektroniskt förvar som myndigheter erbjuder i anknytning till sina elektroniska tjänster.

Hjälptjänst

5 a § *Sekretess gäller i myndighets verksamhet för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar för uppgift om en enskilds personliga eller ekonomiska förhållanden*.

Genom paragrafen, som är ny, införs en bestämmelse om sekretess i myndighets verksamhet för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar för uppgift om en enskilds personliga eller ekonomiska förhållanden. Övervägandena finns i avsnitt 6.3.

Sekretessen begränsas till sådan hjälp som avser uppgifter i ett elektroniskt förvar, som lämnas genom överföring från elektroniskt förvar till en hjälptjänst samt andra uppgifter som lämnas t.ex. vid ett samtal med en befattningshavare i hjälptjänsten i samband med hjälp som avser elektroniskt förvar. I praktiken innebär denna reglering att det finns en tystnadsplikt för personal i en sådan hjälptjänst. Sekretessen gäller emellertid även för handling som inte har gallrats utan finns kvar i en myndighets verksamhet för att tillhandahålla service genom en sådan hjälptjänst.

Uppgifter som den myndighet som tillhandahåller hjälptjänsten använder även för annat än att på den enskildes begäran tillhandahålla service, som avser en hjälptjänst för elektroniskt förvar, omfattas inte av sekretessen. Denna begränsning framgår genom att sekretessen begränsas till *verksamhet* för att tillhandahålla service genom en hjälptjänst för elektroniskt förvar.

Presentationstjänst

5 b § *Sekretess gäller för uppgift om en enskilds personliga eller ekonomiska förhållanden i verksamhet för att presentera en sammanställning för en enskild av uppgifter som helt eller delvis har hämtats in från annan, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs.*

Genom paragrafen, som är ny, införs en bestämmelse om sekretess för uppgift om en enskilds personliga eller ekonomiska förhållanden i verksamhet för att presentera en sammanställning för en enskild av uppgifter som helt eller delvis har hämtats in från annan. Sekretess ska gälla om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs. Som exempel på situationer där det bör kunna antas att den enskilde eller någon närstående till denne skulle lida skada eller men om uppgifter röjs kan nämnas den kartläggning som blir följden om en persons ombudskrets eller anhängiggjorda mål eller ärenden som berör en person kan begäras ut i sammanställd form så att en bild ges av personens rättsliga engagemang eller tvister. Övervägandena finns i avsnitt 6.4.

Sekretessen skyddar inte bara uppgifter som förekommer i elektroniska tjänster utan även muntlig presentation av sammanställningar och kombinationer av sådana funktioner. Eftersom sekretessen gäller för uppgifter som *helt eller delvis* hämtats in från annan kan även en uppgift som hämtats in från den egna myndig-

heten omfattas av skyddet när uppgiften förekommer i myndighetens verksamhet för att presentera sammanställningar för enskilda; jfr 8 kap. 2 § OSL.

8 § Den tystnadsplikt som följer av 1, 2, 4, *5, och 5 a* §§ inskränker rätten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

I paragrafen föreskrivs inskränkningar i rätten att meddela och offentliggöra uppgifter. Den tystnadsplikt som följer av föreslaget om sekretessbestämmelse i 5 a § har företräde framför rätten att meddela och offentliggöra uppgifter. Övervägandena finns i avsnitt 6.3.7.

Kommittédirektiv 2009:19

Delegation för e-förvaltning

Beslut vid regeringssammanträde den 26 mars 2009.

Sammanfattning av uppdraget

Offentliga tjänster måste kontinuerligt utvecklas för att möta nya krav och förväntningar. E-förvaltningen utgör en viktig del i denna utveckling. För att stärka utvecklingen av e-förvaltningen och skapa goda möjligheter för myndighetsövergripande samordning inrättas en delegation för e-förvaltning.

Delegationens första uppgift är att utforma ett förslag till strategi för myndigheternas arbete med e-förvaltning. Förslaget ska redovisas till regeringen senast den 30 september 2009.

Därefter ska delegationen koordinera de statliga myndigheternas IT-baserade utvecklingsprojekt samt följa upp dess effekter för medborgare, företagare och medarbetare. Delegationen ska vidare koordinera vissa IT-standardiseringsfrågor samt bistå regeringen i det internationella arbetet på området.

Delegationen ska årligen lämna delrapporter med underlag och förslag till regeringen. En slutrapport ska lämnas senast den 31 december 2014.

Bakgrund

Regeringen framhöll i budgetpropositionen för 2007 (prop. 2006/07:1 utg.omr. 2, bilaga 1, avsnitt 2) sin avsikt att stärka styrningen av den förvaltningsgemensamma utvecklingen genom att

- säkerställa att förvaltningen utvecklar gemensamma principer för hur statlig registerinformation enklare ska kunna utbytas,
- se till att myndigheter använder enhetliga format för övrig informationsöverföring och kommunikation när det krävs,
- se till att statsförvaltningen i samverkan med kommuner och landsting utvecklar och tillämpar förvaltningsgemensamma metoder för säker elektronisk kommunikation och dokumenthantering,
- identifiera angelägna pilotprojekt som ska samfinansieras, samt utveckla former för en sådan finansiering och fördela samordningsansvaret för dessa projekt, samt
- stärka uppföljningen och granskningen av myndigheternas IT-baserade utvecklingsarbete.

Den 15 mars 2007 beslutade regeringen att tillsätta en statssekreterargrupp med uppgift att stärka samordningen i Regeringskansliet av frågor som är av strategisk betydelse för utvecklingen av elektronisk förvaltning, med målsättningen att förenkla företags och enskildas kommunikation med myndigheter, höja kvaliteten på myndigheternas beslut samt effektivisera användningen av varje satsad skattekrona.

Den 14 januari 2008 fastställde regeringen en handlingsplan för e-förvaltning (dnr Fi2008/491). Regeringen beslutade att handlingsplanen skulle ligga till grund för den fortsatta hanteringen och samordningen på området.

E-förvaltning definieras i handlingsplanen som en del av verksamhetsutvecklingen i offentlig förvaltning där man inte bara drar nytta av informations- och kommunikationsteknik, utan även ser till att utvecklingen på området leder till nödvändiga organisatoriska förändringar och vidareutbildning av medarbetare.

Målet för e-förvaltningsarbetet är att det ska vara så enkelt som möjligt för så många som möjligt att utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av förvaltningens service. Där det är till fördel för medborgare och företagare samt där kvaliteten, säkerheten och produktiviteten kan höjas ska myndigheterna samverka sektorsvis. Därigenom ska Sverige återta en ledande position inom området elektronisk förvaltning.

För att nå detta mål måste de goda erfarenheter som gjorts inom förvaltningen tas till vara samtidigt som möjligheterna till myndighetsövergripande samverkan och integration förbättras. Den ökade

samordningen av e-förvaltningsarbetet som behövs för att uppnå detta bör enligt handlingsplanen företrädesvis ske inom vissa angivna sektorer där regeringen utser samverkansansvariga myndigheter. För närvarande finns sektorsvisa arbeten med att förbättra informationshanteringen och utöka det elektroniska informationsutbytet, t.ex. inom området geografisk information och fastighetsinformation (Geodatarådet), Rättsväsendets Informationsförsörjning (RIF-rådet), IT i vård- och omsorgssektorn.

I handlingsplanen anges också att kommunernas e-förvaltningsarbete är av stor betydelse för utvecklingen av e-förvaltningen i stort. Det är därför viktigt att det statliga utvecklingsarbetet löpande samordnas med Sveriges kommuner och landsting (SKL).

I mars 2008 överlämnade den s.k. stabsutredningen sitt slutbetänkande Ett stabsstöd i tiden (SOU 2008:22). Utredningen föreslog bl.a. att en delegation skulle inrättas med uppgift att säkra att förvaltningens samlade resurser kommer till användning i den fortsatta utvecklingen av e-förvaltningen.

IT-standardiseringsutredningen överlämnade i juni 2007 sitt betänkande Den osynliga infrastrukturen – om förbättrad samordning av offentlig IT-standardisering (SOU 2007:47). I betänkandet, som har remissbehandlats, föreslogs bl.a. att en kanslifunktion skulle inrättas för att utveckla, samordna, förankra, publicera och underhålla förvaltningsgemensamma kravspecifikationer samt ge metod- och expertstöd i IT-standardiseringsfrågor inom den offentliga förvaltningen. Vidare föreslogs att ett IT-standardiseringsråd skulle inrättas i syfte att bistå regeringen när svenska ståndpunkter i internationella IT-standardiseringsfrågor tas fram. Förslagen har fått ett brett stöd av remissinstanserna.

Utredningen pekar på behovet av att använda format och tillämpningar i gemensamma strukturer samt av att tydliggöra ansvaret inom myndigheterna när det gäller informationsutbyte med andra myndigheter. Utredningen lyfter vidare fram behovet av ökad teknisk samverkansförmåga. Andra områden som behandlats av utredningen är användningen av öppna standarder i upphandling, öppna programvaror och samordning av IT-upphandling.

Enligt förordningen (2006:942) om krisberedskap och höjd beredskap har Myndigheten för samhällsskydd och beredskap (MSB) rätten att utfärda föreskrifter om ledningssystem för informationssäkerhet (LIS) enligt bl.a. standard för ledningssystem för informationssäkerhet.

I budgetpropositionen för 2009 (utg.omr. 2, avsnitt 3 och 5) anges att Verket för förvaltningsutveckling (Verva) ska avvecklas den 31 december 2008 och att regeringen avser att inrätta en e-delegation som ska genomföra regeringens handlingsplan för e-förvaltning. Som ett led i regeringens tillväxtsatsning (prop. 2008/09:01, utg.omr. 2, avsnitt 4) ska arbetet med att öka användningen av elektronisk upphandling intensifieras. Kammarkollegiet har fått i uppdrag att utveckla arbetet inom området.

Behovet av en delegation

Myndigheterna ansvarar för att fortlöpande utveckla sin verksamhet samt för att ta till vara de fördelar som kan vinnas för enskilda och för staten som helhet genom samarbete med andra myndigheter och organisationer. Myndigheterna har en generell serviceskyldighet och dessutom ett ansvar för att främja utvecklingen av ett säkert och effektivt elektroniskt informationsutbyte.

Det finns dock vissa styrnings- och samordningsproblem inom statsförvaltningen. Det förekommer t.ex. visst dubbelarbete när skilda myndigheter utvecklar och upphandlar olika lösningar inom likartade områden. Ibland sker utveckling utan att nyttan för användarna tydliggörs. Samverkansprojekt kan försvåras av oklara finansiella, organisatoriska och rättsliga förutsättningar. De tekniska systemens samverkansförmåga varierar.

För att förverkliga den förbättrings- och effektivitetspotential som en utvecklad e-förvaltning rymmer, krävs ett strategiskt synsätt på e-förvaltning som omfattar staten som helhet. Därför behövs ett myndighetsövergripande arbete i delegationsform som koordinerar enskilda myndigheters insatser.

Syftet med delegationen för e-förvaltning är mot denna bakgrund att effektivisera och utveckla arbetet med e-förvaltning inom den offentliga sektorn.

Utgångspunkter för delegationens arbete

Inledning

Samhället förändras på olika områden såväl ekonomiskt och tekniskt som demografiskt och kulturellt. Steg för steg sker en

anpassning till ett integrerat Europa och ett globalt samhälle. Rörligheten av arbetskraft och kapital ökar.

Statsförvaltningen behöver kunna leva upp till de nya krav och villkor som denna utveckling för med sig och ha en god förändringsförmåga. En viktig aspekt i detta sammanhang är medlemskapet i EU som gör att statsförvaltningen behöver arbeta mer sammanhållet och ta hänsyn till förändringar och krav på administrativt samarbete. Även kommuner och landsting berörs av denna tekniska och administrativa utveckling. Samarbetet i EU styr allt mer de krav som ställs på myndigheter, kommuner och landsting avseende elektroniskt informationsutbyte med EU-kommissionen och andra EU-länder.

Den statliga förvaltningspolitiken syftar till att skapa bästa möjliga förutsättningar för att genomföra regeringens politik till nytta för medborgare och företag (prop. 2008/09:1, utg.omr. 2, avsnitt 3.1). E-förvaltning är ett viktigt verktyg för att uppnå detta.

Utgångspunkter

När delegationen utför sina uppgifter ska den basera sitt arbete på följande utgångspunkter.

Medborgare ska kunna utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av förvaltningens service på ett enkelt sätt. E-förvaltningen ska bidra till att förenkla kontakten mellan förvaltning och medborgare och ska präglas av tillgänglighet och användbarhet. Det är mycket viktigt att denna utveckling sker med ett bibehållet starkt skydd för den personliga integriteten. Delegationen ska även beakta den utveckling som sker inom området e-demokrati, dvs. användning av IT i demokratiska processer.

E-förvaltningen ska bidra till att minska företagens administrativa kostnader och även i övrigt åstadkomma en märkbar förbättring i företagens vardag. Näringslivet ska stödjas genom förenklingar för företagen, när det gäller formerna för uppgiftslämnande och möjligheterna att kunna ta del av data från offentliga register och andra uppgifter. Delegationen ska i sin verksamhet främja konkurrens i enlighet med nationella och gemenskapsrättsliga regler om konkurrens. Den offentliga förvaltningens e-tjänster bör i så stor utsträckning som möjligt bygga på öppna standarder samt använda sig av programvara som bygger på öppen källkod och

lösningar som stegvis frigör förvaltningen från beroendet av enskilda plattformar och lösningar.

Elektronisk förvaltning, som syftar till att förenkla kontakten med medborgare och företagare, bör alltid ske utifrån användarnas behov och nytta i kombination med beräkningar av den interna produktiviteten.

Delegationen bör beakta behovet av att tillgängliggöra offentlig information bl.a. för vidareutnyttjande. Sverige har i dag en i stora delar digitalt baserad förvaltning. En mer tillgänglig offentlig information kan bidra till utvecklingen av ekonomin, men också underlätta vardagen för medborgare och företag.

Det är av stor vikt att det långsiktiga digitala bevarandet stärks inom e-förvaltningen, både för system och enskilda handlingar. För att detta ska vara möjligt är det nödvändigt att bevarandeperspektivet beaktas när nya system byggs upp.

Delegationens uppdrag

Allmänt

Regeringen prioriterar e-förvaltningsfrågorna genom att skapa en delegation inriktad på att bl.a. bidra till genomförandet av regeringens handlingsplan för e-förvaltning. Delegationen ska, så som föreslogs i betänkandet Ett stabsstöd i tiden (SOU 2008:22), i nära samspel med statssekreterargruppen för e-förvaltning, samordna och utveckla det fortsatta arbetet med e-förvaltningen. Delegationen ska också, så som föreslogs i betänkandet Den osynliga infrastrukturen (SOU 2007:47), samordna den offentliga sektorns deltagande i det internationella IT-standardiseringsarbetet avseende e-förvaltning.

Delegationen ska ansvara för samordningen på den myndighetsövergripande nivån. Detta innebär dels samordning av e-förvaltningsprojekt som är av strategisk natur, dvs. individuella projekt som påverkar förvaltningens samlade utvecklingsinriktning, dels samordning av de myndigheter som har ett eget ansvar att utveckla ett arbete eller en sektor så att respektive sektor väger in intresset för staten som helhet i sitt utvecklingsarbete.

Delegationen ska ha följande huvuduppdrag.

Utformning av en strategi för myndigheternas arbete med e-förvaltning

Utifrån de utgångspunkter som angivits ovan samt de mål som lades fast i handlingsplanen för e-förvaltning, ska delegationen inledningsvis lämna förslag till en strategi för myndigheternas arbete med e-förvaltning till regeringen. Strategin ska innehålla uppföljningsbara mål och delmål som ska uppnås på fem års sikt. Delegationen ska i förslaget ange de viktigaste utvecklingsprojekten i statsförvaltningen som behöver prioriteras. Strategin ska innefatta följande områden:

- hur samverkan mellan myndigheter, kommuner och landsting samt näringsliv och organisationer kan förbättras och hur ansvaret mellan dessa ska fördelas, bl.a. ska sektorsvisa samverkansansvariga myndigheter föreslås,
- hur den offentliga sektorns försörjning av elektroniska legitimationer, dvs. hanteringen av identifiering och underskrifter, bör genomföras i framtiden med utgångspunkt i rapporten Säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar (Verva 2008:12),
- hur teknisk samverkansförmåga mellan olika system, s.k. interoperabilitet, kan komma till stånd på förvaltningsgemensam nivå och på sektorsnivå,
- hur standardisering och eventuella systemväxlar (växlar för automatisk konvertering mellan standarder och format) bör användas vid utvecklingen av e-förvaltning,
- hur den offentliga sektorns utveckling av e-tjänster bör stödja övergången till ny teknik som t.ex. övergången till ”IPv6”, dvs. ett nytt system för tilldelning av Internets IP-adresser,
- hur en koncentration av administrativa stödtjänster kan ske inom statsförvaltningen,
- hur myndigheterna i framtiden bör driva, utbyta eller köpa och sälja IT-tjänster inom den statliga sektorn samt i samband med tjänsteexport,
- hur samverkan kring e-förvaltningsarbete inom sektorer kan främjas,
- hur fler e-tjänster för medborgare och företagare kan utvecklas, framför allt sådana tjänster som integrerar flera myndigheters

processer i användarvänliga gränssnitt, och hur myndigheters servicenivå för e-tjänster bör regleras samt

- hur IT-utvecklingen kan skapa möjligheter till förbättrad service för medborgare och näringsliv i gles- och landsbygd, med beaktande av lokala förutsättningar samt medborgares olika behov.

Koordinering av arbetet med e-förvaltning

Delegationen ska löpande samla in information om planerade och pågående e-förvaltningsprojekt som är av strategisk natur, dvs. projekt som påverkar förvaltningens samlade utvecklingsinriktning. En utgångspunkt i detta arbete ska vara den rapport som Verva, på uppdrag av regeringen, tog fram på området – 69 myndigheter redovisar 915 strategiska insatser för utveckling av e-förvaltning (Verva 2008:14). Delegationen ska utifrån denna information sammanställa och analysera myndigheternas e-förvaltningsprojekt. Delegationen ska verka för att regeringens förvaltningspolitiska mål vägs in i planeringen och genomförandet av de viktigaste e-förvaltningsprojekten och verka för att dubbelarbete undviks. Delegationen ska årligen redovisa en sammanställning av myndigheternas planerade och pågående e-förvaltningsprojekt samt bedöma om de projekten understöder de förvaltningspolitiska mål som regeringen har satt upp. Delegationen ska vidare i sina rapporter redovisa goda förebilder inom e-förvaltningen.

Uppföljning av det samlade arbetet med e-förvaltning

Delegationen ska från och med 2010, utifrån de förvaltningspolitiska målen, och de mål som regeringen kan komma att besluta på området, följa upp myndigheternas samlade arbete med e-förvaltning. Arbetets konsekvenser för brukarna ska beskrivas och analyseras.

Indikatorer för uppföljning ska utarbetas. Vid utarbetandet av indikatorer angående service, förvaltningens interna effektivitet och administrativ börda ska samråd ske med Myndigheten för tillväxtpolitiska utvärderingar och analyser (TUA). Vad gäller indikatorer på andra områden ska delegationen samråda med andra berörda myndigheter.

Delegationen ska ta fram förslag på metoder för hur planerade besparingar i myndigheternas e-förvaltningsarbete i högre grad kan realiseras och tas till vara.

Koordinering av IT-standardiseringsarbete

Delegationen ska samordna den statliga förvaltningens IT-standardiseringsarbete avseende e-förvaltning. Delegationen ska se till att metod- och expertstöd i IT-standardiseringsfrågor inom den statliga förvaltningen tillhandahålls, också när det gäller begreppsstandarder. Arbetet ska utföras i samverkan med SKL. Samordningen av IT-standardiseringsarbetet ska främja användningen av öppna standarder. Delegationen ska beakta det IT-standardiseringsarbete som pågår på internationell nivå.

Stöd till regeringen i det internationella arbetet

Delegationen ska bistå regeringen i EU-samarbetet och i det internationella arbetet med frågor om e-förvaltning.

Delegationen ska bistå regeringen vid beredningen av svenska ståndpunkter i EU och andra mellanstatliga organ i ärenden som rör standarder och standardisering på IT-området. Delegationen ska leda och samordna ett IT-standardiseringsråd med företrädare för de viktigaste intressenterna i staten, kommuner och landsting samt i intresseorganisationer och företag. Delegationen ska följa utvecklingen på området och delta i diskussioner och informationsutbyte om frågor som rör det internationella arbetet med standardiseringsfrågor på IT-området. Dessa ärenden kan beröra olika samhällssektorer och delegationens uppdrag kan i denna del komma att beröra frågor som inte enbart avser e-förvaltning.

E-nämndens och Vervas vägledningar och rapporter

Delegationen ska inventera och vid behov utveckla den tidigare E-nämndens och dåvarande Vervas vägledningar och rapporter på det aktuella området.

Uppdragets genomförande

I frågor som rör den strategiska utvecklingen av elektronisk förvaltning ska delegationen löpande rapportera till den interdepartementala arbetsgruppen för elektronisk förvaltning (dnr Fi2007/1981) och vid behov även till statssekreterargruppen för e-förvaltning.

Delegationen ska tillkalla en arbetsgrupp bestående av ansvariga för strategiska e-förvaltningsprojekt, eller motsvarande verksamhetsutvecklare, som arbetar på myndigheter eller organisationer som deltar i delegationens arbete.

Vid behov ska delegationen även tillkalla en referensgrupp bestående av företrädare för näringsliv, forskare och brukare för att ta del av deras kunskaper och vidgade perspektiv på delegationens arbete.

Det är angeläget att utvecklingsarbetet avseende e-förvaltningen sker i samverkan med SKL. Samarbetet ska inriktas mot att nå en samsyn mellan staten, landsting och kommuner kring strategiskt viktiga e-förvaltningsfrågor. Samverkan ska också ske med näringslivet bl.a. inom standardiseringsarbetet i likhet med vad som anges i Riktlinjerna till statssekreterargruppen för e-förvaltning (Fi2007/1981).

I syfte att koordinera det strategiska e-förvaltningsarbetet och för att stärka pågående reformer inom e-förvaltningen, ska delegationen föra en dialog kring samordning av pågående insatser med berörda myndigheter.

Delegationens arbete ska genomföras i samråd med de myndigheter som har särskilda uppgifter inom IT-säkerhetsområdet, bl.a. MSB samt Post- och telestyrelsen (PTS). Delegationen ska också samråda med MSB i frågor om elektronisk identifiering och underskrift.

Redovisning

Delegationen ska inledningsvis ta fram förslag till en strategi för myndigheternas arbete med e-förvaltning som ska lämnas till regeringen senast den 30 september 2009 (Finansdepartementet).

Delegationen ska med början 2010 redovisa sitt arbete till regeringen (Finansdepartementet) senast den 20 mars respektive den 1 oktober varje år.

Ett förslag till hur arbetet kan föras vidare i ett längre perspektiv ska lämnas senast den 20 mars 2014.

En slutredovisning av arbete ska lämnas senast den 31 december 2014.

Delegationen ska, utöver vad som i kommittéförordningen (1998:1474) föreskrivs om konsekvensbedömningar, beskriva konsekvenser för användare av e-tjänster.

Delegationen ska också redovisa till regeringen om den i sitt arbete identifierar regelverk som på ett olämpligt sätt hindrar elektroniskt informationsutbyte. Vid behov ska delegationen lämna förslag till författningsändringar.

Delegationen ska hålla berörda centrala arbetsorganisationer informerade om arbetet och ge dem möjlighet att framföra synpunkter.

Det är regeringens avsikt att utvärdera delegationens verksamhet innan 2014.

(Finansdepartementet)

Tilläggsdirektiv 2010:32

Beslut vid regeringssammanträde den 25 mars 2010.

Utvidgning av uppdraget

E-delegationen har tidigare fått i uppdrag att bl.a. koordinera de statliga myndigheternas IT-baserade utvecklingsprojekt. Utöver det ursprungliga uppdraget ges delegationen i uppdrag att främja och samordna myndigheternas arbete med att förbättra förutsättningarna för vidareutnyttjande av handlingar. Arbetet ska ta sin utgångspunkt i den lag om vidareutnyttjande av handlingar från den offentliga förvaltningen som föreslås i propositionen Offentlig förvaltning för demokrati, delaktighet och tillväxt (prop. 2009/10:175). Delegationen ska även inom ramen för sitt uppdrag att utveckla vägledningar ta fram riktlinjer för statliga myndigheters användning av sociala medier exempelvis webbforum och bloggar.

E-delegationens ursprungliga uppdrag

Regeringen beslutade den 26 mars 2009 att ge en kommitté i uppdrag att bl.a. koordinera de statliga myndigheternas IT-baserade utvecklingsprojekt samt följa upp dess effekter för medborgare, företagare och medarbetare. Ytterligare uppgifter är att koordinera vissa IT-standardiseringsfrågor och att bistå regeringen i det internationella arbetet på området. Syftet är att stärka utvecklingen av e-förvaltningen och skapa goda möjligheter för myndighetsövergripande samordning (dir. 2009:19). Kommittén har antagit namnet E-delegationen (Fi 2009:01).

Vidareutnyttjande av offentlig information

Information som samlas in eller framställs av myndigheter har ofta användningsområden utanför den offentliga förvaltningen. Det finns flera exempel på information hos myndigheter som kan användas kommersiellt. Väderinformation kan t.ex. användas för kommersiella vädertjänster och kartinformation och annan geografisk information kan användas för t.ex. GPS-tjänster. Ytterligare ett exempel är den officiella statistiken. Offentlig information från svenska myndigheter vidareutnyttjas sedan länge i betydande omfattning för såväl kommersiella som ideella ändamål. Eftersom svenska myndigheter har betydande informationstillgångar av hög kvalitet i elektronisk form är potentialen för vidareutnyttjande stor.

Det är enligt regeringens mening viktigt att förbättra förutsättningarna för vidareutnyttjande av information från myndigheter för både kommersiella och ideella ändamål.

PSI-direktivet

Europaparlamentet och rådet antog den 17 november 2003 ett direktiv (2003/98/EG) om vidareutnyttjande av information från den offentliga sektorn (PSI-direktivet)[59]. Direktivet innehåller en uppsättning minimiregler för vidareutnyttjande av handlingar som finns hos myndigheter och vissa andra organ. Syftet med direktivet är att skapa förutsättningar för en europeisk informationsmarknad genom att genomföra ett minimum av harmonisering och anta en allmän ram för villkor för vidareutnyttjande av handlingar som produceras inom den offentliga förvaltningen. Direktivet skulle vara genomfört i medlemsstaterna den 1 juli 2005. Direktivet har delvis genomförts genom förordningen (2008:31) om villkor vid vidareutnyttjande av information från statliga myndigheter.

I propositionen Offentlig förvaltning för demokrati, delaktighet och tillväxt (prop. 2009/10:175) föreslås en lag om vidareutnyttjande av handlingar från den offentliga förvaltningen. Genom den föreslagna lagen genomförs PSI-direktivet i svensk rätt.

[59] EGT L 345, 31.12.2003, s. 90, Celex 32003L0098.

Riktlinjer för användning av s.k. sociala medier

E-delegationen redogör i sitt delbetänkande Strategi för myndigheternas arbete med e-förvaltning (SOU 2009:86) för den ökade internetkompetensen hos medborgare och företag. Myndigheterna har samtidigt börjat använda s.k. sociala medier för att fånga upp användarnas behov i syfte att utveckla sina tjänster. Enligt delegationen bör en sådan utveckling främjas.

Uppdraget

Vidareutnyttjande av information

Delegationen ges i uppdrag att, med utgångspunkt i den föreslagna lagen om vidareutnyttjande av handlingar från den offentliga förvaltningen, främja och samordna myndigheternas arbete med att förbättra förutsättningarna för vidareutnyttjande av information från den offentliga förvaltningen.

I sitt arbete för att förbättra förutsättningarna för vidareutnyttjande av information ska delegationen verka för erfarenhetsutbyte och kunskapsspridning om goda exempel på hur information kan tillhandahållas. Delegationen ska undersöka hur information praktiskt och tekniskt kan tillhandahållas för automatiserade uttag i de fall uttag i sådan form är tillåtet och den berörda myndigheten har bedömt att utlämnande av informationen i elektronisk form är lämpligt. Delegationen ska i detta arbete särskilt uppmärksamma behovet av skydd för den personliga integriteten. När det gäller frågor om utlämnande av handlingar i elektronisk form ska delegationen dessutom beakta de överväganden och förslag som redovisas i E-offentlighetskommitténs slutbetänkande Allmänna handlingar i elektronisk form – offentlighet och integritet (SOU 2010:4).

I PSI-direktivets artikel 8.2 anges att myndigheterna ska uppmuntras att använda standardiserade licenser. Delegationen ska bedöma på vilka områden och för vilken typ av handlingar sådana standardiserade licenser kan behövas och vilka frågor de bör reglera. Delegationen ska, om den bedömer att det behövs, i samråd med berörda myndigheter utarbeta sådana standardiserade licenser och föreslå hur de ska hanteras i framtiden.

Vidare ska delegationen verka för att myndigheterna på ett ändamålsenligt sätt informerar om vilka handlingar som finns hos myndigheten och som tillhandahålls för vidareutnyttjande.

Delegationen ska utveckla former för att tillgängliggöra informationen om handlingar för vidareutnyttjande i en samlad form, t.ex. på en gemensam webbplats. Delegationen ska i detta arbete säkerställa att skyddet för den personliga integriteten kan upprätthållas.

Delegationen ska särskilt uppmärksamma förutsättningarna för mindre och nyetablerade företag att få tillträde till marknaden för offentlig information.

Delegationen ska följa utvecklingen på området och bedöma behovet av ytterligare förvaltningsgemensamma insatser. Delegationen ska utreda om någon myndighet behöver ges stödjande, vägledande, samordnande eller andra uppgifter på området.

Riktlinjer för användning av sociala medier

Delegationen ska inom ramen för sitt uppdrag att utveckla vägledningar även ta fram riktlinjer för statliga myndigheters användning av sociala medier, t.ex. Facebook och Twitter. Delegationen ska i detta arbete särskilt beakta rättsliga aspekter på sådan användning.

Uppdragets genomförande

Uppdraget ska genomföras i samråd med berörda myndigheter.

Delegationen ska särskilt samråda med Datainspektionen och Riksarkivet. När det gäller arbetet att främja, leda och samordna myndigheternas arbete med att förbättra förutsättningarna för vidareutnyttjande av information ska delegationen även samråda med Ekonomistyrningsverket och Statskontoret samt på lämpligt sätt med andra aktörer t.ex. näringslivet.

Delegationen ska inte föreslå ändringar i grundlag.

Arbetet ska redovisas i de rapporter som delegationen enligt sina direktiv ska lämna den 1 mars och den 1 oktober varje år.

(Finansdepartementet)

Tilläggsdirektiv 2013:40

Beslut vid regeringssammanträde den 25 april 2013.

Utvidgning av uppdraget

Regeringen beslutade den 26 mars 2009 att tillkalla en delegation för e-förvaltning med uppdrag att bl.a. koordinera vissa it-standardiseringsfrågor (dir. 2009:19). Delegationen antog namnet E-delegationen och ska lämna sin slutrapport senast den 31 december 2014. Utöver det ursprungliga uppdraget ska E-delegationen göra en behovsinventering beträffande standarder inom socialtjänstens område samt angränsande områden inom hälso- och sjukvård inom ramen för regeringens överenskommelse med Sveriges Kommuner och Landsting om stöd till en evidensbaserad praktik för god kvalitet inom socialtjänsten.

Behovet av ökad standardisering lyfts ofta fram från utförare och huvudmän inom både socialtjänst och hälso- och sjukvård. Huvudmännen ansvarar för att ha informationssystem som är ändamålsenliga utifrån ett kvalitets-, effektivitets- och säkerhetsperspektiv. En tydlighet kring vilka standarder som kan användas kan öka förmågan hos olika system att kunna kommunicera med varandra, vilket leder till ökad interoperabilitet. Att kunna dela information digitalt skapar bättre förutsättningar för effektivitet, kvalitet och säkerhet för brukare och patienter. Det kan påskynda införandet av it-stöd och underlätta utveckling av e-tjänster. Det kan även främja konkurrens mellan leverantörer av it-system och därigenom skapa förutsättningar för lägre kostnader.

E-delegationen ska i samverkan med andra relevanta aktörer göra en behovsinventering för att klargöra inom vilka områden som det finns anledning att nationellt enas kring ett antal fast-ställda normer eller regler. Målet med att peka ut ett antal nationella standarder ska vara att åstadkomma en ökad interoperabilitet för en

mer effektiv och säker informationsöverföring mellan individ, utförare, kommun, landsting och statliga myndigheter. Detta bör göras i syfte att skapa bättre förutsättningar för planering, genomförande och uppföljning av socialtjänst och hälso- och sjukvård, vilket är grunden för god kvalitet och effektivitet.

Uppdraget innebär att sammankalla Socialstyrelsen, Sveriges Kommuner och Landsting och andra representanter för kommuner och landsting, Vårdföretagarna, Famna, Swedish Medtech, Inera samt yrkesverksamma inom området och andra relevanta aktörer. Uppdraget innebär vidare att, i samverkan med de nämnda aktörerna, inventera behovet av standarder för att möjliggöra informationsöverföring mellan it-stöd och system. Arbetet ska fokusera på socialtjänsten samt områden i hälso- och sjukvården som angränsar till socialtjänsten, som t.ex. hemsjukvård, missbruks- och beroendevård samt psykiatri.

Arbetet ska resultera i konkreta förslag på områden där nationellt angivna standarder bör användas i högre grad än i dag. Det ska framgå om detta bör åstadkommas genom en ökad tydlighet kring vilka befintliga standarder som kan användas, eller om nya standarder behöver utvecklas. Förslagen ska även gälla vilken typ av standarder som bör användas eller utvecklas. Om det finns ändamålsenliga internationella standarder så är det att föredra jämfört med att ta fram nationella standarder. Vidare ska förslagen gälla hur en ökad användning av standarder kan åstadkommas för att få legitimitet och genomslag. En utgångspunkt för hela arbetet ska vara att tillvarata den effektiviserings-, förbättrings- och besparingspotential som standardisering erbjuder.

Tilläggsuppdraget ska redovisas senast den 1 november 2013. Förslagen bör även gälla hur en ökad användning av standarder kan åstadkommas för att få legitimitet och genomslag. I redovisningen ska E-delegationen ge förslag på parter som kan ta över, förvalta och verkställa förslagen.

(Näringsdepartementet)

Närmare om eget utrymme

Myndigheternas utvecklingsarbete

SAMSET-projektet och E-nämnden

Arbetet för rättslig och teknisk samordning vid myndigheternas utveckling av e-tjänster tog fart på 2000-talet genom att några myndigheter[60] inom ramen för ett projekt som började som ett regeringsuppdrag – det s.k. SAMSET-projektet – utarbetade gemensamma lösningar för e-legitimationer och anknytande frågor om service och ärendehandläggning i digital miljö. Syftet var att bygga en nationell infrastruktur som på bred front skulle kunna stödja e-tjänster på ett juridiskt korrekt sätt.

Resultaten från SAMSET-projektets arbete dokumenterades i ett antal vägledningar som övervägdes och beslutades av Nämnden för elektronisk förvaltning (E-nämnden). Dessa vägledningar kom att bli tongivande för hela myndighetsområdet och de används alltjämt; se E-nämndens vägledningar för

- myndigheternas användning av e-legitimationer och elektroniska underskrifter (E-nämnden 04:02),[61]
- användargränssnitt som uppfyller legala krav (e-nämnden 04:03),[62]

[60] Bolagsverket, Skatteverket, Försäkringskassan, CSN, Riksarkivet och Statskontoret.
[61] Där behandlas rutiner och säkerhetskrav på myndighetsområdet för att utfärda e-legitimationer och för att använda och förlita sig på sådana legitimationer. I vägledningen har dessutom den terminologi som används i samband med hanteringen av e-legitimation och e-tjänster presenterats och kompletterats med en förenklad beskrivning för vanliga användare. E-nämndens vägledning har visserligen inte någon tvingande verkan, såsom lag eller annan författning, men eftersom många av reglerna tagits in i den upphandling av e-legitimationer som gjorts tillämpas de i praktiken på bred front bland statliga myndigheter.
[62] Denna vägledning är utformad som ett komplement till den grundläggande vägledningen och syftar till att samordna myndigheternas användargränssnitt så att medborgaren känner igen sig i olika e-tjänster och till att tydliggöra juridiskt relevanta punkter i processen så att de elektroniska tjänsterna stämmer överens med de juridiska kraven.

- hantering av inkommande elektroniska handlingar (e-nämnden 05:02),[63]
- myndighetsföreskrifter vid införande av e-tjänster (e-nämnden 05:03),[64] och
- information som enligt lag ska lämnas på webbplatser (E-nämnden 05:03).[65]

Viktiga frågor var

- när en handling som ges in med stöd av en myndighets e-tjänst ska anses inkommen enligt förvaltningslagen, och
- hur den kommunikation och de behandlingar ska betraktas från juridiska utgångspunkter som sker i en myndighets e-tjänst i en fas före det att de färdiga handlingarna ges in.

När en enskild använder en myndighets e-tjänst sänds uppgifter tekniskt från ingivarens dator till myndighetens system. I samma skede sänds uppgifter tekniskt från myndighetens system till ingivarens dator, redan för att användaren ska kunna se en webbsida på sin skärm och interagera för att t.ex. upprätta ett utkast till en inlaga. En fråga som övervägdes var om redan dessa informationsmängder skulle bli att anse som inkomna till myndigheten respektive expedierade från myndigheten så att regler om diarieföring, handlingsoffentlighet och arkivering m.m. skulle anses tillämpliga i den fasen.

Av intresse i denna del är E-nämndens vägledning för inkommande elektroniska handlingar. Enligt den skulle punkten för inkommande i digital miljö inte anses inträda förrän en handling har nått den funktion för automatiserad behandling som myndigheten har anvisat som mottagningsställe – i vägledningen kallad *mottagningsfunktion.* Att en enskild mellanlagrar ett utkast i myndighet-

[63] Vägledningen klarlägger grundläggande juridiska och administrativa frågor kring rättsliga krav på utformningen av e-tjänster. Bland annat behandlas när en handling ska anses ha kommit in till en myndighet, var gränsen mellan service och ärendehandläggning går och vilken information som bör finnas tillgänglig för en myndighet som ska kontrollera om elektroniska handlingar är äkta.

[64] Vägledningen kan ge stöd när förslag och remissynpunkter lämnas rörande reglering i lag eller förordning för att införa e-tjänster, när myndighetsföreskrifter tas fram för en e-tjänst och när föreskrifter för e-tjänster skall tillämpas.

[65] Myndigheter är enligt lag skyldiga att lämna juridisk information på sina webbplatser. Av denna vägledning framgår när och hur en myndighet är skyldig att presentera sådan information.

ens informationssystem leder enligt denna vägledning inte till att utkastet anses inkommet i förvaltningsrättslig mening – det har inte ännu nått ”mottagningsfunktionen”.[66] Så länge arbetet med att upprätta inlagor pågår kan användaren enligt vägledningen sägas befinna sig i ett *serviceläge*, vilket beskrevs så att den som använder en e-tjänst får hjälp och stöd på ett sätt som liknar den hjälp som en handläggare ger vid ett personligt besök hos myndigheten.

I vägledningen konstaterades således att en elektronisk handling inte anses inkommen i förvaltningsrättslig mening förrän den ”anländer till myndigheten” – så som det uttrycks i 10 § FL. Enligt vägledningen skulle detta förstås så att handlingen i digital miljö har kommit in *när den har nått mottagningsfunktionen*. I en kommentar till vägledningen anfördes vidare att denna tolkning bör gälla oavsett om försändelsen når en myndighet via en e-tjänst, e-post eller någon annan elektronisk ”kanal” där den kan tas emot.

I praktiken bör därmed, i de allra flesta fall, den punkt där en elektronisk handling anses ha anlänt till myndighet kunna knytas till den tekniska registrering som sker i den mottagningsfunktion som utgör myndighetens ”brevlåda” för att ta emot sådana meddelanden.

I anknytning till SAMSET-projektet publicerades också en artikel i Svensk Juristtidning, Inkommande handlingar – en IT-anpassad tolkning (SvJT 2005, s. 273 ff.). Där noterades att uttalanden i lagmotiv och doktrin rörande inkommande elektroniska handlingar delvis var motsägelsefulla och att utvecklingen på IT-området inte hade beaktats fullt ut. I artikeln påpekades också att vissa av de resonemang som förts i den juridiska doktrinen saknade förankring i informationssystemens och kommunikationsvägarnas sätt att fungera samt kunde ge utrymme för myndigheter att förfoga över inkommandepunkten.[67] Dessa resonemang, som riskerade att resultera i dels ett begränsat hänsynstagande till den elek-

[66] En jämförbar situation i fysisk miljö skulle enligt kommentarer i vägledningen kunna vara att en enskild som besöker en myndighet och inte hinner färdigställa sina inlagor och får löfte att lämna kvar sina papper till nästa dag, när den enskilde återkommer och fortsätter sitt arbete. Den omständigheten att en individ förvarar en väska med handlingarna i myndighetens lokaler medför inte att handlingarna anses inkomna i förvaltningsrättslig mening. Först senare vidtar användaren åtgärder för att ge in handlingarna och först då kommer de in i förvaltningsrättslig mening.

[67] För ingivarna är det emellertid ett självklart rättssäkerhetskrav att myndigheterna inte i enskilda fall ska kunna förfoga över inkommandepunkten genom att t.ex. vänta med att läsa eller skriva ut en elektronisk inlaga och såväl ingivare som myndigheter behöver veta i vilka delar befordran sker på avsändarens respektive mottagarens risk.

troniska miljöns särskilda förutsättningar, dels ett bristande skydd för enskildas rättssäkerhet, redovisades som alternativ utifrån

1. *en tillgänglighetsprincip;* en upptagning anses enligt 2 kap. 6 § jämförd med 3 § TF inkommen till myndighet när annan har gjort den 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,
2. *en utskriftsprincip;* i viss doktrin[68] hade uttalats att en någorlunda säker ståndpunkt synes vara att ett elektroniskt meddelande kommer in först när en behörig företrädare för myndigheten tar hand om det, t.ex. genom att … göra en utskrift, eller
3. *en läs- eller omhändertagandeprincip;* beträffande e-post hade hävdats att det inte räcker att en handling finns tillgänglig för myndighet i dess hårddisk – den också borde ha gjorts tillgänglig för en behörig tjänsteman på datorns bildskärm för att anses inkommen; se Förvaltningsprocesslagen m.m. En kommentar, 4 u., s. 396.

Samtidigt redovisades *en förvaringsprincip* utifrån ett förslag till nya bestämmelser om inkommande handlingar som lagts fram av IT-utredningen i betänkandet Elektronisk dokumenthantering (SOU 1996:40). Utredningsförslaget byggde på att den elektroniska handlingen, för att anses inkommen, skulle ha anlänt till myndighetens elektroniska ”brevlåda”, vilken i förslaget kallades myndighetens ”elektroniska adress”.

Enligt artikeln Inkommande handlingar – en IT-anpassad tolkning kunde en utskrifts- eller en läs- eller omhändertagandeprincip inte ge tillräckligt skydd för den enskilde, medan en tillgänglighetsprincip, så som den elektroniska miljön utvecklats, skulle leda till en alltför vid förvaltningsrättslig inkommanderegel; allt som fanns tillgängligt på Internet riskerade att anses som inkommet till myndighet. En förvaringsprincip kunde däremot, enligt IT-utredningens bedömning och artikeln, ge en avgränsning som mottagande myndighet inte kunde förfoga över och som inte kunde leda till att en handling blev att anse inkommen redan när ett utkast skapas eller vid annan mellanlagring av uppgifter i samband med hjälp och stöd som myndigheter ger i digital miljö.

[68] Hellners och Malmqvist, Förvaltningslagen med kommentarer, 2003, s. 122.

Att digitala data kommuniceras på annat sätt än via en mottagningsfunktion – i vad som i artikeln kallades en *servicefas* – skulle alltså inte anses leda till inkommande i förvaltningslagens mening; handlingen skulle anses inkommen först när den nått myndighetens mottagningsfunktion. Motsvarande synsätt tillämpas också i fysisk miljö. En handling som en person tar med sig till en myndighet eller upprättar där och visar upp för en handläggare för att få råd om hur den ska fyllas i, men därefter tar med sig från myndighetens lokaler, anses inte inkommen i förvaltningslagens mening redan till följd av att den funnits i myndighetens lokaler. En e-tjänst behöver kunna användas på motsvarande sätt vilket förutsätter att elektronisk kommunikation till (och från) en e-tjänst kan äga rum utan att handling anses inkommen.

Oklara eller otidsenliga bedömningar kunde enligt artikeln bli kännbara för användare som ska ta tillvara sin rätt och för myndigheter som ska bygga sina webbplatser och e-tjänster så att de blir förenliga med regler om service, inkommande och handläggning av mål och ärenden.

Fortsatt utveckling mot ”eget utrymme”

I praktiken har det beskrivna synsättet utifrån en förvaringsprincip blivit genomfört på bred front inom e-förvaltningen. Det har på så sättet ansetts möjligt att tolka och tillämpa gällande rätt, i harmoni med digital infrastrukturs funktionssätt. Samtidigt har skyddet för den enskilde kunnat upprätthållas genom att en myndighet inte kan påverka inkommandepunkten genom att t.ex. senarelägga utskrift eller läsning av en handling som nått myndighetens mottagningsställe. En viktig komponent har också varit att ge skydd för den enskilde genom att kvittens sänds. En ingivare får därmed genast veta om en åtgärd för att ge in en handling elektroniskt har lyckats.

E-delegationen har enligt sina direktiv (dir. 2009:19 s. 10) i uppdrag att inventera och vid behov utveckla E-nämndens vägledningar och rapporter inom området.[69] E-delegationen har också vidareutvecklat detta sätt att se på elektronisk miljö genom att

- *dels* i en rapport om Direktåtkomst och utlämnande på medium för automatiserad behandling, hänvisa till vad som beskrivits

[69] SAMSET- projektet och E-nämnden har dock avvecklats. Den myndighet som övertog dessa uppgifter – Verket för förvaltningsutveckling (VERVA) – har också avvecklats.

som ett *serviceläge* (jfr den vid not 63 nämnda vägledningen av E-nämnden för hanteringen av inkommande elektroniska handlingar),

- *dels* i den nämnda juridiska vägledningen för verksamhetsutveckling inom e-förvaltningen, beskriva och använda det juridiska synsätt som tidigare kallats ett *serviceläge* eller en *servicefas*.

Det förtydligandet har också gjorts i E-delegationens juridiska vägledning för verksamhetsutveckling inom e-förvaltningen att det är fråga om ett *förlopp* där service ges åt användare – ett s.k. *serviceskede* – och att detta förlopp äger rum inom ramen för en *skyddad elektronisk plats* – ett s.k. *eget utrymme.* Meningen är att användaren där ska kunna upprätta utkast till handlingar eller annars för egen del behandla uppgifter utan insyn av någon annan.

Vid arbetet med E-delegationens juridiska vägledning för verksamhetsutveckling framkom att sådana utrymmen har kommit att bli bärande komponenter inom i stort sett varje it-baserad tjänst som en myndighet tillhandahåller åt enskilda i digital miljö. E-delegationen har härvid definierat

- *serviceskede* som förlopp där (1) service ges av myndighet enligt 4 § FL, (2) ärendehandläggning inte äger rum hos myndigheten, (3) endast den enskilde ges insyn, och (3) handling inte har kommit in till myndigheten enligt 10 § förvaltningslagen, och
- *eget utrymme* som skyddat förvar hos myndighet som den, enligt 2 kap. 10 § första stycket TF, tillhandahåller endast som led i teknisk bearbetning eller teknisk lagring för annans räkning.

Den bedömning som myndigheter ger uttryck för i anknytning till e-tjänster ger intryck av att frågan om *inkommande enligt förvaltningslagen* har uppfattats som *löst* genom de redovisade tolkningarna av gällande rätt *utifrån en förvaringsprincip;* dvs. att handling anses inkommen när den har nått en myndighets mottagningsställe.

Lagstiftningsarbetet

En utveckling mot en förvaringsprincip

Bedömningen att en handling som ges in elektronisk anses vara inkommen enligt den förvaltningsrättsliga regleringen, utifrån en förvaringsprincip – dvs. när den har nått myndighetens mottagningsställe – har också kommit till uttryck i lagstiftningsarbetet. Undantag följer visserligen av den särreglering som finns för vissa specialområden och som tillkommit innan myndigheter börjat koppla upp sig mot internet; se t.ex. de regler som gäller för tullen, där departementschefen fann att tryckfrihetsförordningens regler om inkommande borde utgöra en förebild (prop. 1989/90:40 s. 28). Under riksdagsbehandlingen betonade emellertid konstitutionsutskottet att det inte var givet att denna lösning skulle kunna användas på andra områden (bet. 1989/90:SkU19, bil. 1 s. 31).

När samma fråga kort därefter aktualiserades på skatteområdet, där förslag hade lagts fram om en inkommanderegel baserad på en förvaringsprincip, fann regeringen inte skäl att införa någon sådan regel. I stället hänvisades till IT-utredningens förslag att införa en sådan regel i förvaltningslagen (prop. 1996/97:100, del 1 s. 462 f.). Regeringen uttalade därvid bl.a. följande:

> Ett elektroniskt dokument har kommit in till myndigheten på sätt som sägs i förvaltningslagen när det kommit in till Riksskatteverket. Enligt regeringens bedömning kan mot bakgrund härav någon särreglering motsvarande den som finns i tullagen inte anses motiverad. Föreliggande och planerade rutiner för mottagningsfunktionen, bl.a. beträffande loggning av hela filer och kvittenser, gör att det i praktiken inte torde bli svårt att avgöra om och när ett dokument skall anses inkommet. Det är i datorbaserade förfaranden möjligt att tidsbestämma olika operationer i ett system.
>
> I enlighet med vad som gäller enligt förvaltningslagen bör sändandet av en upptagning ske på avsändarens risk. Ett elektroniskt meddelande som översänts till mottagningsfunktionen i en fil som är behäftad med ett sådant tekniskt fel att meddelandet inte kan tas emot kan inte anses ha kommit in. Genom ett system med kvittenser av mottagna dokument får avsändaren automatiskt kunskap om att en överföring misslyckats.

En förvaringsprincip har alltså ansetts gälla redan inom ramen för en tillämpning av 10 § FL i gällande lydelse. I senare lagstiftningsärenden har visserligen särreglering införts utifrån bedömningen att 10 § FL vid mera komplexa förhållanden ”ger mycket lite ledning” (prop. 2003/04:40 s. 40 f.). Denna reglering har emellertid byggt på

en förvaringsprincip, efter att det uppmärksammats att allt som nås genom en internetuppkoppling kan bli att anse som inkommet, om en tillgänglighetsprincip ska anses gälla. Regeringen uttalade i det sammanhanget att – vid den kommunikation mellan användare och myndighet som en självbetjäningstjänst innebär – det måste anses naturligt att en handling eller uppgift anses inkommen när den enligt registreringen anlänt till en viss bestämd server och att denna server lämpligen kunde betecknas anvisat mottagningsställe.[70]

Förvaltningslagsutredningen föreslår en förvaringsprincip

Förvaltningslagsutredningen har i sitt betänkande, En ny förvaltningslag (SOU 2010:29), föreslagit den hjälpregeln för inkommande, att en handling som har sänts till ett anvisat elektroniskt mottagningsställe ska anses ha kommit in när den har tagits emot där (s. 393). Förslaget framstår närmast som en kodifiering av vad som redan torde anses följa av 10 § FL.

Myndigheternas tolkning av 10 § FL utifrån en förvaringsprincip, inte en tillgänglighetsprincip, en utskriftsprincip eller en läs- eller omhändertagandeprincip, framstår därmed som förenlig med gällande rätt.

[70] Se även prop. 2005/06:28 s. 38 och prop. 2007/08:158 s. 17 f., där motsvarande bedömningar gjorts för andra förvaltningsområden, samt Förvaltningslagsutredningens redovisning i SOU 2010:29 s. 767 ff.

Statens offentliga utredningar 2014

Kronologisk förteckning

1. Vissa bostadsbeskattningsfrågor. Fi.
2. Framtidens valfrihetssystem
   – inom socialtjänsten. S.
3. Boende utanför det egna hemmet
   – placeringsformer för barn och unga. S.
4. Det måste gå att lita på konsumentskyddet. Ju.
5. Staten får inte abdikera
   – om kommunaliseringen av den svenska skolan. U.
6. Män och jämställdhet. U.
7. Skärpta straff för vapenbrott. Ju.
8. Översyn av statsskuldspolitiken. Fi.
9. Förändrad assistansersättning
   – en översyn av ersättningssystemet. S.
10. Ett steg vidare – nya regler och åtgärder för att främja vidareutnyttjande av handlingar. S.
11. Kunskapsläget på kärnavfallsområdet 2014. Forskningsdebatt, alternativ och beslutsfattande. M.
12. Utvärdera för utveckling – om utvärdering av skolpolitiska reformer. U.
13. En digital agenda i människans tjänst
    – en ljusnande framtid kan bli vår. N.
14. Effektiv och rättssäker PBL-överprövning. S.
15. Investeringsplanering för försvarsmateriel
    En ny planerings-, besluts- och uppföljningsprocess. Fö.
16. Det ska vara lätt att göra rätt
    Åtgärder mot felaktiga utbetalningar inom den arbetsmarknadspolitiska verksamheten. A.
17. Genomförande av Seveso III-direktivet. Fö.
18. Straffskalorna för allvarliga våldsbrott. Ju.
19. Yrkeskvalifikationsdirektivet – ett samlat genomförande. U.
20. Läkemedel för särskilda behov. S.
21. Bredband för Sverige in i framtiden. N.
22. Genomförande av EU:s nya redovisningsdirektiv. Ju.
23. Rätt information på rätt plats i rätt tid. Del 1, 2 och 3. S.
24. Olycksregister och djupstudier på transportområdet. N.
25. Internationella rättsförhållanden rörande arv. Ju.
26. Tillträde till COTIF 1999. Ju.
27. Svensk veteranpolitik. Ett ansvar för hela samhället. + Bilagor. Fö.
28. Lönsamt arbete – familjeansvarets fördelning och konsekvenser. A.
29. Assisterad befruktning för ensamstående kvinnor. Ju.
30. Jämställt arbete? Organisatoriska ramar och villkor i arbetslivet. A.
31. Visselblåsare
    Stärkt skydd för arbetstagare som slår larm om allvarliga missförhållanden. A.
32. Jordbruks- och bostadsarrende
    – några frågor om arrendeavgift och besittningsskydd. Ju.
33. Från hyresrätt till äganderätt. Ju.
34. Inte bara jämställdhet
    Intersektionella perspektiv på hinder och möjligheter i arbetslivet. A.
35. I vått och torrt – förslag till ändrade vattenrättsliga regler. M.
36. Frågor om följerätt och om museernas kopiering. Ju.
37. De svenska energimarknaderna
    – en samhällsekonomisk analys. Fi.
38. Tillväxt och värdeskapande
    Konkurrenskraft i svenskt jordbruk och trädgårdsnäring. L.
39. Så enkelt som möjligt för så många som möjligt
    Bättre juridiska förutsättningar för samverkan och service. N.

Statens offentliga utredningar 2014

Systematisk förteckning

Ett steg vidare – nya regler och åtgärder för att främja vidareutnyttjande av handlingar. [10]

Effektiv och rättssäker PBL-överprövning. [14]

Läkemedel för särskilda behov. [20]

Rätt information på rätt plats i rätt tid. Del 1, 2 och 3. [23]

Utbildningsdepartementet

Staten får inte abdikera – om kommunaliseringen av den svenska skolan. [5]

Män och jämställdhet. [6]

Utvärdera för utveckling – om utvärdering av skolpolitiska reformer. [12]

Yrkeskvalifikationsdirektivet – ett samlat genomförande. [19]