

RA Prof. Dr. Jochen Schneider

Beethovenstraße 6  
80336 München

Tel. 089/ 54 34 9 – 100  
Fax: 089/ 54 34 9 – 111  
E-Mail: jochen.schneider@ssw-muc.de

Kommission von Bundestag  
und Bundesrat zur Modernisierung  
der Bund, Länder, Finanzbeziehungen  
c/o Deutscher Bundestag

11011 Berlin

München, den 19.10.2007

**Anhörung am 08.11.2007**

Sehr geehrte Damen und Herren,

Sie haben mich zu der öffentlichen Anhörung am 08.11.2007 eingeladen. Hiermit sage ich meine Teilnahme gerne zu.

Es folgt meine Stellungnahme, zu deren Abgabe ich freundlicherweise noch etwas Fristverlängerung erhielt. Den Hintergrund, warum ich nur auf einige Fragen eingehe, habe ich einleitend versucht darzustellen.

Mit freundlichen Grüßen



Rechtsanwalt  
(Schneider)

Kommission von Bundestag und Bundesrat  
zur Modernisierung  
der Bund-Länder-Finanzbeziehungen

Kommissionsdrucksache  
070

**Jochen Schneider**

Als Rechtsanwalt bin ich mit IT-Recht, dort v.a. mit IT-Vertragsrecht und wiederum sehr häufig mit IT-Projekten befasst.

Als Honorarprofessor lehre ich an der juristischen Fakultät „Rechtsinformatik“, wozu auch die Automation in der öffentlichen Verwaltung gehört. Mein Bezug zu den Frage-Komplexen besteht zur IT (Informationstechnik) und dabei auch zu TK (Telekommunikation) und zu TM (Telemedien).

Eine Stellungnahme erfolgt vor diesem Hintergrund meiner Arbeit im wesentlichen speziell hinsichtlich Fragen in Kapitel IV., IT-Standards und Systeme, mittelbar und in Ansätzen zu Kapitel III., soweit sie damit in Verbindung stehen (Standardsetzung).

**Gliederung:**

<b>Zusammenfassung, Management-Summary</b>	<b>4</b>
<b>A Zur Abgrenzung von "Aufgabe" und "IT bzw. IT-Systemen"</b>	<b>8</b>
<b>I. Eigenheiten von IT-Projekten</b>	<b>8</b>
1. Eigenheit von Projekten: Änderungen im Projektverlauf	9
2. Differenzierung Planung und Realisierung	10
3. Anstieg der Änderungsrate in Abhängigkeit von der Dauer des Projekts	11
4. Dauer von Projekten	12
5. Änderungsrate und Projektdauer	12
6. Zwischenergebnis	12
<b>II. Verantwortlichkeit und „Stelle“ - Vorgaben des Datenschutzes</b>	<b>13</b>
<b>III. „IT-Sicherheit“</b>	<b>14</b>
<b>IV. (Service orientierte) Architektur(SOA): IT-Netzinfrastruktur</b>	<b>17</b>
<b>V. Kompatibilität, Interoperabilität</b>	<b>17</b>
<b>B. Einzelne Fragen</b>	<b>18</b>
Frage 121	18
Frage 233	18
Frage 251	18
Frage 252	19
Frage 253	20
Frage 254	20
Frage 255	21
Frage 256	22
Frage 257	22
Frage 258	23
Frage 259	23
Frage 260	24
Frage 261	24
Frage 262	24
Frage 263	25
Frage 264	25
Frage 265	25
Frage 267	26
Frage 268	26
<b>C. Ergebnis</b>	<b>27</b>
<b>D. Konsequenz für weitere Fragen:</b>	<b>28</b>

Die vorliegende Stellungnahme ist wie folgt aufgebaut:

Ein wesentlicher Punkt ist in **A** die Darstellung von etwas ungleichgewichtigen Komplexen, die zusammen auf Projekte einwirken und insgesamt das Verhältnis von Aufgabe zu IT-Lösungen beeinflussen. Diese fünf Komplexe sind also vor die "Klammer" gezogen. In **B** werden einzelne Fragen beantwortet und in **C** das Ergebnis dargestellt. In **D** sind noch zu einzelnen Fragen Antworten mit Bezug zu den vorausgehenden Ausführungen wiedergegeben. Dabei wird auf Aspekte verwiesen, die in Antworten zu anderen Fragen bereits Relevanz besitzen.

## Zusammenfassung, Management-Summary

IT-Anwendungen der öffentlichen Verwaltung dienen – genauso wie im privaten Bereich – zur technischen Unterstützung bei der Lösung fachlicher Aufgaben. Hinzu kommen Telekommunikations- und Mediendienste (TK- und TM-Dienste), die solchen Anwendungen zugrunde liegen können, um den Datentransport bzw. die sonstigen Dienste zu ermöglichen, die die (Tele-)Kommunikation und Erreichbarkeit/Verfügbarkeit, evtl. verbunden mit Verschlüsselungs- und Authentifizierungsverfahren, bewerkstelligen. Die Gestaltung und Errichtung solcher IT-, TK- und TM-Dienste, insbesondere die Planung, Erstellung bzw. Anpassung der Software für solche IT-Anwendungen wird als **Projekt** verstanden.

IT-Projekte weisen - ebenso wie im privaten - auch im öffentlichen Bereich **Eigenheiten** auf, wobei im Hinblick auf die Kooperationsformen und die Standardisierungen u.ä. zwischen dem Projekt im Sinne der Erstellung der Software bzw. des Systems einerseits und dessen Betrieb und Weiterentwicklung andererseits unterschieden werden kann. Diese Eigengesetzlichkeit bezieht sich v.a. auf Projektstrukturen und Projektrisiken, weniger auf den Betrieb.

Die technische Aufgabenlösung bzw. -erfüllung wird durch eine Software-Ausgestaltung bewerkstelligt, die es, jeweils zugeschnitten auf den einzelnen Aufgabenbereich, zu erstellen oder durch Anpassung von Standardsoftware zu gewinnen gilt. Für die fachgerechte Durchführung eines Projekts ist es hinsichtlich der erforderlichen **Projektschritte und der typischer Weise auftretenden Probleme** nicht sehr entscheidend, ob man ein Projekt **intern** innerhalb einer Verwaltung oder **extern** durch ganze oder teilweise Vergabe durchführen will. Auch bei externer Vergabe verbleibt ein Projekt mit dem Inhalt „Mitwirkung“ im Hause des Auftraggebers. Allerdings treten die Probleme und die einzelnen Verarbeitungsschritte bei externer Vergabe wesentlich deutlicher hervor.

Die „richtige“ Projektstruktur wäre also auch dann einzuhalten, wenn ein Projekt intern nur mit eigenen Kräften realisiert würde. Die Auswirkungen, dass sich erfahrungsgemäß Projekte nicht an die „richtige“ Struktur halten“, sind bei großen Projekten unverhältnismäßig stärker.

**Die Eigengesetzlichkeit kurz zusammengefasst:**

Je umfangreicher ein Projekt und komplexer die Aufgabenstellung ist und je länger das Projekt deshalb dauert, desto mehr ändert sich während des Projektverlaufs bereits die Technik. Die Technik, auf der das Projekt planerisch aufbaut, kann bereits veraltet sein, wenn das Projekt fertig gestellt ist. Des Weiteren entstehen während des Projektverlaufs in vielen Fällen unabweisbare Ergänzungs- und Änderungswünsche der Anwender (z.B. Fachabteilungen), die zu einem erheblichen Teil auch durch Änderungen der zugrunde liegenden Gesetze und Verordnungen hervorgerufen werden. Das heißt, dass das Projekt mit einer Quote von Änderungswünschen zu rechnen hat, die sich umso gravierender auswirken, je umfangreicher die Änderungen sind und je größer das Projekt ohnehin angelegt ist. Ein Grund dafür, dass Projekte so komplex angelegt sind, bilden die Varianten der Forderungen der Anwender. Je größer die Zahl beteiligter Einheiten, umso größer ist die Rate individueller Anforderungen. Bei Effektuierung von Projekten ist eine hilfreiche Formel, dass 85 %, teilweise vielleicht auch 90 % mit Standard bzw. mit gemeinsamen Forderungen diverser, also auch Länder-übergreifender Forderungen abgedeckt sein könnten, so dass nur 10 % oder 15 % jeweils Anwender- oder Landes- bzw. Verwaltungsindividuell beschaffen sein müssten.

Die beiden Einflussfaktoren - technische Entwicklung und Änderungsforderungen - multiplizieren sich in gewissem Sinne mit der Folge, dass längerfristig angelegte Projekte hinsichtlich ihrer zusätzlichen Verlängerung überproportional unter **Verlängerungsgefahr** und **Zusatzaufwand** für Änderungen leiden. Die Effekte beider Einflussfaktoren schaukeln sich gegenseitig hoch. Die **Gefahr des Scheiterns** wächst damit ebenfalls stark, wenn nicht überproportional [ s. Beispiel: FISCUS, Frage 233].

Dies ruft **einerseits** danach, Kooperationsformen zu schaffen, die diese Aufwandsverteilung nutzen. Z.B. kann „einer für alle“ die 85 % und 15 % für sich entwickeln und den übrigen Beteiligten die Möglichkeit geben, bei einer Entscheidung für die Nutzung der Lösung neben der Nutzung der 85 % Standard 15 % Eigen-Entwicklung zu betreiben, also die Abweichungen zu realisieren.

Ebenso wäre auch eine gemeinschaftliche Basis von Anfang an zu schaffen, indem die 85 % „Standard“ gemeinsam entwickelt werden und sich jeder Teilnehmer 15 % individuell entwickeln lässt. Schließlich wäre es denkbar und wird auch praktiziert, dass Standardsoftware angeschafft wird, die diesen Abdeckungsgrad eventuell in Kombination mit gemeinschaftlichen Arbeiten erreicht, um dann auch noch die Möglichkeit aufzuweisen, durch Parametrierung u.ä. Maßnahmen die individuellen Eigenheiten im Übrigen abzubilden.

Beispiele für die angedeuteten Kooperationen bzw. Formen individueller Ausgestaltungen sind etwa, dass beim Grundbuch 14 Bundesländer die maßgeblich unter der Führung eines Landes entwickelte Lösung einsetzen, zwei Länder eine andere. Beim elektronischen Handelsregister setzen alle 16 Bundesländer die maßgeblich unter der Führung eines Landes entwickelte Lösung ein. Es gibt also funktionierende Mechanismen, wie auch die Beispiele des Mahnverfahrens mit mehrheitlicher Anwendung der Lösung aus einem Land zeigen. Dabei ist noch zu berücksichtigen, dass Mahnverfahren und Grundbuch mit ihren Ursprüngen technisch gesehen in einer Zeit wurzeln, wo die Möglichkeiten zu parametrierbarer bzw. anpassbarer Software wie heute nicht bestanden.

Andererseits würde eine Zentralisierung der Projektentwicklung selbst die Projekte nicht beschleunigen, sondern in dem Umfang überproportional verlängern, in dem 16 Länder sich abzubilden und abzustimmen hätten.

Die Kooperationsformen wie sie heute bestehen, sind nicht durch Zentralisierung abzulösen, sondern deren Nebeneinander und „Wildwuchs“ ist dahingehend einzudämmen und deren interne Prozesse zu strukturieren, dass nicht mehrere Institutionen oder Ebenen unabgestimmt die Themen bearbeiten. Es wäre also wichtig, eine einheitliche Gremien-Struktur unter einem relativ hoch „aufgehängten“ oberstem Gremium zu schaffen.

Aufgabe dieses Gremiums kann nicht die Koordinierung technischer und fachlicher Entwicklungen der Länder und des Bundes sein, sondern Kernaufgabe muss die Sicherstellung der Interoperabilität der möglichen Lösungen sein. Dies bedeutet, dass eine Absprache über (Austausch-) Standards schnell und verbindlich erfolgen muss. Die Umsetzung in Produkte kann in der Folge jeweils dezentral oder durch projektbezogene Partnerschaften erfolgen.

Bei der zentralen Abstimmung der Austauschstandards ist weitgehend die Länder-Struktur abzubilden, um die föderale Struktur zu repräsentieren. Dies folgt auch daraus, dass die verschiedenen, je nach Art der Projektumsetzung und der zu realisierende Lösung auf Basis der einschlägigen Gesetze, Verordnungen und ggf. Verwaltungsvorschriften die technischen Lösung unterschiedlich angelegt sein können, aber – falls notwendig - im Sinne der Interoperabilität einheitliche Datenaustausch-Standards eingehalten werden müssen. Eine Struktur könnte damit etwa wie folgt aussehen:

Es gibt, Bundesland-bezogen, Entscheidungsträger, die in einem definierten Abstimmungsmodus die evtl. mit externer Unterstützung aufbereiteten Planungen beraten. Sie bereiten so eine Entscheidungsgrundlage für ein demokratisch legitimes Gremium vor. Hierfür bietet sich die Ministerpräsidentenkonferenz bzw. die Konferenz der Chefs der Staats- und Senatskanzleien an.

Dieses System könnte über einen **Grundlagenstaatsvertrag** etabliert werden. Damit würde eine grundsätzliche Übereinkunft zur Nutzung von möglichst einheitlichen Standards und damit zur Interoperabilität der technischen Lösungen zu Grunde gelegt. Über jeweils einen gesonderten Staatsvertrag würde dann die Möglichkeit bestehen, dass die Bundesländer jeweils für sich entscheiden können, ob sie der Umsetzung einer technischen Lösung beitreten wollen.

Die strukturellen Probleme zentraler und damit zugleich sehr großer Projekte beim Staat gleichen denen bei großen Projekten im Bereich der Privatwirtschaft. D.h. also, dass Verzögerungen praktisch eingebaut sind. Die Strukturen, die evtl. gerade die Schwierigkeiten machen, wenn sie in zentrale Projekte eingebracht werden, können evtl. wesentlich leichter dadurch abgebildet werden, dass Landes-spezifische Ausprägungen unterschiedlich ausgestaltet werden, jeweils aber die Anforderungen der gesetzten Schnittstellen einhalten und so die Interoperabilität zwischen den Ländern ermöglichen. Damit hat auch jedes Land die Entscheidung bei sich, ob und wie weit es sich dem Standard anpasst oder nicht

Die Abstimmung, wo noch erforderlich, könnte in den oben bereits angedeuteten Gremien bzw. nach dem Entscheidungsablauf, wie oben dargestellt, erfolgen. Gegenüber den bisher praktizierten Verfahren und Strukturen würde die Vielzahl der bisherigen Gremien und deren Entscheidungsprozesse abgebaut und vereinheitlicht werden. Dies betrifft etwa den Arbeitskreis Informationstechnologie, den „Kooperationsausschuss ADV“, die Staatssekretärsrunde für eGovernment, die jeweiligen Arbeitsgruppen der Fachministerkonferenzen u.ä.

Weiter ist zu beachten, dass sich die IT-Lösung für eine vorgegebene Verwaltungsaufgabe an den Organisationsentscheidungen des jeweiligen Landes und der Kommunen orientieren muss. Bei der Übernahme einer zentral und standardisiert vorgegebenen Lösung hätte die Verwaltung lediglich die Möglichkeit, die Standardlösung auf ihre Belange anzupassen oder aber ihre Organisationsabläufe und Strukturen an die IT-Lösung anzupassen. Beides kann mit erheblichem Aufwand verbunden sein:

Eine Standardlösung kann (wie oben bereits angesprochen) zwar durchaus ca. 85 % der notwendigen Anforderungen abdecken, muss dies aber nicht; hinzukommt, dass oftmals gerade die letzten 15 % der Realisierung einer individuellen Ausprägung für die jeweilige Stelle den größeren Aufwand verursachen.

Als Beispiel für den erheblichen Aufwand bei etwaiger Anpassung der Organisation an die IT-Lösung können Einführungsprojekte für betriebswirtschaftliche Standardsoftware in Unternehmen dienen: Nach Implementierung der IT-Lösung sind die Abläufe und Strukturen der Unternehmen in sehr vielen Fällen identisch und den Vorgaben der Software angepasst, da die Anpassung der IT-Lösung auf die Unternehmensstrukturen und –abläufe unverhältnismäßig hohe Kosten verursacht hätten. Im öffentlichen Bereich wäre es nicht anders: Würde eine IT-Lösung zentral entwickelt bzw. die Konzeption vorgegeben, dann wäre entweder der Abstimmungsprozess derartig langwierig, dass die Lösung bei Fertigstellung veraltet wäre, oder es entstünde eine Lösung, die aus rein wirtschaftlichen Gründen die Nutzer zwingen würde, ihre Verwaltungsabläufe der IT-Lösung anzupassen.

**Beide Wege führen damit nicht zum Ziel, durch Nutzung der IT die Verwaltung effizienter zu gestalten:**

Im ersten Fall steht eine Lösung nicht oder nur sehr spät zur Verfügung. Im zweiten Fall bestimmt die IT-Lösung den Verwaltungsaufbau und –ablauf und nimmt faktisch über die finanziellen Zwänge den Ländern und Kommunen ihre Kompetenz zur Ausgestaltung der Verwaltungsverfahren. Bestünde dann noch eine Kompetenz des Bundes zur Steuerung im Bereich der IT-Nutzung in der Verwaltung, dann würde aufgrund der dargestellten faktischen Auswirkungen das austarierte und im Rahmen der Föderalismusreform I neu justierte System der grundgesetzlichen Kompetenzverteilung konterkariert.

## **A Zur Abgrenzung von "Aufgabe" und "IT bzw. IT-Systemen"**

### ***I. Eigenheiten von IT-Projekten***

Im Hinblick auf die Zentralisierbarkeit bei der Beschaffung, insbesondere aber auch im Hinblick auf die Aufgaben-Nähe bzw. –Abhängigkeit können schematisch folgende Gegenstände, die zusammen wiederum ein System bilden (können), differenziert werden:

- 1.) Planung (Beratung) Gewinnung von „Pflichtenheften“, Spezifikationen bzw. Unterstützung hierbei
- 2.) Hardware, Netz
- 3.) Wartung von Hardware und Netz-Komponenten
- 4.) Software
  - 4.a) Standardsoftware
  - 4.b) Anpassung von Software
  - 4.c) Erstellung von Software
5. Pflege der Software
6. Services (Roll Out, Installation, Einweisung ..)
7. Outsourcing/Providing, etwa
  - 7.1 Host
  - 7.2 Access
  - 7.3 Content
  - 7.4 usw., u. a. auch Domain-bezogene Services
  - 7.5. ASP, Rechenzentrums-Betrieb, fällt auch unter Outsourcing

Im Hinblick auf die Begriffe wie Kompatibilität und Interoperabilität empfiehlt es sich, neben Hardware und Software als weitere Ebene auch noch Regelungen zu den „Daten“ (im Sinne von Datawarehouse u.ä.) aufzunehmen. Dies ist v.a. gerade wegen der Möglichkeiten des Outsourcing, z. B. auch ASP, vorzusehen.

Die Föderalismusreform I hatte zum Ziel, die Handlungs- und Entscheidungsfähigkeit von Bund und Ländern zu verbessern (und die politischen Verantwortlichkeiten deutlicher zuzuordnen). Die Zentralisierung der IT hebt praktisch dieses Ergebnis auf. Statt der Zentralisierung bzw. Rückführung auf den Bund müssen deshalb Organisationsformen gewählt werden, die diesem Ziel entsprechen und die zu erhöhter Flexibilität und zugleich auch zu verbesserter Nutzung der technischen Entwicklung führen (können).

Der Regelungsbedarf, wenn überhaupt einer besteht, betrifft deshalb die Gestaltung von Kooperationsformen sowohl zwischen den Ländern als auch zwischen Ländern und Bund.

In Verbindung mit der Stärkung der Eigenverantwortlichkeit wird es sich empfehlen, nach Aufgabennähe zu unterscheiden, wenn es um die Frage geht, inwieweit gemeinschaftlich bzw. zentral die einzelnen IT-/TK-Komponenten zusammengeführt und angeboten werden (z. B. in einer Netzwerkstruktur bzw. von einem Rechenzentrum aus). Dabei müsste sich zeigen, dass die Hardware mit dem Betriebssystem und den Datenbanken als Standardsoftware, die nicht Aufgaben-spezifisch sind, ei-



gentlich sehr weit entfernt von der einzelnen Aufgabe sind, während schon die genaue Einstellung der Datenbank, zum Teil auch der Roll out, besonders aber die Einstellungen, die für die Anwendung erforderlich sind (z. B. beim Dokumenten-Management-System) sehr aufgabennah sind.

Infolgedessen werden sich **Kooperationsformen empfehlen**, bei denen die Auftraggeber-Eigenschaft der einzelnen Behörde bzw. des einzelnen Landes erhalten bleibt, wobei dies zugleich durch eine verstärkte Zusammenarbeit der Länder ökonomischer ausgestaltet werden kann.

**Ohne grundgesetzliche Verankerung ist eine Intensivierung und Strukturierung mit Standardisierung (auch der Abläufe der Zusammenarbeit) der Kooperation zwischen den Ländern durch Verträge gestaltbar. Die Frage ist, ob zusätzlich eine Grundlage für Verfahren mit Mehrheitsentscheidungen geschaffen werden soll und kann. Für Projekte wäre diese Grundlage noch nicht erforderlich. Für die Verpflichtung zum Einsatz der Ergebnisse des Projekts in allen Ländern besteht der Bedarf an Rechtsgrundlage. Vorzugswürdig erscheint aber der Weg, möglichst gemeinsam (auf Vertragsebene) Standards und Standardlösungen zu (be-)schaffen und die im übrigen notwendigen Anpassungen jedem Land (Software und/Oder Organisation) zu überlassen (einschließlich der Kostentragung).**

## **1. Eigenheit von Projekten: Änderungen im Projektverlauf**

Es gibt einige in der Praxis immer wieder auftretende "Gesetzmäßigkeiten", also typische Eigenheiten von Projekten und auch IT-Systemen, die man kaum ändern kann. Es wird zwar seit Jahren, wenn nicht Jahrzehnten versucht, diese Eigenheiten in den Griff zu bekommen. Dies gelingt jedoch nur, wie zahlreiche scheiternde Projekte belegen, in Grenzen.

Eines der Hauptprobleme ist, ein komplexes Projekt über längere Zeit bei sich verändernden Umgebungsbedingungen erfolgreich durchzuführen.

Im IT-Bereich ändert sich die Technologie in sehr hoher Frequenz. Das bedeutet, dass man etwa bei einer bestimmten Hardware-Orientierung bei einem Projekt zu Projektbeginn von einer anderen Hardware ausgeht, als sie angeboten wird, wenn das Projekt "fertig" ist. Anders gesagt: Die Hardware ist bereits zum Projektende veraltet.

Während der Projektlaufzeit ändert sich aber nicht nur die Hardware, sondern die darauf ablaufenden Betriebssysteme und auch Datenbank- u.ä. Standardprogramme, da sie ständiger Aktualisierung und Fortschreibung unterworfen sind.

Schließlich ändern sich während der Laufzeit auch die Anforderungen bzw. die den Anforderungen zugrunde liegenden Bedingungen. Letzteres lässt sich einigermaßen über Änderungsklauseln in Verträgen berücksichtigen. Die daraus resultierende Wirkung, längere Dauer des Projekts, Änderung der Technik usw. lassen sich praktisch aber nicht vermeiden.

Eine der Eigengesetzlichkeiten bei Software bei der Kombination von Standardsoftware und Pflege ist, dass in der Regel die Pflegeverträge mit ihren Updates und der Mängelbeseitigung nur den Standard umfassen, so dass, wenn die Anpassungen nicht releasefest sind, in der Regel noch Nacharbeiten bei dem Einpflegen von Updates erforderlich werden. Das bedeutet, dass zentral beschaffte Software, die dann bei den einzelnen Anwendern doch unterschiedlich ausgestaltet wird (im Wege der Anpassung) erhebliche Folgekosten nach sich ziehen kann.

Die zentrale Beschaffung von Software als solcher kann u. U. erheblich preiswerter gestaltet werden (Ausschreibungs- bzw. kartellrechtliche Probleme als gelöst vorausgesetzt). Es ist aber bei evtl. Kostenerhebungen auch zu berücksichtigen, dass sehr viele Anbieter bei der Vergütung darauf abstellen, wie viele zugelassene User der einzelne Anwender hat. An der Zahl der User ändert sich aber bei zentraler Beschaffung nichts. Allerdings kann dieser Einsparungseffekt dann erzielt werden, wenn „Pakete“ erworben werden, die pro Einzel-Lizenz umso preiswerter werden, je größer das „Paket“ ist. In diese Richtung gehen die Microsoft-Rahmenverträge.

Die derzeitige Rechtslage führt im Übrigen zivilrechtlich dazu, dass das „Abgeben“ ebenso wie auch das Nutzen-Lassen von Software durch andere Stellen als die, die die Software beschafft haben, erhebliche Probleme aufwirft. Besonders bekannt geworden sind in diesem Zusammenhang die Entscheidungen des LG München I und OLG München zu „Gebrauchsoftware“.

Eine weitere Faustformel besagt, dass – zumindest in späten Phasen der Projekte diese nicht dadurch beschleunigt werden, dass mehr Leute daran arbeiten.

Daraus ergibt sich als **Folgerung**: Dezentral aufgesetzte Projekte, die sich im Sinne der Interoperabilität an gemeinsam vereinbarten (Austausch)-Standards orientieren, dienen der schnellen Bereitstellung einer Lösung und lassen sich optimal auf die Rahmenbedingungen des jeweiligen Nutzers anpassen. Die Anpassung ist auch notwendig, da der Nutzer (Land/Kommune) aufgrund eigener Kompetenz die Entscheidungen zu Art und Ausgestaltung der Umsetzung einer Verwaltungsaufgabe trifft.

## 2. Differenzierung Planung und Realisierung

Wie auch immer das Vorgehensmodell genau beschaffen ist, so lässt sich eine ganz grobe Zweiteilung als generell gerade im Hinblick auf die Differenzierung von Aufgabe und deren Automatisierung vornehmen, nämlich in

- Planung und
- Realisierung.

Ähnlich den Vorgaben der BVB/EVB-IT müsste am Ende des Planungsprozesses eine Spezifikation stehen, die in der BGH-Rechtsprechung "Pflichtenheft" genannt wird und - anders als die Definition in den DIN jedoch- eine fachliche Spezifikation meint, die evtl. auch eine fachliche Feinspezifikation ist, sogar sein sollte. Erst aufgrund einer solchen fachlichen Feinspezifikation lässt sich normalerweise eine Realisierung eines Projekts in Auftrag geben. "Normalerweise" heißt, ohne einen ver-

traglichen oder projektmäßigen Fehler zu machen. Dass die Rechtsprechung diese Fehler ausbügelt und z.B. bei Fehlen eines Pflichtenhefts einen *mittleren Ausführungsstandard* gelten lässt, verbessert das Problem nicht. Mit einem mittleren Ausführungsstandard ist der auftraggebende Anwender im Zweifel nicht zufrieden.

Es ist also praktisch unabweisbar, für die Automatisierung einer Aufgabe zunächst eine fachliche Spezifikation zu erstellen, was durchaus Monate, wenn nicht Jahre dauern kann. Für die Zeit gelten die Restriktionen bzw. die Merkmale, wie oben kurz skizziert.

Der jeweilige Anwender mit seinem Fachwissen muss seine rechtlichen Rahmenbedingungen, die umzusetzenden Abläufe und die fachlichen Anforderungen selbst artikulieren, wobei ihn ein Berater unterstützen kann. Aber beurteilen, ob die Ausgestaltung als „Spezifikation“ seinen Anforderungen entspricht, muss der Anwender selbst.

### 3. Anstieg der Änderungsrate in Abhängigkeit von der Dauer des Projekts

Es gilt eine weitere Gesetzmäßigkeit, die sich indirekt bereits aus dem Gesagten ergibt, dass nämlich Änderungen einen um so größeren Aufwand erzeugen, je später der Zeitpunkt bzw. der Projektschritt ist, zu dem sie Einfluss nehmen. Wird also etwa kurz vor der endgültigen Freigabe eines Programms festgestellt, dass noch etwas zu ändern ist, z.B. weil einfach ein Fehler enthalten ist, dann erzeugt das einen 10- bis 25-fachen (genaue Zahlen liegen wohl nicht vor) Aufwand, jedenfalls einen unvergleichlich viel höheren Aufwand, als wenn dies in der Grobkonzeption bzw. bei der Feinspezifikation bereits oder zu Beginn der Realisierung bei der technischen Spezifikation erkannt worden wäre.

Daraus hat man in Juristenkreisen sinngemäß folgenden etwas boshaften Schluss erzeugt, an dem aber viel Wahres dran ist, wie die Erfahrung zeigt: *„Wenn die Techniker des IT-Projekts sagen, dass sie etwa 95 % der Aufgabenstellung geschafft haben, kann man annehmen, dass das Projekt in etwa noch genauso lange weiter dauert, wie bisher“.*

Natürlich stimmen diese Zahlen nicht bzw. sind unterschiedlich je nach dem, ob eine bestimmte (service-orientierte) Technik der Systemarchitektur, die entsprechend flexibel ist, zugrunde liegt, ob eine gute Dokumentation geschaffen worden ist, ob strukturiert vorgegangen wurde usw.

Jedenfalls steht fest, dass im Laufe der Jahre sich die Relationen zwischen Planungszeitraum und Realisierung enorm zugunsten des Planungszeitraums verschoben haben. D.h. also, dass der Umfang des Planungszeitraums einen unvergleichlich höheren Aufwand inzwischen verdient und auch erhält, als früher und demgegenüber im Projekt selbst relativ gesehen der Realisierungsaufwand eher geringer wird.

Als **Folgerung** heißt das auch hier: Lieber kleinere, landes- oder kommunalbezogene Projekte nach einheitlichen Standards als große, länderübergreifende Projekte,

die sämtliche Besonderheiten aller Beteiligten einbeziehen und abstimmen wollen/müssen.

#### **4. Dauer von Projekten**

Wirtschaftlich im Sinne von kalkulierbar, termintreu und effektiv sind kleinere und mittlere Projekte.

Mit der Dauer des Projektes steigt das Risiko dessen Scheiterns (wahrscheinlich) überproportional. Dies hängt damit zusammen, dass zwei Strömungen während der Laufzeit des Projekts immer zu berücksichtigen sind bzw. drohen:

- a) Zum einen ändert sich der Anwender mit seiner Organisation und auch subjektiv mit seinen Wünschen, ausgedrückt meist in sogenannten CR, Change Request. Je länger das Projekt dauert, umso größer der Druck, solche CR zu realisieren. Um die Dauer der Projekte zu verkürzen, wird zudem zu dem Mittel gegriffen, keine Feinspezifikation zu erstellen (die zudem im Rahmen einer Ausschreibung dem Ergebnis zu weit vorgreifen bzw. dieses zu sehr einengen würde), so dass als eine der ersten Aufgaben der Auftragnehmer diese Feinspezifikation nachzuholen hat. In diesem Zusammenhang stellen sich eine Fülle von zusätzlichen Fragen im Hinblick auf die Konkretisierung, ob es sich also wirklich nur um Konkretisierungen oder schon um Änderungen, meist in Form der Erweiterungen, handelt.
- b) Zum anderen ändert sich die Umwelt bzw. ändern sich die Umwelтанforderungen an das Projekt während der Laufzeit, etwa in Form neuer gesetzlicher Regelungen einschließlich Verordnungen und Durchführungsbestimmungen, aber auch sonstigen Anforderungen, wie sie etwa sich durch Änderungen bei den Betroffenen (Bürgern) und deren Verhältnissen ergeben. Von daher empfiehlt es sich grundsätzlich Projekte überschaubar zu gestalten, ihre Beendigungssicherheit zu erhöhen und möglichst wenig Änderungen schon während des Projekts zuzulassen bzw. dulden zu müssen. Dies spricht gegen zwangsläufig länger dauernde, weil größere Projekte zentraler Verwaltung.

#### **5. Änderungsrate und Projektdauer**

Die Wahrscheinlichkeit von Änderungsforderungen, die sogar untereinander divergieren, steigt bei komplexen, großen Projekten, insbesondere also für zentrale Systeme, die eine Vielzahl der beteiligten Anwender versorgen. Entsprechend steigt der Aufwand bei den Nacharbeiten und den individuellen Anpassungen beim Anwender. Umso länger dauert das Projekt bis zur Einführungsreife.

#### **6. Zwischenergebnis**

Ein Rückschluss bzw. eine Rückwirkung von der IT-Lösung auf die Aufgabe würde erfolgen, wenn man ohne fachliche Feinspezifikation die Umsetzung rein nach technischen Notwendigkeiten und Möglichkeiten realisiert. Eine Zentralisierung der IT als ein ordnungsgemäßes, projektmäßiges Vorgehen erhöht den Bedarf an Abstimmung

der fachlichen Forderungen oder nivelliert diese über einen einheitlichen Ausführungsstandard, der technisch orientiert wäre und die spezifischen, insbesondere kompetenz- und organisationsrechtlichen Anwenderforderungen nicht erfüllen würde.

Wenn man für die fachlichen Vorgaben und deren Gestaltung bereits die technischen Vorbedingungen festlegt, ist auch über fachlichen Vorgaben und die Organisationsstruktur der Aufgabenerfüllung mit entschieden.

Im öffentlichen Bereich resultieren die fachlichen Vorgaben aus der Kompetenzordnung des Grundgesetzes, den Gesetzen und Verordnungen. Wenn man die IT deshalb vordefiniert und in der Realisierung der Spezifikation, die aus der Kompetenzordnung und den rechtlichen Vorgaben zur Aufgabenerfüllung heraus abzuleiten wäre, vorgeht, gestaltet man praktisch das Gesetz und lässt die eigentliche Kompetenz des für die Umsetzung des Rechts Verantwortlichen leer laufen.

## **II. Verantwortlichkeit und „Stelle“ - Vorgaben des Datenschutzes**

Der gemeinsame Betrieb von Rechenzentren ist Datenschutz-konform gestaltbar. Die gemeinsamen Lösungen im Rahmen einer einheitlichen Anwendung bereiten erhebliche Probleme.

Es gibt eine Vielzahl von Formen der Zusammenarbeit, die bereits, wenn auch in den einzelnen Bundesländern und im Bund unterschiedlich, gehandhabt werden.

Einige strukturelle Vorgaben stehen jedoch einer allzu starken Verquickung der verschiedensten Bereiche entgegen. Deren Grundlage sollte nicht aufgegeben werden

Eine dieser Vorgaben ist die „**Verantwortlichkeit**“.

Die Abschottung unterschiedlicher Aufgaben und Stellen ist ein Gebot des Datenschutzes und zwar sowohl gemäß der EU-Richtlinie als auch des BDSG.

Nach § 2 Abs. 2 BDSG gehören zu den öffentlichen Stellen der Länder die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstige der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Es gibt also einen spezifischen datenschutzrechtlichen Stellen-Begriff. Diese ist zentral für das Verständnis der Mechanik, des Datenschutzes, auf die verschiedenen Phasen aufzubauen und dabei hinsichtlich der Zulässigkeit u.a. und v.a. auf die Zulässigkeit der Übermittlung.

Die einzelnen Landesdatenschutzgesetze haben dementsprechend für die Begrifflichkeit gesorgt, dass nach einzelner Behörde zu unterscheiden ist bzw. jede einzelne Behörde als verantwortlicher Stelle zu sehen ist, die auch ihren eigenen Datenschutzbeauftragten stellt. Die Regelungen sind in Details je Bundesland etwas unterschiedlich. Die Regelung des Anwendungsbereichs des BDSG stützt sich in § 1 Abs.

2 BDSG ebenfalls auf die Differenzierung öffentlicher Stellen sowohl des Bundes als auch der Länder.

In der Folge geht es u. a. bei den Zulässigkeits-Regelungen jeweils um die Aufgaben und zwar der in der Zuständigkeit der verantwortlichen Stelle.

Diese Begrifflichkeit ist Tradition im deutschen Datenschutz. Sie wurde auch nicht etwa geändert, nachdem die EU-Datenschutz-Richtlinie (vom 20. Oktober 1995) umzusetzen war. Bei der Gestaltung und Auslegung des Datenschutzes ist jedoch auf die Einhaltung dieser Richtlinie zu achten. Art. 2d) definiert „für die Verarbeitung Verantwortlicher“: *die natürliche oder juristische Person, Behörde, Einrichtung oder jeder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.*“

Gemäß EU-Datenschutz-Richtlinie ist jede Stelle einzeln sowohl hinsichtlich der Zweckbestimmung als auch hinsichtlich der Verantwortlichkeit und schließlich auch der Privilegierung zu sehen.

Die Konsequenz ist, dass sehr sorgfältig darauf zu achten ist, dass bei Outsourcing bzw. Service-Rechenzentren die Verantwortlichkeit der Stelle und damit die Datenhoheit unverändert bleiben, keine Funktions- Übertragung erfolgt. Dies muss auch gegenüber Amtshilfe gelten.

Auch bei **Auftragsdatenverarbeitung** bleibt der Auftraggeber vollverantwortlich, was die Zulässigkeit und Sicherheit der Verarbeitung betrifft.

**Der EU-Gesetzgeber hat also entschieden, dass bei einer Abwägung der Ziele die Privatsphäre bzw. der Datenschutz weit vor der Rationalisierung der Datenverarbeitung bzw. weit vor der Effektivität rangieren.**

Dies ändert sich wieder bei spezialgesetzlichen Ausnahmen für höherrangige Rechtsgüter wie etwa Terrorismusbekämpfung, Steuergerechtigkeit o.ä..

### **III. „IT-Sicherheit“**

Eines der zentralen Themen derzeit und in absehbarer Zeit ist das Thema IT-Sicherheit bzw. Sicherheit der gesamten IT-Struktur. Es ist wohl nahezu unausweichlich und auch sinnvoll, dass **das Thema „Sicherheit“ in seinen Grundsatzfragen zentral bearbeitet, also erforscht wird** und dazu auch zentral Ansätze, Konzepte, Prinzipien (s. etwa „Grundschutz und dessen Kriterien beim BSI) sowie ggf. auch Werkzeuge entwickelt werden. Als technische Standards können diese Sicherheitsempfehlungen auch gemeinsam akzeptiert und zur Anwendung empfohlen werden. Ggf. wäre es sogar möglich, dass sich die Nutzer von IT-Verfahren und zusammenschalteten Datennetzen auf einzuhaltende Mindeststandards auch im Bereich der IT-Sicherheit verständigen.

Andererseits ist es ebenso wichtig und richtig, dass diese Lösungen **dezentral realisiert** werden müssen. Insofern kann das BSI als Modell für die richtige Lösung die-

nen. Dessen Einrichtung ändert nichts an der Eigenverantwortlichkeit im Hinblick auf die Sicherheit, wie sie sich letztlich auch aus der insgesamt IT-Compliance als Maßgabe zur Forderung und speziell aus dem Datenschutz ergibt (§ 9 BDSG), womit nämlich jede einzelne Stelle adressiert ist.

In diesem Zusammenhang ist eines der wichtigen Stichworte die Zentralisierung. Es wird dafür plädiert, zwar eine zentrale Institution zu schaffen, die die wichtigsten Themen zentral erforscht und erarbeitet, gleichzeitig aber eine dezentrale Anwendung- bzw. Lösungsstruktur – ggf. auch mittels unterschiedlicher Produkte und Techniken - zu schaffen. Hintergrund hierfür ist v.a. die **wesentlich höhere Angreifbarkeit von zentralen Systemen.**

Unter diesem Aspekt ist auch die derzeitige Internet-Grundlage wesentlich zu zentral, wie sich immer wieder, wenn Attacken bzw. Notlagen stattfinden, zeigt. Es treten dann Engpässe auf. Im Sinne einer nationalen und europäischen Sicherheit wäre es aber wünschenswert, wozu es ja auch schon Bestrebungen gibt, die Redundanz wesentlich zu erhöhen, was mit Zentralisierung schwer erreichbar ist, vor allem, wenn es um die Verringerung der Auswirkungen bei evtl. erfolgreichen Attacken geht.

Es gab Bestrebungen, eine Art virtuellen Rotlichtbezirk bei den Domains durch Schaffung einer einheitlichen Domain entstehen zu lassen. Als man dieser Idee näher trat, schaltete sich ein beratender Regierungsausschuss des ICANN Governmental Advisory Committee – GAC ein. Im Zusammenhang mit diesem Streit kam es dann dazu, dass z.B. das US-Heimatschutz-Ministerium Ansprüche anmeldete, „Alleinverwalter des Masterschlüssels für die neue Sicherheitssoftware DNSSec für den Internetroot zu werden“. Hiermit sollte gewährleistet sein „Sicherheit und Stabilität einer für US-Wirtschaft und Politik kritischen Infrastruktur“. Es ist also durchaus denkbar, dass immer zunehmender politischer Druck auf „das Internet“ schließlich zu einer Re-Nationalisierung führt, dem sich Europa zwingend pro aktiv stellen müsste, dabei ist keineswegs gewährleistet, dass bei ICANN bzw. IAN (Internet Assigned Numbers Authority) Europa genügend Mitsprache hat, da es sich in keiner Weise um ein demokratisch bzw. rechtlich abgesichertes Gremium handelt. Würde also eine Netzwerkbildung neuerer Art bzw. verwaltungsspezifischer Art gefordert und gefördert, so sollte sie zwar voll „internetfähig“, jedoch dann auch funktionsfähig sein, wenn die bisherigen Institutionen nicht so funktionieren bzw. nationale Alleingänge entstehen.

Auch die zahlreichen Meldungen über die Ausspähungen von Lücken bei sehr weit verbreiteten Systemen also naturgemäß insbesondere bei Microsoft zeigen, dass mit völliger Monostruktur die Angreifbarkeit eher höher ist. Bedenkt man noch, dass strukturell der gleiche Effekt, wie etwa für den Bundestrojaner diskutiert wird, längst schon Praxis der Angreifer ist, so vergrößert sich deren Schadenspotential mit der produktmäßigen und strukturellen Monokultur. Produkte von Microsoft und etwa auch HP haben sich Presse-Meldungen zufolge bei geeigneter Online-Konstellation jeweils beim Hersteller „zurückgemeldet“, ohne dass dies der Anwender merkte bzw. erfuhr.

Ein möglicherweise typisches Beispiel für die Angreifbarkeit bei zentralen Systemen wäre die so genannte Jahr-2000-Fähigkeit. Möglicherweise hat der Schaden seinerzeit nur deshalb sich nicht wie befürchtet entwickelt, weil die Anwendungen doch sehr verschieden ausgestaltet und ausgestattet waren.

Bei (kritischen) Infrastrukturbereichen wurde bislang weniger darauf geachtet, wie das Verhältnis von Versorgungsauftrag zu dem Staat ist, Bedrohungen, die von dieser Infrastruktur ausgehen bzw. die bei deren Ausfall bedrohen, abzuwägen und auszugleichen. Im „Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen“, 15.11.2002, in Teilen überarbeitet 05. Mai 2005, BSI (vorgelegt vom Konsortium *Holzner/König* unter Mitarbeit von *Alexander Koch* und *Christian Schulz*) wird unter „geltendem Recht“ ausdrücklich darauf hingewiesen, dass es zweifelhaft sein mag, „*inwieweit von dieser grundsätzlichen Infrastruktur-Gewährleistungspflicht auch eine Verpflichtung zur Sicherung der Infrastrukturen gegen Angriffe erfasst ist*“ (Seite 7). Sie meinen, dass den Grundrechten zwar primär eine Abwehrfunktion gegen staatliche Eingriffe zukommt, aber darüber hinaus diese auch den Staat verpflichten, „*die grundrechtlich geschützten Güter vor Eingriffen Dritter zu schützen*“.

Man wird also zwischen der Gewährleistung der Grundversorgung einerseits und der Gewährleistung des Schutzes vor Auswirkungen der Infrastruktur, die diese Grundversorgung sicherstellt, unterscheiden, andererseits diese aber auch ins Verhältnis bringen müssen.

Das Bundesverfassungsgericht hat mehrfach darüber zu entscheiden gehabt, ob und inwieweit bestimmte Methoden der Erfassung des Einzelnen, dessen Bewegungen und Einstellungen verfassungsmäßig sind, insbesondere im Zusammenhang mit der Überwachung bzw. Strafverfolgung. Dabei hat im Hinblick auf die Zulässigkeit, die noch gegeben war, etwa was ein Ortungsgerät betraf, eine Rolle gespielt, dass es sich um keine Totalerfassung handelt. Eine Forderung nach einer einheitlichen Telekommunikations- bzw. IT-Infrastruktur – was auch immer dies dann ganz genau sei – müsste also gleichzeitig daraufhin überprüft werden, ob sie etwa eine Totalerfassung ermöglicht. Selbst wenn eine solche Totalerfassung im Hinblick auf einzelne Personen unter Berücksichtigung überragender Rechtsgüter, zu deren Schutz die Überwachung erfolgt, zulässig sein mag, also aufgrund spezial-gesetzlicher Erhebung, so unzulässig wäre eine pauschale, totale Abbildung des Einzelnen oder die vollständige Erfassung seiner Bewegungen. Äußerungen und Datenspuren.

Wie weiter ausgeführt hat der Bundesgesetzgeber diese strukturellen Vorgaben nicht einfach in seiner Kompetenz, da das Datenschutzrecht insoweit EU-Richtlinien folgt und folgen muss. Insoweit ist speziell für die Telekommunikation auch die hierfür spezielle TK-Datenschutzrichtlinie zu berücksichtigen, dabei ist das Interessante, dass diese TK-Datenschutzrichtlinie den Schutz des Einzelnen und damit die Gewährleistung der Sicherheit für diesen im Auge hat, während die Sicherheit derjenigen, die sich als Anwender dieser Infrastruktur bedienen, nicht Schutzgegenstand ist. Aufgrund der geringen präventiven Wirkung von Strafnormen dürfte es unbedingt erforderlich sein, die Sicherheits-Vorschriften für TK-Netze und –Anwendungen nicht nur zum Schutze des Betroffenen, sondern auch der Allgemeinheit bzw. des Staates und der Anwender zu stärken (wie zahlreiche Beispiele ungeschützter WLAN belegen).

Daraus **folgt**: Dezentral verantwortete und gesteuerte Netze und Anwendungen sind bei Zugrundlegung eines einheitlichen Sicherheitsniveaus vorzuziehen, da dabei die Angreifbarkeit und Verwundbarkeit geringer ist.



Zudem ist die – vom Bund wohl geforderte – Kompetenz im Bereich der Sicherheit der Datennetze abzulehnen, da dann für eine denkbare Totalüberwachung – jedenfalls bei vollständiger Ausweitung auf alle Netze – die verfassungsrechtliche Rechtfertigung sehr fraglich wäre.

#### **IV. (Service orientierte) Architektur(SOA): IT-Netzinfrastruktur**

SOA kann als Beispiel für die effiziente Möglichkeit der Nutzung von dezentralen Systemen dienen, die über standardisierte Schnittstellen zusammenwirken.

#### **V. Kompatibilität, Interoperabilität**

Kompatibilität wird bezogen auf

- Daten
- Programme
- Hardware.

Sie ist mehr oder weniger intuitiv, nicht identisch mit Interoperabilität. Interoperabilität ist ein Begriff aus der Technik, der Eingang ins Urheberrecht genommen hat.

Das Interessante bzw. Besondere ist, dass der Anwender berechtigt ist, auch ohne dass ihm vom „Lizenzgeber“ die dazu erforderlichen Rechte explizit eingeräumt werden, die Interoperabilität des ihm überlassenen Programms mit einem anderen Programm bei ihm herzustellen. Dieses Recht gilt nicht für den Marktteilnehmer, dieser darf aber den Kunden dabei unterstützen bzw. im Auftrag für ihn diese Arbeit vornehmen. Dieses Recht gilt auch, wenn es bereits eine Schnittstelle oder Schnittstellen gibt.

§ 69e UrhG spricht in diesem Zusammenhang in der Überschrift allerdings nicht von Interoperabilität, sondern von *Dekompilierung*. Die Dekompilierung ist bei § 69 e UrhG das Mittel, um die erforderlichen Informationen zur Herstellung der Interoperabilität eines unabhängig geschaffenen Computerprogramms mit anderen Programmen zu erhalten.

Will man, wofür manches spricht, keine reine Monokultur eines einzelnen Software-Anbieters (dessen Programme eher in sich kompatibel bzw. interoperabel sind), so wäre das Mittel der Wahl, als Auftraggeber die Schnittstellen vorzugeben, und gleichzeitig damit die Interoperabilität in der gewünschten Weise sicherzustellen.

Diese Interoperabilität, verbunden auch mit der v.a. Daten-Kompatibilität als Forderung des Kunden, lässt sich im Wege einer entsprechenden Gestaltung der Beschaffung zentral unterstützen, kann dezentral ausgeübt werden.

**Es kommt also auf folgende Feststellung an:**

Notwendig ist **Interoperabilität der Anwendungen**. Diese kann durch Vorgabe von Produkten, die zentrale Entwicklung und Bereitstellung von Produkten, v.a. aber –

vorzugswürdig – durch die Einigung auf Austauschstandards und –prozesse erfolgen. Danach ist dann eine Einzelentwicklung / -entscheidung, aber auch eine Lösungserstellung gemeinsam, in Gruppen oder jeder für sich möglich. Dabei ist aber die „gleiche Sprache“ zugrunde gelegt.

## **B. Einzelne Fragen**

### **Frage 121**

Die Zusammenfassung, die Ausführungen in A und in den folgenden Antworten sprechen sich für eine intensiviertere Zusammenarbeit der Länder aus. Diese fördert den Ideenwettbewerb v.a., wo keine Anschlusszwänge geschaffen werden. Dies wird auch für die Steuerverwaltung gelten.

### **Frage 233**

Soweit ein echtes Nebeneinander von Anwendungen existiert, wird es lohnend sein, deren Übereinstimmung zu prüfen und Mittel zu schaffen, die weitere Übereinstimmungen erzielen helfen, soweit die Geschäftsprozesse dies zulassen..

Der Betrieb auf einigen wenigen „Plattformen“ kann kostengünstig sein. Die Flexibilität einerseits muss erhalten bleiben, der Koordinierungsaufwand darf nicht überproportional steigen. Bei FISCUS handelte es sich um ein Projekt, das eher als Beispiel dafür herhalten kann, welche Schwierigkeiten auftreten, wenn ein völlig einheitliches System für alle geschaffen werden soll. Beispiele, die im Sinne des „Ideenwettbewerbs“, s. Frage 121, gelten können, sind etwa diejenigen, wo ein Großteil der Bundesländer sich für die eine, ein anderer Teil für die andere Lösung entschieden hat, wie dies etwa im Bereich des Grundbuchs der Fall war.

Eine einheitliche Lösung für alle Länder über ein Großprojekt zu erzielen, scheint auf Grund der bereits unter A. dargestellten Implikationen kaum zielführend. Sinnvoll wird sein, den gemeinsam einzusetzenden Standard zu ermitteln, diesen ggf. gemeinsam (bzw. über einen Federführer) entwickeln zu lassen oder auch nur, diesen als den zu verwendenden Standard festzulegen und dann im Rahmen von kleineren / mittleren Projekten, die überschaubar bleiben, die jeweils erforderliche IT-Lösung unter Beachtung des vereinbarten Standards entwickeln zu lassen.

Die Vorschläge würden auch echtes Nebeneinander zügig erkennen und nach genauerer Prüfung der Übereinstimmungen dieses abbauen helfen. Es würden wettbewerbsfähige „Standard-Produkte“ entstehen, für deren Durchsetzung die Kostenzuordnung für Änderungsaufwand als Marktmechanismus sorgt.

### **Frage 251**

Es gibt erhebliches Potential für eine effizientere und kostengünstigere Verwaltungszusammenarbeit deutscher Behörden durch Informationstechnik. Dabei ist zwischen den Projekten im Sinne der Gewinnung der Aufgabenlösung und dem Betrieb zu unterschei-

den. Im Hinblick auf die Projektrisiken und die Effizienz der Durchführung der Projekte erscheint das Potential dann besonders groß, wenn es gelingt, Formen der Zusammenarbeit zu schaffen, die hinsichtlich eines verbleibenden „Rests“, oben mit etwa 10 bis 15 % angeben, individuelle Ausgestaltungen ermöglichen.

Hinsichtlich des Betriebs erscheinen die Potentiale wesentlich größer, weil die Rationalisierungseffekte hinsichtlich Hardware, Betriebssystem, Datenbanken, deren kostengünstiger Beschaffung, Betrieb und Pflege im Verbund großer Rechenzentren kostengünstiger erfolgen kann. Dies gilt auch für den Betrieb von Kommunikationsnetzen.

Im Extremfall wird die Zusammenarbeit der Verwaltungen durch das Fehlen medienbruchfreier Kommunikation behindert. Aber selbst bei der Nutzung von IT-Lösungen kann es in Einzelfällen dazu kommen, dass wegen fehlender abgestimmter Austauschformate Probleme auftreten.

Als ein besonders erfolgreiches Beispiel für eine Steigerung der Effizienz lässt sich die erfolgreiche Verabredung des XML-Datenaustauschformats (X-meld) durch die Länder für die elektronische Rückmeldung eines Umzugs von der Zuzugsgemeinde an die Wegzugsgemeinde aufführen, was bereits in kurzer Zeit zu spürbaren Einsparungen und Prozessbeschleunigungen geführt hat.

## Frage 252

Sich **Steuerungsmechanismen** hinsichtlich des IT-Einsatzes vorzustellen, kann sich eigentlich nur auf die Ebenen Hardware, Hardwarebeschaffung, Betriebssysteme, ggf. Datenbanken beziehen. Des Weiteren ließe sich dies auf die Schaffung von Tools für Sicherheit und für projektmäßiges Vorgehen, also zur Unterstützung der jeweiligen Anwendungen und deren Schaffung beziehen. Ansätze hierzu gäbe es, - relativ weit entwickelt - für die Sicherheit im Rahmen von BSI, für das Vorgehen etwa das V-Modell und insoweit die Einrichtung KBST.

Im Hinblick auf das unter I. Gesagte wäre eine weitere "Steuerung" praktisch eine Beeinflussung der Aufgabe und der Aufgabenstellung.

Neben der praktischen Steuerung des IT-Einsatzes in den Verwaltungen bestehen die Abstimmungsgremien auf Länderebene und im Verhältnis Bund-Länder. Hier findet sich eine Vielzahl von Gremien, die fachbezogen und damit vielfach unabgestimmt Fragen des IT-Einsatzes in der Verwaltung behandeln. Dies kann dazu führen, dass Parallelentwicklungen angestoßen werden, aber es können auch zueinander konträre Lösungen angegangen werden. Ebenso werden Ressourcen dadurch gebunden, dass eine Vielzahl von Gremien beschickt werden muss und Fachfragen – teils nur um Facetten geändert – mehrfach diskutiert werden.

**Zusammenfassend ist festzuhalten**, dass im Hinblick auf die Sicherstellung der Interoperabilität und die Vereinbarung gemeinsamer technischer Standards die derzeitige Gremienstruktur suboptimal ist.

**Wünschenswert** wäre es, wenn ein von den Ländern als den Hauptverantwortlichen für den Verwaltungsvollzug ein Gremium eingerichtet würde, in dem Fragen der für den ebe-

nen- und länderübergreifenden Datenaustausch notwendigen Standardisierungen behandelt und verbindlich empfohlen werden können. Soweit daneben Abstimmungen in den jeweiligen Fachgremien erfolgen, sollten diese jedenfalls zu den technischen Standards auf den Festlegungen des Standardisierungsgremiums beruhen.

### Frage 253

Ob die EDV bzw. die IT letztlich die Kosten senken hilft, ist wohl kaum feststellbar und zwar deshalb, weil eine feststehende Referenz fehlt. Völlig klar ist, dass heute mit wesentlich weniger Personal bestimmte Aufgaben erledigt werden können, dass aber gleichzeitig in anderen Bereichen dafür ein ganz erheblicher Aufwand anfällt. Es gibt allerdings auch Aufgaben, die früher überhaupt nicht lösbar gewesen wären. Insofern wäre die Frage hinsichtlich des Einflusses der Informationstechnik auf die wirtschaftliche Entwicklung v.a. dahingehend zu sehen, dass die Informationstechnologie selbst ein erheblicher Wirtschaftsfaktor ist, bei dem ein Zurückfallen insgesamt im Rahmen der Wettbewerbsfähigkeit einen Rückschritt darstellt.

Da die öffentliche Verwaltung einen beachtlichen Prozentsatz der gesamten IT-Beschaffung ausmacht, ist praktisch die IT-Beschaffung auch eine Standort-Frage. Da aber die Beschaffung zu einem erheblichen Teil auf ausländische Hersteller entfällt, ist der Wirtschaftsfaktor v.a. dort zu sehen, wo es um die Anpassung, die Weiterentwicklung u. ä. geht, am wenigsten bei der Hardware und bei Standardsoftware (Datenbanken, Textprogramme u.ä.).

Daneben hat eGovernment und überhaupt die Möglichkeit der Beschleunigung von Verwaltungsverfahren durch den Einsatz von IT wesentlichen Anteil am Standortwettbewerb. Ein besonderes Qualitätsmerkmal einer Verwaltung ist die Möglichkeit, innerhalb einer angemessenen Zeit eine sichere Entscheidung zu erhalten. Hier kann der Einsatz von IT innerhalb der Verwaltung erheblichen Anteil an der Beschleunigung der Verfahrenslaufzeiten, aber auch durch die Bereitstellung des vorhandenen Verwaltungswissens eine bessere Entscheidungsgrundlage für die Verwaltung liefern.

Zudem weist die EU-Dienstleistungsrichtlinie den Weg in Richtung einer rein elektronischen Abwicklung von Verwaltungsvorgängen, so dass die Nutzung der IT in der Verwaltung zunehmend zu einer Basistechnologie wird.

Kann eine Verwaltung daher die IT zielführend einsetzen, um ihr Handeln schneller, besser und auch kostengünstiger zu gestalten, so wird die IT auch zum Hilfsmittel im Standortwettbewerb.

### Frage 254

Es ist nicht ersichtlich, dass es eine bedeutende Zahl von Geschäftsprozessen gibt, die IT-mäßig unterstützt werden und durchgängig Bund und Länder durchlaufen. Durch Koordination bei den Projekten und durch Abstimmung bei den Standards, ggf. auch gemeinsame Einrichtungen, die die Standards mit beeinflussen können, wäre eine entsprechende Optimierung möglich, ohne in die Kompetenzen ansonsten einzugreifen.

Die IT ist immer auf die Unterstützung der Verwaltungsprozesse beschränkt. Damit hängt die Möglichkeit der Nutzung von IT davon ab, wie aufgrund der Verwaltungskompetenzen die Verfahren gestaltet sind. Prozessoptimierungen sind dabei nicht zwingend Teil des IT-Einsatzes, sondern sollten als Daueraufgabe zur Optimierung der Tätigkeit der Verwaltung gesehen werden. Zwar scheinen bei der Einführung einer IT-Lösung Organisationsprobleme auf, diese liegen aber in historischen Entwicklungen und der kritiklosen Hinnahme gewachsener Abläufe. Insoweit stellt der (Neu-)Einsatz von IT zumindest eine Chance dar, solchen Organisationsprobleme zu entdecken und hierfür andere Lösungen zu entwickeln, sofern erforderlich.

Eine an der IT ausgerichtete Prozessoptimierung würde zu einer Nivellierung und Angleichung der Verwaltungsabläufe führen. Als Beispiel mag die Einführung einer betriebswirtschaftlichen Standardsoftware dienen: Wird das Produkt als Standard eingeführt, dann müssen alle Abläufe an den Strukturen der Software ausgerichtet werden. Sollen die Eigenarten des Unternehmens berücksichtigt werden, ist ein erheblicher wirtschaftlicher Aufwand erforderlich, der die Einführungskosten der Software häufig deutlich übersteigt.

Auf die Verwaltung gewendet bedeutet dies: Würde anhand einheitlicher Verwaltungsablaufbeschreibungen eine Software eingesetzt, liefe die Organisationskompetenz der Länder und Kommunen leer, da die zentrale Lösung verbindlich wäre. Werden Anpassungen zugelassen, entscheidet die wirtschaftliche Stärke und Leidenschaft des Nutzers, ob die – aufgrund der kompetenzgerechten Organisationsentscheidungen ermittelte – besondere Struktur der jeweiligen Verwaltungsabläufe auch künftig Geltung beanspruchen kann. Die Abwägung findet damit statt zwischen der Aufgabe der Organisationskompetenz und der wirtschaftlichen Kraft des jeweiligen Nutzers.

**Sinnvoll kann daher nur die Sicherstellung der Interoperabilität der technischen Lösungen sein.** Unabhängig davon haben Interessierte die Möglichkeit, zusammen aufgrund ihrer autonomen Entscheidung IT-Lösungen zu entwickeln, die eine gemeinsame Basis für die technische Unterstützung von Verwaltungsaufgaben bilden und einen wirtschaftlichen Umgang mit Steuermitteln sicherstellen.

### Frage 255

Zur Netzwerkverwaltung: Je heterogener die an einem Netzwerk beteiligten Stellen hinsichtlich ihrer Berechtigungen, sonstigen Ausgestaltungen sind, umso aufwändiger gestaltet sich die Netzwerkverwaltung. Es macht deshalb wohl auch Sinn, gestaffelt nach Aufkommen des gesamten Datenverkehrs bzw. der Zugriffe die Systeme so zu gestalten, dass der wohl als Hauptanteil anfallende interne Netzwerk-Verkehr der entsprechenden (dezentralen) Verwaltung unterliegt, und nur weitere Verwaltungen eingeschaltet werden, soweit der Datenverkehr dann extern erfolgt, wobei im Hinblick auf die wohl überwiegend dabei vorliegenden personenbezogenen Daten die Regelungen des Datenschutzes zu beachten sind. Diese lassen keine zentrale Netzwerkverwaltung zu.

Daneben muss bei der Gestaltung der Netzwerke die grundgesetzliche Kompetenzverteilung zur Wahrnehmung der Organisationskompetenz beachtet werden. Auch die Gestaltung von Verwaltungsnetzen orientiert sich an den Entscheidungen der jeweiligen Ebene zur Einrichtung und Ausrichtung ihrer Verwaltung. Wird die Netzstruktur zentral vorgegeben, so wird der Verwaltungsebene mittelbar ihre Kompetenz zur Entscheidung über Verteilung von Behörden etc. genommen.

### Frage 256

Es gilt ein ähnlicher Ansatz wie zum Thema Sicherheit. Einige Grundstrukturen, Mechanismen und hilfreiche Werkzeuge lassen sich zentral untersuchen und entwickeln. Deren Einsatz jedoch, also die konkrete Ausgestaltung und Installation ist letztlich eine lokale Angelegenheit, d. h. also dezentral zu bewerkstelligen, da der überwiegende Teil der Bürger-Kontakte eben auf einer dezentralen Ebene stattfindet. Um aber – soweit überhaupt notwendig - die Durchgängigkeit der Verwaltungsprozesse zu gewährleisten, wäre es dann weiterhin ausreichend, bei der Gesamt-Realisierung kooperativ, wie die Frage auch vorschlägt, vorzugehen und Maßnahmen zu ergreifen, die die Interoperabilität zumindest auf Datenebene, nicht aber auf Prozessebene gewährleisten.

**Es wird also befürwortet, den dezentralen Verwaltungsaufbau auch bei der Ausgestaltung von eGovernment zu berücksichtigen, dafür aber – soweit für den Datenaustausch und die Kommunikation notwendig - zentral Abstimmungsgremien bereitzustellen.**

Es kann im Rahmen des eGovernment auch durchaus ermöglicht werden, gerade ortsunabhängig den Bürgern ein Bündel von Verwaltungsleistungen über ein Portal bzw. über eine Anlaufstelle zur Verfügung zu stellen. Unter Aspekten sowohl der kompetenziellen Aufgabenzuweisung als auch des Datenschutzes aber dürfte der Bürger kaum damit einverstanden sein, dass etwa die Einheitlichkeit des Counters bzw. Centers dazu führt, dass sämtliche seiner Daten zusammengeführt werden, dass alle Aufgaben zusammen von einer Stelle erledigt werden usw. (was ohnehin unrealistisch erscheint).

Insofern ist vielleicht der Vergleich mit dem Call Center durchaus nahe liegend. Auch wenn Firmen etwa im Rahmen ihres Vertriebs oder ihrer Kunden-Services Call Center als Externe beauftragen, die also verschiedene Auftraggeber haben, ist es gerade so, dass der Kunde genau diese Verschiedenheit durchaus dann bei der Betreuung „erlebt“, wenn auch über einen einheitlichen Anlauf. D.h. also anders gesagt, dass die einheitliche Anlaufstelle nichts an der Kompetenz-orientierten Aufgabenerledigung und den jeweils spezifischen Prozessen ändern muss.

Wesentlich entscheidender wohl im Hinblick auf die Einheitlichkeit ist, dass der Kontakt des Bürgers mit dieser Anlaufstelle (oder den einzelnen Verwaltungsstellen) bei eGovernment medienbruchfrei erfolgt. Dies setzt allerdings ganz erhebliche Maßnahmen bzw. Leistungen im Bereich Sicherheit voraus.

Diese Überlegungen spielen dann auch für die Frage 260 eine Rolle.

### Frage 257

Wie dargelegt, ist der Datenschutz, auch dessen Basis (Zweckbindung, Aufgabenorientierung) so ausgerichtet, dass eine Zentralisierung praktisch das Fundament und das Grundprinzip aushebeln würde. Insofern stellt der **Datenschutz eine massive Grenze zentraler Strukturen** dar. Dabei geht es nicht einfach um das Verhältnis von Ländern zu Bund, von Kommune zu Land, sondern es geht insgesamt um die Abschottung der verschiedenen

Stellen auch auf der gleichen Ebene gegeneinander. **Dies ist ein datenschutzrechtliches, grundgesetzlich abgesichertes Gebot.**

Denkbar wäre etwa, dass bei einer Verarbeitung aller Daten in einem Rechenzentrum Begehrlichkeiten hinsichtlich einer „Zweitnutzung“ von zulässigerweise vorhandenen Daten für andere Zwecke möglich wäre und bei geeigneter Gelegenheit auch politisch gefordert würde. Die Herrschaft über die Daten würde nicht mehr bei der zuständigen und damit i.S.d. Datenschutzes verantwortlichen Behörde liegen. Die „Zweitnutzung“ muss spezialgesetzlich zu regelnden Ausnahmefällen vorbehalten bleiben, deren Erfüllung über die Schnittstellen und Einhaltung der Standards erleichtert wird.

### **Frage 258**

Die Aufhebung aller Behörden- und Ländergrenzen unter dem Banner von Interoperabilität und Verfügbarkeit der Daten steht, soweit ersichtlich, nicht zur Debatte, müsste jedenfalls abgelehnt werden.

**Interoperabilität** heißt nicht einfach Durchlässigkeit gegenüber jedem Datenstrom. Interoperabilität heißt nur, dass ein zulässig angestoßener Prozess ohne technische Schwierigkeiten, v.a. aber auch ohne Medienbrüche, ohne zusätzliche manuelle Arbeiten u.ä., wohl aber als gesicherter Prozess durchgeführt wird. Das heißt, dass die Interoperabilität, insbesondere, wenn sie auf Datenebene stattfindet, nicht zu einer Verwischung der Grenzen führt. Dies lässt sich auch anhand der Rechenzentrums- bzw. Service-Einrichtung zeigen, die entsprechende Abschottungen technisch realisieren (müssen).

Sinnvoll ist dagegen die **Vereinbarung von Sicherheitsstandards**, die alle Teilnetze einhalten müssen, um an dem Netzverbund teilnehmen zu können. Auch für den Austausch von Daten sollten Sicherheitsstandards zur Anwendung kommen, die die Sicherheit und Verlässlichkeit der Kommunikation gewährleisten. Die Implementierung dieser Vorgaben in die entsprechenden, dezentral verantworteten und wohl nicht identischen Produkte trägt ihren Teil zur Vermeidung der Ausnutzung von Schwachstellen bei.

### **Frage 259**

Es erscheint sinnvoll, ökonomisch und im Hinblick auf Bürgerservice geboten, sowohl auf Bundes- als auch erst recht auf Landesebene stets bei einer Neu-Regelung eine Aufgabe zu prüfen, inwieweit es sich durch entsprechende technische Ausgestaltung erreichen lässt, die Bürgernähe zu erhöhen und gleichzeitig den eGovernment-Ansatz zu verbessern, d.h. also die Möglichkeit der direkten elektronischen Erledigung bzw. Kontaktaufnahme und Ausführung.

Dem Wissensaustausch dienen die Fachgremien sowie – bei der vorgeschlagenen Struktur – das zentrale Steuerungsgremium, das die Standards berät, definiert und zur Anwendung empfiehlt. Im Sinne der best-practice-Betrachtung können auch die Implementierungen von Lösungen als modellhafte oder im Wettbewerb erfolgreiche Umsetzungen dienen.

### Frage 260

Es scheint nicht der Sicherheit ohne weiteres zu dienen, sämtliche Netze so miteinander zu koppeln, dass ein einheitliches Gesamtnetz entsteht.

Die hohe Verfügbarkeit ist – u.a. – ein Resultat von Redundanz und Ausfallsicherheit, die aber durch Zentralisierung bzw. Gesamt-Kopplung eher erhöht wird. Eine die Durchlässigkeit der Kommunikations-Infrastruktur – dort wo sie erforderlich ist – lässt sich insofern sicherer durch die Standardisierung mit gleichzeitiger Absicherung der verteilten Systeme erreichen.

Da es keine absolute Sicherheit, gerade nicht im IT-Bereich gibt, z.B. auch der geplante Bunderstroganer letztlich dazu führt, die Sicherheit an einzelnen Stellen wieder einzureißen, erscheint es nicht sinnvoll, zentrale Systeme so zu schaffen, dass dann, wenn die Sicherheit an einer Stelle wie erwartbar einmal nicht gegeben ist, das gesamte System dadurch geöffnet wird.

### Frage 261

Als das geeignete Mittel zur reibungslosen Kooperation auf v.a. Datenebene erscheinen Standards auf genau dieser Ebene, etwa aber auch Werkzeuge, die eine reibungslose und fehlerfreie Umwandlung verschiedener Formate (soweit diese erforderlich sind) bzw. unterschiedlicher Standards ermöglichen.

### Frage 262

Der Vergleich mit verschiedenen anderen Infrastrukturen hinkt. Wenn man ihn heranzieht, ist zu beachten, dass die Post ursprünglich neben der Postbank auch die gelbe Post zusammen mit der Telekommunikation, damals Telefonie, enthielt. Diese Entzerrung in den diversen Postreformen hat nun dazu geführt, dass die Telekommunikation zunächst einmal überhaupt als eigenständiger Bereich erkannt wurde. Später hat sich dann dieser Bereich weiterentwickelt, diversifiziert und ist nun ansatzweise erfolgreich in Trägerschaft verschiedenster Einrichtungen. Bei Wasserwegen, Fernstraßen, Eisenbahn und Luftverkehr sind ganz unterschiedliche Diskussionen im Gang, so etwa bei der Eisenbahn die Trennung zwischen dem Betrieb und den Gleisen.

Man könnte also gerade sagen, dass es verfehlt wäre, nachdem nun sämtliche früher einheitlichen Infrastrukturen eher aufgelöst werden, gerade im IT-Bereich, der gelungener Weise dezentral entwickelt wurde, in einen Zentralismus zu verfallen. Eine Regelungsbedürftigkeit besteht insofern allenfalls im Bereich des Datenschutzes – die bereits abgedeckt ist – und ein gesteigerter Bedarf an Leistungsfähigkeit insbesondere im Bereich der IT-Sicherheit, s.o. Der Schutz vor Angriffen ist durch eine Dezentralisierung eher gewährt. Trotz seines dezentralen bzw. redundanten Ansatzes ist z.B. auch das Internet noch im Hinblick auf einige wenige Knoten durchaus allzu anfällig. Richtig ist allerdings, dass zentrale Institutionen dazu verhelfen müssen, die Sicherheit insgesamt auf ein hohes Niveau zu heben, was aber nicht eine zusätzliche Gesetzgebungskompetenz erfordern würde. Zum Beispiel gibt es einen entsprechenden Ansatz bereits in § 9 BDSG. Für den privaten



Bereich gibt es eine ganze Reihe von Vorschriften, die implizit auch die Verfügbarkeit bzw. Sicherheit der IT fordern bzw. betreffen.

**Hier ist eine Unterstützung des Staates im Hinblick auf die Förderung der Sicherheit und die Entwicklung von Methoden und Werkzeugen gefordert, keine zentrale Verwaltung.**

### **Frage 263**

Die Frage ist schon richtig aufgeteilt. Die Antwort wäre, dass eine sichere Netzinfrastruktur einheitlich für alle Fachanwendungen schlecht gestaltbar erscheint, außer, was die „Standards“ betrifft, während im Bereich technisch aktuell und sicher zur Verfügung stehender Werkzeuge und Standards die Frage bejaht bzw. eine zentrale Institution schon vorhanden ist (BSI).

### **Frage 264**

Die Erfahrungen aus den genannten Projekten im Hinblick auf die Sicherheit können genutzt werden. Themen, wie Verschlüsselung, Signatur, Erkennen und Eingriffen/Angriffen u.ä., also Authentifizierung, Überprüfungsverfahren, Verifizierung u.ä. können zentral erarbeitet und dezentral ausgeführt werden.

Soweit sinnvoll können Module aus erfolgreichen Anwendungen auch für andere Anwendungen zur Verfügung gestellt werden (SOA-Ansatz). Auch hier zeigt sich der Vorteil einer dezentralen Software- und Lösungsentwicklung, da im Wettbewerb sich die bessere Lösung herausbilden kann. Diese Evolution der Lösungen wäre im Fall einer zentralen Vorgabe von Verwaltungsabläufen und IT-Lösungen nicht gegeben.

### **Frage 265**

In Kombination mit der Frage 266 ist zunächst festzuhalten, dass ein einheitliches Sicherheitsrisiko eigentlich nur im Hinblick auf ein Mindestniveau Sinn macht bzw. ausreichend wäre, da es andererseits aus Kostenaspekten kaum sinnvoll erscheint, generell unabhängig von den Anforderungen ein Maximalniveau erreichen zu wollen. Wie früher für das Grundschutzhandbuch und jetzt für den Grundschutzkatalog ist eine Einschätzung sowohl der Bedrohungslagen im jeweiligen Bereich als auch der sonstigen Risiken und der Anforderungen an die Kontinuität, Integrität usw. erforderlich.

Im Hinblick auf Frage 266 ist das wesentliche im Hinblick auf die Sicherheit wohl die Einheitlichkeit, da Brüche bzw. Verbindungen zwischen Netzen eher wieder sicherheitsanfällig sind.

Wichtig wäre dabei noch, dass eine gesamte einheitliche Netzinfrastruktur im Grunde die Risiken bei Ausfall eher drastisch erhöht. Es kann deshalb Sinn machen, auch unter Gesichtspunkten der Ausfallsicherheit bzw. Redundanz die bundeseinheitliche und bundesweite IT-Struktur für bestimmte Bereiche/Aufgaben zu schaffen, während die nicht für den

entsprechenden Bedarf sowohl an Einheitlichkeit als auch an Sicherheit haben, während andere, wohl in der Überzahl befindliche Anwendungen diese Merkmale nicht aufweisen.

Eine zentrale IT-Netzverkehrsbehörde wäre abzulehnen. Das Argument: Kommunikationsbeziehungen sind weitgehend landesintern, es besteht kein Bedarf nach einer bundeseinheitlichen Datenautobahn, die Sicherheit wird durch ein zentrales Backbone eher verringert. Die Einhaltung des Datenschutzes wird fraglich, wenn nicht klar ist, wie Daten geroutet werden.

### **Frage 266**

s. Frage 265

### **Frage 267**

Grundsätzlich sind die Bereitstellung und Sicherheit Aufgabe der Infrastrukturbetreiber, nicht aber des Staates. Der Staat kann Rahmenbedingungen schaffen und Regulierungsanreize bieten.

Die Frage impliziert im Grunde den dezentralen Ansatz. Im Hinblick auf die doch zum Teil in einzelnen Bundesländern starke flächenmäßige Verteilung der Bürger erscheint u.a. ein Zugang der Bürger von hervorragender Bedeutung. Diesen müsste dazu der entsprechend breitbandige Telekommunikationsdienst zur Verfügung stehen. Ob auf Dauer das Internet-Protokoll dafür der richtige Ansatz ist, kann im Hinblick auf die Sicherheitsprobleme, die damit verbunden sind, bezweifelt werden. Dies spricht für eine Mehrfacheinteilung: Die behördenmäßige Kommunikation dürfte stets eine gewisse Sicherheitsanforderung erfüllen. Speziellere Anwendungen erfordern höhere Sicherheitsstufen.

Ein pauschales Gebot der Internetnutzung bzw. der Nutzung dieses Protokolls erscheint verfehlt. Es hat mehrfach auch nicht zuletzt im Hinblick auf die Domains Ansätze gegeben, dass die USA, wenn es denn einmal kritisch wird, die Folgen von Änderungen für die übrige Welt in keiner Weise berücksichtigen. Diese Abhängigkeit müsste vorrangig abgebaut werden. D.h., dass die dem Internet entsprechende Redundanz, Schnelligkeit und geringe Anfälligkeit stärker ausgebaut werden sollten, und zwar über ein eigenes Netz, das aber ein kompatibles Protokoll benutzen lässt, ohne, dass man von Zufälligkeiten irgendeines Abstimmungsverhaltens etwa bei ICANN beeinflussbar ist. Es wäre also zentral, ein europäisches Sicherheits- und Domainkonzept insoweit für das Internet-Protokoll zu entwickeln.

### **Frage 268**

Der breitbandige Internetzugang als Universaldienst wäre zwar eine Erleichterung und würde evtl. auch die Kommunen von den im Zusammenhang mit der Zugangsproblematik, s. Frage 267 angedeuteten Leistungsanforderungen teilweise befreien, insbesondere, wenn diese Infrastruktur nicht von den Gemeinden mitgetragen werden muss. Damit erledigt sich jedoch nicht das Problem der Aufgabenbewältigung bzw. der Rationalisierung

hinsichtlich der Aufgaben, deren Ergebnisse über diese Breitband-Infrastruktur verteilt werden sollen.

Die Fragen 269 – 275 sind mit vorstehenden Antworten angesprochen, wenn auch nicht gelöst.

## C. Ergebnis

Die bisherigen Mechanismen zur Abstimmung zwischen Bund und Ländern zeigen, dass eine Änderung der grundgesetzlichen Kompetenzverteilung nicht notwendig ist. Es ist in der Vergangenheit gelungen, untereinander Abstimmungsprozesse zu etablieren, die die Nutzung der Informationstechnik in der Verwaltung und den notwendigen Austausch von Daten ermöglicht haben.

Ein Defizit, das eine Kompetenzverlagerung auf den Bund wegen der Unmöglichkeit der Abstimmung der Länder untereinander oder aufgrund der Anforderungen an die Sicherheit der Datenübermittlung rechtfertigen würde, liegt nicht vor.

In Hinblick auf die zunehmende Bedeutung der Nutzung der IT in der Verwaltung sind jedoch die Abstimmungsmechanismen kritisch zu hinterfragen mit dem Ziel, eine schnellere und effizientere Vereinbarung von technischen Standards zu ermöglichen.

Neue verfassungsrechtliche Instrumente sind dafür nicht erforderlich. Notwendig ist nur, auf der Basis der föderalen Kompetenzverteilung für die Verwaltungsorganisation im jeweiligen Kompetenzbereich die bestehenden Instrumente zu nutzen.

**Ein schematischer Aufbau im Bereich ITK könnte entsprechend der sehr einfachen Zweiteilung in Planung und Realisierung sinngemäß ohne Kompetenzverschiebung wie folgt gestaltet werden:**

- Erarbeitung von (übergreifenden) technischen (Datenaustausch-) **Standards** ist zentralisiert möglich; in der Umsetzung durch die Länder ist eine Koordinierung gleichgelagerter Aufgabenstellung durch Vereinbarungen gemeinsamer Aufgabenerledigung auf Basis der Standards möglich.
- Die Beibringung der **Anforderungen** ist genuin Sache des Anwenders. Er kann sich dabei (Erstellung von Spezifikationen) unterstützen lassen. Die Erstellung der Software selbst als Realisierung kann fremd vergeben werden. Die Rechtseinräumung bei diesen Projekten kann so ausgestaltet werden, dass die Software auch innerhalb der Verwaltung an jeder anderen Stelle eingesetzt werden könnte – bei entsprechenden Verrechnungen intern. Zur Aufgabenstellung kann, wo dies nicht zu unverhältnismäßigem Aufwand oder zur Verzögerung von Projekten führt, mit gehören, die Software so zu gestalten, dass sie für unterschiedliche Größenordnungen und Ausgestaltungen geeignet ist, also etwa im Sinne von Skalierbar, Parametrierbar u.ä.
- Der **Betrieb** solcher Software kann sowohl im eigenen Hause als auch in Fremd-Rechenzentren, seien diese öffentlich oder privat, erfolgen. Soweit gleichartige Aufgabenstellungen bei verschiedenen Stellen anfallen, kann es sich empfehlen, sie zentral oder im Service, einer für alle, durchzuführen.

- Bei bundesweit **übergreifenden Projekten**, wie etwa Grundbuch, können einzelne Länder die Federführung übernehmen, wie dies etwa ansatzweise auch bei der Verteilung im Mahnverfahren einerseits, Grundbuch andererseits, geschehen ist.
- In sämtlichen Phasen, insbesondere im Bereich der **Sicherheit** können zentrale Institutionen, wie hier beispielsweise das BSI **beraten**.
- Für die **Beschaffung** können einheitliche, die Vergabe erleichternde Vertragsmuster und vielleicht auch Muster-„Pflichtenheft“ zur Verfügung gestellt werden. Ansätze finden sich in den BVB/EVB-IT, im Vorgehensmodell u.ä. Unterlagen der KBSt (Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung). Dieser Ansatz könnte wesentlich verstärkt bzw. ausgebaut werden.

## D. Konsequenz für weitere Fragen:

Die vorstehenden Ausführungen betreffen ansatzweise auch folgende Fragen:

**216, 220:** Die vorgeschlagenen Lösungen über Flexibilität und Interoperabilität zusammen mit Schnittstellenförderung sollte eigentlich Innovationspotentiale und deren Entfaltung fördern.

**217:** Nicht nur die fehlende Legitimation, sondern auch die Veraltung und Starrheit der DIN sprechen für die vorgeschlagene Verstärkung der Kooperation.

**221, 223:** Benchmarking kann ein Mittel im Kontext der Reformvorschläge sein. Vorrangig wäre die Prozessoptimierung, auch in der Zusammenarbeit.

**274:** Die Vorschläge für Verstärkung und Strukturierung der Zusammenarbeit lassen eine zentrale Bundeskompetenz weitgehend entbehrlich erscheinen. Beim Thema Sicherheit erscheint eine zentrale Unterstützung notwendig.

**276:** Die Vergabeproblematik kann mit den Vorschlägen entspannt werden.

**277** Sinnvoll erscheint v.a. die gemeinsame Abstimmung im Hinblick auf Standards, Interoperabilität als Vorgaben und die gemeinsame Beauftragung mit den übereinstimmenden Anforderungen („85%).

**278, 279, 282 283 und 284** sind oben durch die Ausführungen in der Zusammenfassung sowie A l. beantwortet, zumindest angesprochen.

München, den 19.10.07

