Digitale Gewaltenteilung als Marktverantwortung

Kriterien zur rechtlichen Abgrenzung staatlicher und privatwirtschaftlicher Entfaltungsmöglichkeiten auf dem Markt der IT-Herstellung und IT-Services

Eine Studie im Auftrag des Verbandes der mittelständischen IT-Dienstleister und Softwarehersteller für den öffentlichen Sektor, DATABUND e.V.

Passau und Berlin, im März 2016

Autoren

Univ.-Prof. Dr. Dirk Heckmann, MdBayVerfGH

Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht
Forschungsstelle für IT-Recht und Netzpolitik
Universität Passau

Dr. Wilfried Bernhardt, Staatssekretär a.D.

Stv. Vorsitzender des Nationalen E-Government-Kompetenzzentrums

Inhaltsübersicht

Problemübersicht und Aufgabenstellung

Mit der Digitalisierungsoffensive in der Öffentlichen Verwaltung hat sich ein mittlerweile hart umkämpfter Markt etabliert, auf dem sich private und öffentlich-rechtliche Dienstleister dem Wettbewerb um Aufträge der Öffentlichen Hand stellen. Technologische Selbstversorgung, Inhouse-Geschäfte oder Preisdumping sind nur wenige Stichworte, die etwa mittelständische IT-Anbieter in Bezug auf die Herstellung und den Vertrieb „staatlicher Software", den Betrieb von Rechenzentren in öffentlicher Hand und das Angebot flankierender Dienstleistungen beklagen.[1] Dem halten die staatlichen Verantwortungsträger Zuständigkeitsgrenzen und Funktionsvorbehalte zugunsten der öffentlich-rechtlichen Anbieter, etwa aus Gründen des Datenschutzes oder der notwendigen Nachhaltigkeit und Interoperabilität der Anwendungen entgegen. Dabei geht es um mehr als Wettbewerbsanteile oder politische Präferenzen. Die Abgrenzung staatlicher Einflussmaßnahme auf den IT-Markt hat eine hohe rechtliche Relevanz, ist unterdessen aber bislang kaum geklärt. Dies gilt grundsätzlich sowohl für die Maßstäbe des Verfassungs-, Vergabe-, Wettbewerbs- und Datenschutzrechts als auch für die rechtlichen Spezifika der relevanten Verwaltungsbereiche. Klärungsbedürftig sind so etwa die kostenlose Abgabe „staatlicher Software" oder die umsatzsteuerrelevante Unternehmenseigenschaft von Verwaltungsträgern, die im IT-Markt agieren, aber auch die ausschreibungsfreie „Inhouse-Vergabe" von IT-Dienstleistungen und bestimmte Werbemaßnahmen von öffentlich-rechtlichen IT-Dienstleistern, denen ihre hoheitliche Nähe zu den Kunden (Bürgern oder anderen Nutzern) zugute kommt. Deshalb gilt es Kriterien zur rechtlichen Abgrenzung staatlicher und privatwirtschaftlicher Entfaltungsmöglichkeiten auf dem Markt der IT-Herstellung und IT-Services zu entwickeln. Leitbild hierfür ist das Prinzip der „digitalen Gewaltenteilung".

Grundsätzlich steht außer Frage, dass die Öffentliche Hand berechtigt ist, sich am Wirtschaftsleben – in welcher Form auch immer – zu beteiligen. Allerdings hat sie häufig einen Vorsprung im Vergleich zu Unternehmen der Privatwirtschaft, der sich aus Vorteilen wie Steuerbefreiungen, Finanzkraft, Zugang zu amtlichen Informationen, Vertrauensvorschuss in der Bevölkerung und amtlicher Autorität ergeben kann. Freilich kann daraus wiederum keine generelle und grundsätzliche Unzulässigkeit einer erwerbswirtschaftlichen Betätigung des Staates hergeleitet werden. Vielmehr geht es – aus verfassungsrechtlicher Perspektive – um die Frage, ob der Anspruch privater Unternehmer auf wirtschaftliche Entfaltung, Chancengleichheit, Berufsfreiheit und Gewährleistung des Eigentums verletzt worden ist. Dies liegt immer dann nahe,

[1] Die folgenden Ausführungen nach *Heckmann*, juris Praxiskommentar Internetrecht, 4. Aufl. 2014, Kap. 5, Rn. 146 ff.

wenn der Staat die genannten strukturellen Vorteile gegenüber privaten Akteuren auf dem Markt in besonderer, den Wettbewerb beeinträchtigender Art und Weise ausnutzt, indem er z.B. gezielt Marktpreise unterbietet, um private Akteure von Aufträgen fernzuhalten. Soweit der Staat hier allein und ohne Transparenz agiert, sind allerdings oft private Anbieter ohne nähere Informationen gar nicht in der Lage, eventuelle Beeinträchtigungen ihrer Grundrechtspositionen zu prüfen. Angesichts der möglichen Grundrechtsbeeinträchtigungen privater Unternehmen ist zu fordern, dass der Staat die Gründe für die eigene erwerbswirtschaftliche Betätigung transparent darlegt.

In komplexen E-Government-Strukturen sind die Interoperabilität der Systemkomponenten und die Sicherheit, Stabilität und Zugänglichkeit der Netzwerkstrukturen wesentliche Voraussetzungen für eine effiziente und rechtskonforme Behördenkommunikation. Insoweit besteht ein unstreitiges Bedürfnis nach staatlicher Setzung von Sicherheits- und Interoperabilitätsstandards. Angesichts der diesbezüglichen verfassungsrechtlichen Implikationen unterliegen aber staatliche Technologievorgaben strengen Anforderungen.

Verbindliche staatliche Technologievorgaben können in Konflikt mit Verfassungs- und Vergaberecht geraten, soweit den verankerten IT-Standards eine spürbare marktregulierende Wirkung zukommt, etwa weil sie all jene IT-Produkte und Dienstleistungen vom Beschaffungsmarkt der Öffentlichen Hand abkoppeln, die sich als nicht „standardkonform“ erweisen. Dabei wird die unter Bedarfszwecken notwendige Interoperabilität (oftmals ohne Not) durch einen intransparenten Standardisierungsprozess gesteuert. Insbesondere liegen hierbei die Entscheidungsstrukturen und die Entscheidungsgrundlagen nicht offen. Abseits der Problematik eines verfassungsrechtlich nur schwer zu rechtfertigenden Markteingriffs durch eine monopolartige oder marktbeherrschende Stellung kann der Staat durch seine Marktteilnahme mittelbar die Bedingungen für die privaten Teilnehmer auf dem IT-Markt verändern und so in grundrechtsbeeinträchtigender Weise an der Strukturierung der privaten Angebotsseite mitwirken. Es kommt insoweit nicht nur darauf an, ob der Staat bestimmte Teilnehmer von seinen (öffentlichen) Aufträgen ausschließt, sondern auch darauf, dass der Staat durch die (vordergründig „neutralen“) Technologievorgaben Marktteilnehmer zugleich mittelbar von der Beteiligung am übrigen IT-Markt ausschließen und dadurch einzelne Betriebe oder gar ganze Produktionszweige in ihrer Existenz gefährden kann. Der entscheidende Faktor der staatlichen Marktverzerrung durch technologiemarktorientierte Standardisierung liegt danach in deren mittelbaren Auswirkungen auf den Gesamtmarkt: Die Produkt- und Systementscheidungen der öffentlichen Verwaltung und die damit verbundene Dokumentation der Akzeptanz und

Zustimmung machen diese Produkte zu Referenzobjekten auch für die Produkt- und Systementscheidung anderer Nachfrager. Darüber hinaus führt die vom Verbreitungsgrad abhängige Attraktivität eines Produkts auf dem Markt (sog. Netzeffekt) gerade vor dem Hintergrund des Umfangs der – insoweit gebundenen – Beschaffungsaufträge der öffentlichen Hand und den daraus resultierenden Interoperabilitätsnotwendigkeiten zu einer Verengung des Marktes auf ein bzw. einige wenige Produkte. Die Unternehmen werden „gezwungen“, im Interesse der Anpassung an die vorherrschende Systemtechnologie auf „den Zug aufzuspringen“ und sich zumindest hinsichtlich der Kompatibilität dem vorherrschenden Produkt/System anzupassen (sog. Winner-takes-it-all-markets).

Standards begründen damit eine faktische Ausschlusswirkung für jeden – nicht den gewünschten Vorgaben entsprechenden und damit in gewisser Weise „bemakelten“ – Markteilnehmer. In diesem Sinne stellt jede regulative Beeinträchtigung des Marktgefüges im oben genannten Sinne eine Umverteilung der durch die Bedingungen des Marktes geschaffenen Erwerbschancen und insoweit einen mittelbaren Grundrechtseingriff dar. Je größer der Einfluss des Staates auf den Markt ist, desto höher sind die Anforderungen an die grundrechtliche Rechtfertigung staatlicher Marktbeeinflussung (hier: Standardisierung). Schließlich handelt es sich bei den Standards zunächst um Grundentscheidungen, die unter dem Gesichtspunkt der Nachhaltigkeit und Kontinuität die IT-Beschaffung der öffentlichen Hand determinieren, nicht aber im Detail regeln sollen.

Vor diesem Hintergrund müssen die technologiemarktorientierten Standards zum Schutz des Wettbewerbs vor zu engen, auf bestimmte Produkte oder Bieter zugeschnittenen Vorgaben eine angemessene Abstraktionshöhe besitzen.

Da nur ein Parlamentsgesetz geeignet ist , die notwendige – auch politische – Kontinuität zu vermitteln und zugleich den verfassungsrechtlichen Rechtfertigungsbedarf von grundrechtlicher Seite zu befriedigen, wird man generell eine gesetzliche Grundlage auch für das Setzen von IT-Standards durch den Staat fordern müssen. Der (Staats-) Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern (Vertrag zur Ausführung von Artikel 91c GG) weist in § 1 Abs. 1 Nr. 2 dem IT–Planungsrat die Aufgabe zu: (..) „beschließt fachunabhängige und fachübergreifende Interoperabilitäs- und IT-Sicherheitsstandards“. Nähere inhaltliche Maßstäbe für die Standards enthält der IT-Staatsvertrag nicht. Es ist daher Aufgabe von Wissenschaft und Rechtsprechung, die sich aus den Leitprinzipien der Rechtsordnung ergebenden Maßstäbe für die Standardisierung zu benennen.

Neben dieser Herausforderung will sich die vorliegende Studie im Folgenden

auch der Frage zuwenden, wie staatliches Handeln zu bewerten ist, das sich nicht in Standardsetzung erschöpft, sondern als direkte staatliche IT-Dienstleistung (z.B. Behördensoftware, Rechenzentrumsbetrieb) darüber hinausgeht. Welche Maßstäbe gelten hierfür, wenn die Potentiale und die Verantwortung der IT-Wirtschaft einbezogen werden? Wie weit reicht in diesem Lichte die - was zu erläutern sein wird - mittlerweile gewachsene Verantwortung des Staates, wie weit die Verantwortung der Wirtschaft? Wie ist tatsächlich staatliches Handeln dementsprechend verfassungsrechtlich, aber auch verfassungspolitisch zu bewerten? Wie ist ein daraus erwachsendes Verantwortungsgeflecht zwischen Staat und Wirtschaft zu definieren und zu konkretisieren und welche Verfahrensempfehlungen sind daraus abzuleiten?

Insgesamt erwächst aus den Entfaltungsmöglichkeiten in Verbindung mit dem Störpotential staatlicher IT-Entscheidungen eine staatliche Marktverantwortung für den IT-Sektor, die der ansonsten bestehenden Gestaltungshoheit des Staates Grenzen zieht. Im Rahmen einer sog. IT-Markt-Verträglichkeitsprüfung sind alle staatlichen Entscheidungsträger gehalten, die Auswirkungen ihrer IT-Entscheidungen (Softwareherstellung und Vertrieb, das Setzen von IT-Standards oder die Bereitstellung von IT-Services in Rechenzentren etc.) auf den relevanten IT-Markt zu prüfen. Im Rahmen einer nachhaltigen IT-Strategie muss eine Balance zwischen staatlicher Schutzpflicht und marktorientierter Zurückhaltung gefunden werden (technical self-restraint).

I. Einleitung

1. Zunehmende Digitalisierung öffentlicher Aufgabenwahrnehmung

These 1: Die Digitalisierung erreicht zunehmend auch die öffentliche Hand. Elektronische Kommunikation, elektronische Aktenführung und automatisierte Geschäftsprozesse in Behördennetzwerken bestimmen künftig das Bild öffentlicher Aufgabenwahrnehmung. Dabei dienen das Internet und vielfältige IT-Ressourcen nicht nur als Plattform und Medium, sondern zugleich der Maßnahmensteuerung. Der Bedarf an sachdienlicher Hardware und Software und entsprechender IT-Services steigt exponentiell. So verpflichten z.B. die E-Government-Gesetze von Bund und Ländern die Verwaltungen zur Einführung der elektronischen Verwaltungsakte in jeweils festgelegten Zeiträumen. Gerade die elektronische Aktenführung wird mit ganz bedeutsamen IT-Beschaffungsentscheidungen auf Bundes- und Landesebene verbunden sein. Die Aktensysteme werden sich wiederum auf die sogenannten Fachverfahren auswirken, die entweder einzubinden, anzupassen oder zu ersetzen sind. Der Medienwechsel von Papier zur Elektronik (Einscannen) oder umgekehrt von den elektronischen Medien zu Papier

(Ausdrucken) erfordert für viele Jahre eine zusätzliche Infrastruktur (Scanner, Drucker, Software). Aber auch die Instrumente für die Kommunikation zwischen Verwaltung einerseits und Bürgern bzw. Wirtschaft andererseits entwickeln sich – auch aufgrund der Vorgaben der E-Government-Gesetze oder europäischer Vorgaben (z.B. der eIDAS-Verordnung) – weiter. Daraus ergeben sich Fragen rechtskonformer Herstellung, Beschaffung und Bereitstellung von IT-Produkten und IT-Dienstleistungen, die als Nebenschauplatz der umfassenden digitalen Transformation bislang kaum beachtet werden. Man schaut eher, ob der hohe Bedarf überhaupt gedeckt werden kann, nicht aber, durch wen dies erfolgt. Vielfach fehlt auch ein Problembewusstsein, dass diffuse Beschaffungsprozesse oder das Fehlen einer Marktanalyse (kann der Bedarf durch die Dienstleistung eines privaten Unternehmens gedeckt werden?) rechtlich geschützte Interessen verletzen könnten.

2. Zunehmende Verrechtlichung des digitalen Staates

These 2: In den letzten Jahren zeigt sich eine zunehmende Verrechtlichung der digitalen Prozesse in Staat und Kommunen. Nach ersten zögerlichen Reformbemühungen in den Verwaltungsverfahrensgesetzen haben das E-Government-Gesetz des Bundes (2013) und mehrere seiner Abbilder auf Landesebene (Sachsen, Bayern, Baden-Württemberg) einen ersten größeren Rechtsrahmen gesetzt. Ähnliches gilt für die Förderung des elektronischen Rechtsverkehrs im Justizwesen durch das E-Justice-Gesetz (2013). Das IT-Sicherheitsgesetz (2015) ergänzt die rechtliche Struktur um Vorgaben für ein adäquates IT-Sicherheitsniveau, bei denen das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine zentrale Stellung einnimmt. Das Ende 2015 beschlossene E-Health-Gesetz bemüht sich um die Regulierung des elektronischen Gesundheitswesens und setzt Akzente mit der Gestaltung einer staatlich kontrollierten Telematikinfrastruktur.

Mittlerweile werden nationale Regelungen auch durch europarechtliche Verpflichtungen überlagert. So ermächtigt die eIDAS-Verordnung die Kommission zum Erlass sogenannter Durchführungsrechtsakte, die wiederum sehr spezifische – teils auch technische - Regelungen treffen.[2] Solche Durchführungsrechtsakte gehen – soweit sie sich im Rahmen der Ermächtigung durch die Verordnung halten – nationalem Recht, z.B. der Signaturverordnung, vor.

Allen diesen Gesetzen ist ein eher partielles und zuweilen rudimentäres Vorgehen gemeinsam. Aussagen zum Verhältnis hoheitlicher oder privatwirtschaftlicher

[2] Z.B. der Durchführungsbeschluss (EU) 2015/1505 der Kommission vom 8. September 2015 über technische Spezifikationen und Formate in Bezug auf Vertrauenslisten oder der Durchführungsbeschluss (EU) 2015/1506 der Kommission vom 8. September 2015 zur Festlegung von Spezifikationen für Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel, die von öffentlichen Stellen (…) anerkannt werden.

Betätigung bei der Aufgabenerledigung werden kaum getroffen. Explizite Ausnahmen bilden zum Beispiel:

- Nach Art. 3 BayAGBMG (früher: Art. 34 BayMeldeG) dürfen die Meldebehörden bestimmte Aufgaben der Meldedatenverarbeitung auf die Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) übertragen.
- Eine ähnliche Lösung sieht Sachsen vor: Die Sächsische Anstalt für kommunale Datenverarbeitung (SAKD) betreibt seit 1. November 2015 das Sächsische Melderegister (SMR) - Nachfolge des Kommunalen Kernmelderegisters (KKM) - auf der Grundlage der Vorgaben des § 2 Sächsisches Gesetz zur Ausführung des Bundesmeldegesetzes. Ferner prüft und zertifiziert die SAKD im gesetzlichen Auftrag in Sachsen die Software, die die automatisierte Ausführung von Kassengeschäften und anderen Geschäften im Bereich des kommunalen Finanzwesens programmtechnisch umsetzt.
- Art. 7 BayAGPStG regelt den Betrieb des Personenstandsregisters durch die AKDB.
- Zu nennen ist auch § 7a Abs. 1 BSIG, demzufolge das BSI auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen und bewerten darf.

Im Übrigen verbleibt es bei einzelnen Vorschriften, die einen staatlichen Einfluss auf den IT-Einsatz sicherstellen sollen.

Bei den genannten Vorschriften stellt sich die Frage, ob der Staat vor der Rechtsetzung hinreichend geprüft hat, ob die geltend gemachten Gründe für eine Zuweisung der IT-Dienstleistungsaufgaben an Behörden angesichts etwaiger Möglichkeiten privater Unternehmen stichhaltig sind. Angesichts der möglichen Grundrechtsbeeinträchtigung privater Dienstleistungsanbieter müsste auch der Gesetzgeber die Gründe für die Zuweisung der Aufgaben an die Behörden darlegen.

3. Zunehmende Bedrohungen der Funktionsfähigkeit von IT

These 3: Je stärker sämtliche Geschäftsprozesse der Öffentlichen Verwaltung digitalisiert werden, um so größer wird die Notwendigkeit, diese Prozesse vor Fehlfunktionen, Angriffen und Instabilität zu schützen. Durch IT-Unsicherheit werden nicht nur die Vorteile der aufwändigen digitalen Transformation aufgehoben. Die Funktionsfähigkeit von Staat und Verwaltung insgesamt kann dadurch in Frage gestellt werden. Deshalb steht die öffentliche Hand nicht nur vor der Herausforderung, sich zeitgemäß zu organisieren. Sie muss auch gewährleisten, dass der Übergang zur elektronischen Verwaltung reibungslos funktioniert (change management), die neuen Prozesse stabil und sicher sind und ihre

permanente Anpassung an alle relevanten Aktionsräume (A2A, A2B, A2C) gelingt. Auch hierfür ist wiederum geeignete IT einzusetzen. Die Bedrohung der Funktionsfähigkeit von IT wird um so eher zur Bedrohung des Gemeinwesens selbst auswachsen, so weit es dem Staat, aber auch anderen verantwortlichen Akteuren nicht gelingt, die digitale Transformation des öffentlichen Sektors im Sinne eines nachvollziehbaren und nachhaltigen Risikomanagements zu steuern anstatt einfach geschehen zu lassen.

So betonte der bayerische Finanzminister in seiner Einbringungsrede zum BayEGovG: „Übrigens setzen wir bei Ausschreibungen bewusst auf Insourcing, um uns von technischen Lösungen, die uns aus dem Ausland angeboten werden, unabhängiger zu machen. Und wir verstärken das Personal, damit wir wissen, wie man auf die jeweiligen Herausforderungen reagieren kann.“[3]

Allerdings stellt die abstrakte Bedrohung der IT-Sicherheit noch nicht ohne Weiteres eine ausreichende Rechtfertigung dafür dar, Informationstechnologie durch Behörden selbst entwickeln oder in ausschließlicher Verantwortung des Staates betreiben zu lassen. Es gibt keinen plausiblen sachlichen Grund, dass der Staat diese Gefährdungslage besser bewältigen kann als dies durch privatwirtschaftliche Lösungen geschehen würde. Hinzu kommt, dass private Anbieter hierdurch in ihren Grundrechten verletzt sein könnten. Allenfalls wird man aus der Bedrohungssituation eine stärkere Steuerungsverantwortung des Staates folgern können. Innerhalb dieser Steuerungsverantwortung muss dann der Staat konkret prüfen, ob er selbst Software zu entwickeln bzw. IT-Dienstleistungen selbst betreiben sollte oder die Bedrohung zum Anlass nehmen sollte, die Aufsicht über die Dienstleistungserbringung durch Private zu verstärken. Auch ist der schlichte Hinweis darauf, dass IT „aus dem Ausland“ angeboten wird, noch nicht geeignet, ein „Insourcing“ plausibel zu begründen. Denn gerade die europäische Rechtssetzung z.B. in Gestalt der Datenschutzgrundverordnung soll ja europaweit Grundrechte absichern und daher Argumenten entgegenwirken, man müsse nationale Maßnahmen ergreifen, um Grundwerte zu schützen.

4. Öffentliche Hand zwischen Haushaltsdisziplin und Digitalisierungserfordernis

These 4: Aufgrund der Haushaltszwänge sind Bund, Länder und Kommunen gehalten, enger zusammenzuwirken und die Aufgabenwahrnehmung durch Einsatz der Informationstechnologie intensiver aufeinander abzustimmen.[4]

[3] S. 6 der Plenums-Vorgangsmappe zur Drucksache Nr. 17/9295 vom 02.12.2015.

[4] „In Bund, Ländern und Gemeinden werden an vielen Stellen Aufgaben automatisiert. Es besteht hierbei jedoch die Gefahr, dass gleiche Aufgaben an mehreren Stellen gleichzeitig bearbeitet werden. Die möglichen Doppelarbeiten könnten vermieden werden und die Wirkung der von der öffentlichen Hand für die Automation eingesetz-

Ein solches Zusammenwirken verschiedener Verwaltungsträger führt jedoch zu immer komplexer werdenden Beschaffungsentscheidungen und erheblichen Auswirkungen auch auf das Ausgabenvolumen. So gebieten die Vorschriften des Haushaltsrechts (z.B. § 7 Abs. 2 SächsHO – Pflicht zu einer Wirtschaftlichkeitsuntersuchung - in Verbindung mit den Regeln des Vergaberechts, des Wettbewerbsrechts und des Kartellrechts[5]) oft eine intensive Befassung mit den finanziellen Auswirkungen und führen teilweise zu komplizierten Rechtsfragen, die in zwei vom IT-Planungsrat in Auftrag gegebenen Gutachten zur Evaluierung der Kieler Beschlüsse untersucht wurden[6].

Das Vergaberecht privilegiert den kostenlosen Erwerb von Hard- und Software, denn nur *entgeltliche* Verträge sind öffentliche Aufträge im Sinne des § 99 Abs. 1 GWB. Wenn z.B. ein Bundesland von einem anderen eine Lizenz oder eine Softwarepflegeleistung *unentgeltlich* erwirbt, liegt darin *keine vergabepflichtige Beschaffung*. Eine *kostenlose* Übertragung der durch einen Verwaltungsträger erworbenen Rechte auf andere Länder ist daher ohne Verstoß gegen das Vergaberecht möglich. Allerdings untersagt normalerweise umgekehrt das Haushaltsrecht eine kostenlose Abgabe der Software. So regelt § 63 Abs. 3 SächsHO, dass Vermögensgegenstände nur zu ihrem vollen Wert veräußert werden dürfen. Ausnahmen können im Haushaltsplan oder im Haushaltsgesetz zugelassen werden. Mit den „Kieler Beschlüssen“ von 1968, die 1979 überarbeitet wurden, hat der „Kooperationsausschuss Automatisierte Datenverarbeitung Bund/Länder/Kommunaler Bereich (KoopA)“ Vorkehrungen dafür getroffen, die Kosten durch Vermeidung von Doppelarbeiten zu senken, die personellen Ressourcen effizient zu nutzen und auch Gebietskörperschaften mit geringerer Finanzkraft an der Verwaltungsautomation teilhaben zu lassen. Investitionen in verwaltungseigene IT-Programme sollten durch Zusammenschluss mehrerer öffentlicher Verwaltungen mehrfach genutzt werden können, um gemeinsam ein automatisiertes Verfahren zu entwickeln oder um gemeinsam ein bestehendes automatisiertes Verfahren zu pflegen. Die Kieler Beschlüsse betreffen „allein oder im Verbund erstellte Programme (Eigenentwicklung oder Fremdentwicklung im Auftrag;
der ‚Kauf' von Standard-Programmen)“. Diese sollten „im Rahmen der insoweit bestehenden allgemeinen Gegenseitigkeit“ einer anderen Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt, grundsätzlich ohne Kostenverrechnung zur Nutzung überlassen werden können. Die Kieler Beschlüsse setzten kein Haushaltsrecht außer Kraft, führten aber zu entsprechenden Anpassungen in den Haushaltsgesetzen des Bundes und der Länder, indem dort zugelassen wurde,

ten finanziellen Mittel könnten wesentlich erhöht werden, wenn ein gut abgewogenes Aktionsprogramm vorhanden wäre.“ (Protokollauszug zu Thema II des 6. Erfahrungsaustausch EDV Bund/Länder am 9. und 10. Mai 1968 in Kiel)

[5] §§ 97 ff GWB sowie Verordnung (EU) Nr. 1336/2013.

[6] Einsehbar unter Internetlinkverzeichnis Nr. 1.

dass von Landesdienststellen im Bereich der Datenverarbeitung entwickelte oder erworbene Programme unentgeltlich an Stellen der öffentlichen Verwaltung abgegeben werden, soweit Gegenseitigkeit besteht. Allerdings sind sich Bund und Länder darüber einig, dass die Kieler Beschlüsse nicht mehr zeitgemäß und weiterzuentwickeln sind. So hat der IT-Planungsrat 2012 ein Projekt zur Evaluierung der Kieler Beschlüsse gestartet, um Antworten auf zahlreiche Fragen - z.B. zum finanziellen Ausgleich - bei einem nachträglichen Beitritt zu bestehenden Kooperationen beantworten zu können. Mittlerweile sind zwei Gutachten erschienen. Das erste, 2013 vom IT-Planungsrat angenommene Gutachten enthält eine rechtswissenschaftliche Evaluation der Gültigkeit und Anwendbarkeit der "Kieler Beschlüsse“. Das zweite rechtswissenschaftliche Gutachten legt die von den Kieler Beschlüssen nicht erfassten Fragen der rechtssicheren Gestaltung von institutionalisierten Kooperationen bei der Entwicklung, Pflege und Betrieb von Software dar. Hinzukommt ein Praxisleitfaden zur Gestaltung vertraglicher Software-Kooperationen. Beide letztgenannte Dokumente hat der IT-Planungsrat in seiner 15. Sitzung am 16. Oktober 2014 angenommen.

II. Verantwortung des digitalen Staates

These 5: Der „digitale“, umfassend IT einsetzende Staat ist nicht nur Nutznießer neuer Medien und Formen der Aufgabenerfüllung. Er trägt auch die Verantwortung für die Funktionsfähigkeit der IT-Systeme und ihrer Komponenten, soweit er diese initiiert, zur Verfügung stellt oder für seine Belange nutzt. Diese Verantwortung ist die Kehrseite seiner Organisationshoheit, für die ihm verfassungsrechtlich ein erheblicher Gestaltungsspielraum gegeben ist, von dem er aber auch nur in bestimmten (verfassungs-) rechtlichen Grenzen Gebrauch machen darf. Vor diesem Hintergrund obliegen dem Staat eine IT-Infrastrukturverantwortung, eine IT-Zugangsverantwortung, eine IT-Anwendungsverantwortung und eine IT-Sicherheitsverantwortung.

1. IT-Infrastrukturverantwortung

These 6: Mit der Einfügung des Art. 91c GG in das Grundgesetz durch die Föderalismusreform 2009 wurde eine verfassungsrechtliche Grundlage für die Zusammenarbeit von Bund und Ländern im Hinblick auf deren informationstechnische Systeme geschaffen und damit die im „KoopA“ und in den „Kieler Beschlüssen“ angelegte Zusammenarbeitsform mit einer neuen rechtlichen Qualität versehen. Das betrifft sowohl den hoheitlichen Betrieb von IT-Systemen als auch die hoheitliche Festlegung von IT-

Standards. Die Einrichtung eines IT-Planungsrats durch den IT-Staatsvertrag ergänzt das Aufgabenspektrum in Zusammenhang mit IT-Projekten. Aus alledem lässt sich folgern, dass die öffentliche Hand das Recht zur eigenverantwortlichen Schaffung und zu dem Betrieb jener IT-Infrastruktur („informationstechnische Systeme", staatliche Rechenzentren, öffentlich-rechtliche IT-Dienstleister) hat, die zur Erledigung der Verwaltungsaufgaben auf Bundes-, Landes- und kommunaler Ebene erforderlich ist. Aus dieser Infrastrukturverantwortung lässt sich allerdings nicht zwingend schlussfolgern, in welchem Maße die Aufgaben durch den Staat selbst wahrzunehmen, Privaten überlassen werden können, und ggf. sogar überlassen werden müssen. Aus dem Prinzip der Wirtschaftlichkeit staatlichen Handelns, das in Art. 114 GG[7] vorausgesetzt wird, lässt sich allerdings das verfassungsrechtliche Gebot zur Prüfung entnehmen, ob und welche Handlungsformen in Betracht kommen, um staatliche Ausgaben zu senken. Entsprechend verpflichten § 7 BHO und die parallelen Länderregelungen dazu, bei Aufstellung und Ausführung des Haushaltsplans die Grundsätze der Wirtschaftlichkeit und Sparsamkeit zu beachten: „Diese Grundsätze verpflichten zur Prüfung, inwieweit staatliche Aufgaben oder öffentlichen Zwecken dienende wirtschaftliche Tätigkeiten durch Ausgliederung und Entstaatlichung oder Privatisierung erfüllt werden können"[8].

2. IT-Zugangsverantwortung

These 7: Der Staat kann sich nicht darauf beschränken, IT-Systeme für Informationen, Kommunikation und Interaktion bereitzustellen. Er muss auch den reibungslosen Zugang dorthin gewährleisten. Eine solche staatliche IT-Zugangsverantwortung ist nunmehr für die elektronische Behördenkommunikation im E-Government-Gesetz des Bundes normiert (insbesondere auch durch die avisierte Standardkommunikation über De-Mail); die Bundesländer folgen sukzessive. Noch weitergehend als der Bund beschreibt Art. 2 BayEGovG mit dem „Recht auf elektronische Verfahrensdurchführung" die digitalen Zugangs- und Verfahrensrechte. Darüber hinaus lassen sich der eIDAS-VO Regelungen entnehmen, die einen diskriminierungsfreien Zugang auch aus anderen EU-Mitgliedsstaaten zu E-Government-Instrumenten im Verhältnis zwischen Bürger, Unternehmen und Verwaltung fordern. IT-Zugang geht aber noch weiter: Erfasst wird auch der elektronische Zugang zu bestimmten Behördeninformation (Open Data, Open Government, Open Access), den der Staat gewährleisten muss. Die Reichweite dieses Zugangsrechts ist allerdings stark umstritten. Während Länder wie Hamburg und Rheinland-Pfalz in Transparenzgesetzen

[7] Dort ist explizit die Prüfungskompetenz des Bundesrechnungshofs zur Wirtschaftlichkeit angesprochen.

[8] § 7 Abs.1 S. 2 BHO.

mittlerweile eine weitgehende, aktive Bereitstellungspflicht des Staates für bestimmte Daten normieren, betont Bayern in seinem EGovG die Grenzen des Zugangsrechts, um das Recht auf informationelle Selbstbestimmung nicht zu gefährden.

Darüber hinaus lässt sich der IT-Zugang auch noch dahingehend verstehen, dass bestimmte Bandbreiten zur Verfügung gestellt werden müssen, um eine angemessene technische Qualität der Datenübertragung zu erzielen. So unumstritten die staatliche Verantwortung für den Breitbandausbau ist, so sehr wird eine wettbewerbliche Lösung zur Umsetzung angestrebt. Aus Art. 87f Abs. 2 S. 1 GG lässt sich herauslesen, dass der Staat gehalten ist, der Verpflichtung zur Gewährleistung zum Breitbandzugang nicht durch eigene Dienstleistungen nachzukommen, sondern durch Einschaltung Privater; insoweit wird in der Literatur von „negativer Kompetenzschranke“ gesprochen.[9]

Dies hat auch den bedeutsamen Nebeneffekt, den ländlichen Raum besser an das Leistungsspektrum im Internet anzubinden. Relevant wird dies u.a. auch für die Gesundheitsvorsorge, die im Kontext von E-Health und Telemedizin ohne entsprechende Bandbreiten nicht funktionieren würde. Dies hat (insbesondere im Freistaat Bayern) auch eine verfassungsrechtliche Grundlage. So wurde Art. 3 Abs. 2 S. 2 BV durch einen Volksentscheid 2013 ergänzt: „Er [der Staat] fördert und sichert gleichwertige Lebensverhältnisse und Arbeitsbedingungen in ganz Bayern, in Stadt und Land.“

3. IT-Anwendungsverantwortung

These 8: Wer die IT beherrscht, beherrscht zuweilen auch die Inhalte. So können Vorgangsbearbeitungssysteme den genauen Ablauf eines Verwaltungsverfahrens lenken, starre elektronische Formulare lassen dem Nutzer keinen Spielraum für kreative, den Rahmen des Formulars überschreitende Inhalte, elektronische Kommunikationsinstrumente bieten die Chance, Kommunikationsinhalte auch Dritten zur Verfügung zu stellen, die der Nutzer eigentlich nicht adressieren will. Dementsprechend muss der Staat bei der IT-Organisation für die Erfüllung eigener Aufgaben auch dafür sorgen, dass die jeweilige IT-Anwendung rechtskonform erfolgt. Dies gilt sowohl für die Reichweite einer Auftragsdatenverarbeitung (Art. 11 BDSG) als auch für die Frage, ob Private überhaupt tätig werden dürfen.

Zwar ist nach Art. 33 Abs. 4 GG die Erfüllung hoheitlicher Aufgaben öffentlich-rechtlich organisierten IT-Dienstleistern vorbehalten. Hierbei ist aber zu beachten, dass der größte Teil jener IT-Dienstleistungen, die auch von Privaten erbracht werden können, ohne-hin nicht den Kern hoheitlicher Tätigkeiten betrifft.

[9] *Thomas Kleist/Nicola Lamprecht-Weißenborn/Alexander Scheuer* ‚Rechtliche Schlussfolgerungen, insbesondere aus Artikel 73Absatz 1 Nr. 7 und Artikel 87f Grundgesetz, S. 30 f., einsehbar unter Internetlinkverzeichnis Nr. 2.

Selbst im Kontext hoheitlicher Verwaltung sind sog. technische Hilfstätigkeiten unproblematisch durch Private zu bewerkstelligen.

Eine besondere Verantwortung kommt dem Staat zu, wenn die Gefahr besteht, dass ein anderes Rechtsregime das Handeln eines an der Datenverarbeitung Beteiligten bestimmt und dieses Rechtsregime nicht mit den Vorgaben des Grundgesetzes z.B. zum Recht auf informationelle Selbstbestimmung, korrespondiert. Nach dem Urteil des EuGH zum Safe Harbor-Übereinkommen dürfte § 4c BDSG keine Standardklauseln mehr zur Auftragsdatenverarbeitung mit US-Unternehmen mehr erlauben.[10].

4. IT-Sicherheitsverantwortung

These 9: Die Gewährleistung von IT-Sicherheit gehört zu den überragenden Obliegenheiten des Staates im 21. Jahrhundert. Das ergibt sich aus der signifikanten Bedrohungslage (siehe BSI Bericht zur Lage der IT-Sicherheit 2015). Die rechtliche Verpflichtung folgt aus den staatlichen Schutzpflichten, die aus dem objektiven Gehalt des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht) oder aus dem Rechtsstaatsprinzip hergeleitet werden. Dabei bleibt klärungsbedürftig, wie diese Schutzpflicht im Detail umzusetzen ist, weil der Staat entgegen dem Wortlaut des IT-Grundrechts IT-Sicherheit nicht wirklich gewährleisten (sic!) kann. Unstreitig ist aber die Schutzpflicht als solche und damit ein verfassungsrechtliches Verbot einfachen Untätigbleibens (Untermaßverbot). Unmittelbare Pflichten werden bestimmten Akteuren dabei durch das Gesetz zur Erhöhung der IT-Sicherheit (IT-Sicherheitsgesetz) auferlegt. Die Abgrenzung dieser Pflichten ist ungeklärt. In den weiteren Bereich der IT-Sicherheitsverantwortung auf der Grundlage des Rechtsstaatsprinzips gehört auch die Frage, wie der Staat sicherstellt, dass grundrechtsrelevante Verwaltungsvorgänge umfassend dokumentiert werden und auch nach einem Medienwechsel das bisherige sachbezogene Geschehen sowie mögliche Erkenntnisquellen für das zukünftig in Frage kommende behördliche Handeln gesichert gespeichert bzw. aufbewahrt werden.[11] So fordern die E-Government-Gesetze (z.B. § 6 S. 3 EGovG), durch „geeignete technisch-organisatorische Maßnahmen nach dem Stand der Technik sicherzustellen, dass die Grundsätze ordnungsgemäßer Aktenführung eingehalten werden“. Der „Stand der Technik“ wird demzufolge durch die Technische Richtlinie des BSI -TR-03138 Ersetzendes Scannen (RESISCAN) festgehalten[12].

[10] Als Alternative kommen Einwilligungserklärungen der Kunden in Betracht. Diese sind aber nur schwer umzusetzen, da sie einhergehen müssen mit einer ausführlichen Darstellung der übermittelten Daten, ihrer Zwecke und der mit ihrer Übermittlung verbundenen Risiken. Vgl. *Heckmann/Starnecker*, jM 2016, 58 ff.

[11] BVerfG, NJW 1983, S. 2135 f.

[12] BSI TR 03138, einsehbar unter Internetlinkverzeichnis Nr. 3; zur Kritik an der Technischen Richtlinie: Einsehbar unter Internetlinkverzeichnis Nr. 4.

III. Verantwortung der digitalen Wirtschaft

Auch wenn der Staat die Hauptverantwortung für eine funktionierende, stabile und sichere IT trägt, ist die Verantwortung der digitalen Wirtschaft in diesem Kontext nicht von der Hand zu weisen.

1. Notwendigkeit von IT-Innovationen

These 10: Eine bedeutende Folge der Digitalisierung ist die zunehmende Komplexität und Weiterentwicklung der IT-Strukturen, die eine ständige Anpassung an neue Systemkomponenten erfordert. Die Zerbrechlichkeit, Angreifbarkeit und Störanfälligkeit des Systems bringt zudem erhebliche Herausforderungen für die Sicherheit und Funktionsfähigkeit der IT-Systeme und ihre einzelnen Komponenten mit sich. Insgesamt ergibt sich hieraus eine Innovationsspirale: Innovationen in Teilen des Systems erfordern Anpassung und Ausgleich durch Innovationen an anderer Stelle. So muss die „Mobilisierung" der IT im Sinne einer komfortablen Nutzung mobiler IT-Endgeräte auch durch Behördenmitarbeiter einhergehen mit neuen IT-Sicherheitsherausforderungen: Das versehentliche „Liegenlassen" von Smartphones/Notebooks darf fremden Personen den Zugriff auf sensible Behördendaten nicht ermöglichen. Neue Zugriffssperren sind in die mobilen Endgeräte einzubauen. Die Kombination der Nutzung von Mobilnetzen/GPS-Funktionen/ Kamera mit ihren Möglichkeiten, Profile von Nutzern zu erzeugen, schafft neue Datenschutzprobleme, gegen die neue Absicherungen erforderlich sind.

Der Staat „befeuert" diese Innovationsspirale mit seinen IT-Strategien, trägt aber nur teilweise zur Weiterentwicklung und Stabilität des Systems bei. Im Gegenteil: Teilweise erfordern gerade seine Systementscheidungen (Beispiel: verbindliche Einführung der De-Mail) Systemanpassungen, die er selbst nicht leisten kann und die dann in der Wirtschaft und bei den Bürgerinnen und Bürgern zu Mehrkosten führen. Ohne eingehende Folgenanalyse verbindlicher Vorgaben drohen so Lähmungen alternativer dynamischer Fortentwicklungen durch die Wirtschaft. So konnte im Gesetzgebungsverfahren zum EGovG gerade noch ein „closed shop" der Schriftformersatzmöglichkeiten verhindert werden.[13] Der Bundesrat setzte sich mit dem Ziel einer technikoffenen Entwicklung erfolgreich dafür ein, neben der Verankerung von qualifizierter Signatur, De-Mail und Nutzung des neuen Personalausweises als Schriftformersatz im neuen § 3a Abs. 4 VwVfG auch „sonstige sichere Verfahren" zu verankern, „die durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates festgelegt werden, welche den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes sowie die Barrierefreiheit gewährleisten".

Die Anpassung, Weiterentwicklung und Qualitätssicherung der IT-Instrumente

[13] Hierzu *Heckmann/Albrecht*, ZRP 2013, 42 ff.

leistet die private Internetwirtschaft mit ihren Softwareherstellern und IT-Dienstleistern. Auch wenn für sie kommerzielle Interessen im Vordergrund stehen mögen, steht sie auch in einer gesamtgesellschaftlichen Verantwortung, für IT-Innovationen „im Großen“ zu sorgen. Hinzu kommt eine konkrete Update-Verantwortung. Auch wenn sich eine Produkthaftung durch Obsoleszenz nicht einfach begründen lässt, können sich Unternehmen ihrer Verantwortung für eine nachhaltige IT-Entwicklung nicht ohne weiteres entziehen.

2. Kooperationsobliegenheiten und Interoperabilität der IT-Systeme

These 11: Der Aufbau und Betrieb komplexer IT-Systeme, an dem die öffentliche Hand und private Unternehmen mitwirken, fordert eine Kooperation der Beteiligten, insbesondere zur Herstellung von Interoperabilität der Systemkomponenten, auf die nur bestimmte Akteure Zugriff haben. Grundsätzlich enthält die Bereitstellung von IT-Komponenten das Versprechen an die Nutzer, diese Komponenten innerhalb des IT-Systems, für das sie geschaffen wurden, in sachlicher und zeitlicher Hinsicht adäquat einsetzen zu können. Unabhängig von konkreten vertraglichen Garantien und Gewährleistungsansprüchen besteht die Obliegenheit der Hersteller und Dienstleister, ihre Leistungen in den Kontext der heterogenen IT-Systeme zu stellen. Das betrifft sowohl die öffentlich-rechtlichen als auch die privaten Anbieter.

3. IT-Sicherheit zur gesamten Hand

These 12: IT-Sicherheit kann nur zur gesamten Hand gewährleistet werden. Insoweit müssen Staat, Unternehmen und Privatpersonen entsprechend ihren Kompetenzen, Fähigkeiten und Ressourcen zusammenwirken, um Gefahren entgegenzuwirken, die auch durch diese als Akteure in verbundenen Systemen mitverursacht werden[14]. Der Staat selbst ist nicht in der Lage, eigene Hard- und Softwarelösungen herzustellen, die der dynamischen Entwicklung der IT und damit auch den Gefährdungen der IT-Sicherheit ausreichend Rechnung tragen. Ihm fehlen zumeist die Möglichkeiten einer agilen Entwicklung. So scheiterte vor 10 Jahren zunächst das Bemühen des Bundesministeriums des Innern, die damals bei den Politikern und Bundesbediensteten beliebten Blackberrys durch eine besonders sichere Eigenentwicklung für rund 1000 Topleute in Regierung und Ministerien abzulösen („Top 1000“). Spä-

[14]Siehe S. 4 des BSI Berichts zur Lage der IT-Sicherheit 2015 (Vorwort de Maizière): „Weder Staat noch Wirtschaft können die IT-Sicherheit in unserem Land allein erreichen. Jeder muss seinen Teil dazu beitragen. Wir müssen daher die Zusammenarbeit zwischen Wirtschaft und Staat intensivieren und auch neue Formen der Zusammenarbeit finden.“ Weiter S. 15: „Die Verantwortung für die digitale Sicherheit tragen alle Beteiligten: Nutzer, Management in Unternehmen und Behörden, Hersteller, Provider und Dienstleister. Für ein hohes Sicherheitsniveau der IT in Unternehmen trägt das Management entscheidende Verantwortung.“ S. 41: „hat jedoch auch der Staat im Rahmen der Daseinsvorsorge eine Fürsorgepflicht gegenüber seinen Bürgern und somit die Gewährleistungsverantwortung für die Kritischen Infrastrukturen. Dem Staat und den Betreibern Kritischer Infrastrukturen kommt somit eine besondere Verantwortung zu, die Anlagen vor Ausfällen und Beeinträchtigungen zu schützen“.

ter wurde eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlene Lösung zur sicheren mobilen Kommunikation (SiMKo) aufgrund eines Vertrages mit T-Systems entwickelt und in der Bundesregierung verteilt. Oft zeigen aber solche Auftragslösungen mit engmaschigen auf IT-Sicherheit ausgerichteten Vorgaben, dass letztlich aufgrund unzureichenden Anwendungskomforts die Akzeptanz leidet.

IV. Staatliche IT-Selbstversorgung zwischen zulässigem Monopol und unzulässiger Wettbewerbsverzerrung

These 13: Herstellung, Nutzung und Regulierung von IT müssen in jenem Maße erfolgen, dass öffentliche Aufgaben effizient und rechtskonform erledigt werden, der Staat seiner Verantwortung für die Sicherheit und Funktionsfähigkeit der IT-Systeme gerecht wird und zugleich der Notwendigkeit und Verantwortung privatwirtschaftlicher Bereitstellung und Weiterentwicklung von Software und Services Rechnung trägt. Weder darf der Staat das Übermaßverbot durch unnötige Marktbeeinflussung noch das Untermaßverbot durch sorglose Zurückhaltung verletzen. Gerade eine solche Sorglosigkeit findet sich aber oft in der Verwaltungspraxis, indem der Herausforderung wenig Priorität beigemessen wird, eigenes kompetentes Personal für die IT-Steuerungsaufgabe vorzuhalten. Die Verwaltung weiß dann nicht, was sie will oder auch nur wollen soll. Behörden sind oft nicht mit dem erforderlichen Fachpersonal ausgestattet, das erforderlich wäre, beauftragte externe Dienstleister wirkungsvoll zu steuern. Oft fehlt es sogar am behördeninternen Knowhow zur rechtskonformen und auf den Bedarf ausgerichteten passgenauen Ausschreibung. Auch insoweit bedient man sich dann externer Berater und kann sich doch nicht auf eine marktneutrale Beratung verlassen. Oder man wird von der Expertise eines Unternehmensberaters gleich so abhängig, dass man ihn zum (kommissarischen) Behördenchef ernennt.[15] Auf Bundesebene stellt seit 2002 das Bundesverwaltungsamt den Bundesbehörden und institutionellen Zuwendungsempfängern Beratungsdienstleistungen (Projektmanagement, Prozess-, IT- und Organisationsberatung) im Drei-Partner-Modell zur Verfügung: Der „Kunde“ - die Bundesbehörde - bestellt Leistungen beim Bundesverwaltungsamt, das als zweiter Partner bei der Feststellung des Bedarfs und der Zieldefinition berät und den formellen Abwicklungsprozess übernimmt und den dritten Partner beauftragt, der aus der Reihe von externen Unternehmen ausgewählt wird, die mit dem Bundesverwaltungsamt

[15] So arbeitet seit dem 2015 arbeitet das Berliner Landesamt für Gesundheit und Soziales (Lageso) bereits mit der Unternehmensberatung McKinsey zusammen, um z.B. auch die Möglichkeiten einer Digitalisierung der Abläufe im Umgang mit den Flüchtlingen zu prüfen. Nun wurde einer der Berater (Sebastian Muschter) kommissarisch an die Spitze der Behörde berufen.

nach Ausschreibung und einer Zuverlässigkeitsprüfung Rahmenverträge abgeschlossen haben. Zwar wird das „Drei-Partner-Modell“ des Bundesverwaltungsamts als Erfolgsgeschichte beschrieben, da damit mehr als 1.000 Projekte, darunter „die Neuorganisation der IT-Steuerung Bund, die fristgerechte Einführung des neuen Personalausweises, die Entwicklung innovativer Dienste wie D115 und De-Mail“ zur Zufriedenheit der Kunden „erfolgreich durchgeführt“ worden seien.[16] Die Behörden könnten sich so auf ihre Kernaufgaben konzentrieren. Doch gerade an dieser Bewertung sind Zweifel angebracht, denn diese Dienste haben in Deutschland bei Weitem nicht die Verbreitung erfahren, die offenbar der Bundesregierung vorschwebte. So wurden zwar Regelungen zum Schriftformersatz im E-Government-Gesetz des Bundes verankert: Versand eines elektronischen Dokuments mit einer De-Mail, Nutzung des Identitätsnachweises des neuen Personalausweises u.a.m. Zudem wurde der Bund verpflichtet, flächendeckend De-Mail-Zugänge zu schaffen[17] und zum 1.1.2015 die nPA-Identifizierung[18] flächendeckend anzubieten (§ 2 EGovG). Bislang wurden die entsprechenden Infrastrukturen unterdessen (noch) nicht vollständig geschaffen. Auch sind nur wenige Länder (Sachsen, Bayern und Baden-Württemberg) der Anregung des Bundes gefolgt, entsprechende Bestimmungen in Landes-E-Government-Gesetze aufzunehmen.

Auch die Behörden der Länder behelfen sich angesichts des Mangels an einer ausreichenden Anzahl eigener Fachkräfte der Unternehmensberatungen, die oft über Rahmenverträge für viele Jahre gebunden werden, aus denen dann einzelne Beratungsleistungen abgerufen werden.

Rahmenverträge schaffen für die Behörden Stabilität und vermeiden häufige Ausschreibungen, sind aber zuweilen einem Wettbewerb gerade auch der kleinen mittelständischen Unternehmen abträglich.

1. Marktregulierung: Grundrechtseingriff und Gesetzesvorbehalt

These 14: Der Vertrieb einer sog. Behördensoftware (als einer von der öffentlichen Hand entwickelten oder von ihr in Auftrag gegebenen Software, deren Verbreitung in Konkurrenz zu vorhandener Software tritt) bedeutet einen faktischen Grundrechtseingriff in die Berufsfreiheit am Markt agierender Softwarehersteller bzw. IT-Dienstleister. Dieser Grundrechtseingriff bedarf einer gesetzlichen Grundlage, aus der sich Art und Umfang einer etwaigen Marktregulierung demokratisch legitimieren lassen. Auf welcher Stufe (im Sinne der Drei-Stufen-Theorie des Bundesverfassungsgerichts) die Rechtfertigungsanforderungen dieses

[16] Einsehbar unter Internetlinkverzeichnis Nr. 5.
[17] § 2 Abs. 2 EGovG ; diese Pflicht tritt gem. Art. 31 Abs. 4 Satz 1 G v. 25.7.2013 ein Kalenderjahr nach Aufnahme des Betriebes des zentral für die Bundesverwaltung angebotenen IT-Verfahrens, über das De-Mail-Dienste für Bundesbehörden angeboten werden, in Kraft. Dies bedeutet eine Eröffnung nunmehr bis zum 24. März 2016.
[18] § 2 Abs. 3 EGovG i.V. mit Art. 31 Abs.3.G, v.25.7. 2013.

Eingriffs anzusiedeln sind, hängt von dem Vertriebsmodell für die Behördensoftware ab: Bei einem echten oder unechten Verwaltungsmonopol kann ein Eingriff in die Berufsausübungsfreiheit mit objektiv berufsregelnder Tendenz vorliegen. Dann bedarf es eines wichtigen Gemeinschaftsgutes (z.B. nationale Sicherheitsinteressen bei der IT-Entwicklung im Verteidigungsbereich), für dessen Schutz das Monopol begründet wird. Unter marktgerechten Wettbewerbsbedingungen genügen hingegen vernünftige Erwägungen des Gemeinwohls. Ein legitimer Zweck kann je nachdem bereits in der Realisierung einer sachlichen E-Government-Strategie liegen oder erst durch die Beseitigung von Missständen und auch durch hohe Sicherheitsanforderungen oder vergleichbare Schutzgüter begründet sein. Neben der Eignung (Zwecktauglichkeit) der Softwareverbreitung setzt die verfassungsrechtliche Rechtfertigung des Eingriffs deren Erforderlichkeit voraus. Als milderes Mittel ist besonders die Möglichkeit der staatlichen Vorgabe von Sicherheits-, Interoperabilitäts- und Qualitätsstandards (einschließlich der Forderung nach Zertifizierung) zu prüfen. In diese Kategorie fallen auch technische Richtlinien des BSI, in denen z.B. der „Stand der Technik“ festgehalten wird[19]. Im Rahmen der Verhältnismäßigkeit i.e.S. sind die Auswirkungen auf den bestehenden Markt der E-Government-Fachanwendungen auch unter dem Aspekt der Innovationshemmung und nachhaltiger Aufgabenerfüllung zu untersuchen. [20]

Von der direkten Erstellung einer Software durch Behördenmitarbeiter selbst unterscheidet sich nur geringfügig die Erstellung einer Software aufgrund einer Ausschreibung, die durch enge Vorgaben dafür sorgt, dass Marktprodukte nicht konkurrenzfähig sind. Auch die Ausschreibung einer Weiterentwicklung eines im staatlichen Auftrag entstandenen Prototyps täuscht über die langfristige Kostenentwicklung hinweg und nimmt Herstellern von Standardsoftware die Chance, bei der Beauftragung zum Zuge zu kommen.

Als milderes Mittel gegenüber einer „Behördensoftware“ bietet sich auch an, auf dem Markt erhältliche Software durch sogenanntes Customizing an die Bedürfnisse eines Kunden (einer Behörde) anzupassen. Denn „von der Stange“ erhält-

[19] Siehe oben: BSI TR-03138 Ersetzendes Scannen (RESISCAN)

[20] So wird teilweise dem BSI vorgeworfen, es habe durch die technische Richtlinie RESISCAN weitgehende Pflichten zum Signieren und Nachsignieren festgehalten und in den Markt eingegriffen, indem damit der Branche der Anbieter von Dokumentenmanagement- und Scanning-Lösungen die Möglichkeit geboten wurde, mehr Komponenten und Services zu verkaufen und mit dem Kunden eine langfristige Bindung einzugehen. Wer einmal mit dem Signieren und regelmäßigen Nachsignieren angefangen habe, komme davon kaum noch los, es sei denn, er ignoriere die Beweiswerterhaltungsargumente. Andererseits ist hier eine gewisse Orientierungshilfe unerlässlich, um Rechtsunsicherheiten beim Medienbruch zu vermeiden; denn ohne eine solche Sicherheit auch im Hinblick auf den fortbestehenden Beweiswert besteht die Gefahr, dass das Papier neben den elektronischen Dateien aufbewahrt wird und so Effizienzgewinne der Digitalisierung nicht realisiert werden können. Dazu *Bernhardt*, NJW 2015, 2776.

liche Serienprodukte passen zumeist nicht hundertprozentig zu den Anforderungen der konkreten Behörden bzw. Gerichte. Um zu verhindern, dass durch ein solches Customizing neue Abhängigkeiten von Behörden an Produktentwicklungen spezieller Hersteller entstehen, sollten durch staatliche Vorgaben insbesondere Interoperabilitätsstandards gesetzt werden.

So wurde es z.B. versäumt, frühzeitig im E-Justice-Rat Mindeststandards für offene Schnittstellen für elektronische Gerichtsaktensysteme festzulegen, die verhindern, dass der (elektronische) Aktentransfer zwischen Gerichten aus unterschiedlichen Entwicklungsverbünden behindert wird. [21] Das Fehlen solcher Standards kann auch dazu führen, dass ein Produktwechsel ohne erhebliche neue finanzielle und personelle Ressourcen bei größeren IT-Systemen kaum mehr möglich ist. Mittlerweile beschäftigen sich Arbeitsgruppen der Bund-Länder-Kommission für Informationstechnik in der Justiz, die dem E-Justice-Rat zuarbeitet, mit der Schnittstellenfrage.

2. Marktöffnung: Vergaberechtliche Bindungen

These 15: In vergaberechtlicher Hinsicht sind – je nach Vertriebsmodell – die Grenzen zulässiger Inhouse-Vergabe oder die formalen Ausschreibungsbedingungen zu klären. Vor allem muss eine Diskriminierung kleinerer oder mittlerer Unternehmen vermieden werden, indem diesen zum Beispiel eine Teilnahme an einer Ausschreibung im Rahmen einer Vergabe nach Losen ermöglicht wird.

Schwierig ist in der Praxis oft die Entscheidung, welche Anforderungen an eine neue Software zu stellen sind. Ein zu stark modular aufgebautes System mit IT-Lösungen verschiedener Anbieter kann Interoperabilitätsprobleme erzeugen, die nur mit erheblichem Aufwand zu lösen sind. Umgekehrt ist aber auch eine Komplettlösung für ganze „Behördenfamilien“ dann nicht zwingend, wenn ein modular zusammengestelltes IT-System mit Lösungen verschiedener Anbieter die angestrebten Ziele genauso oder sogar noch besser erfüllen kann. Zentrale, eine ganze Behördenlandschaft erfassende Lösungen sind zuweilen innovationsfeindlich, weil neue Lösungen in einem Teilsystem oft die Änderung des Gesamtsystems bedingen. Änderungen des Gesamtsystems sind dann oft mit hohen Kosten verbunden, was wiederum eher die Behörde dazu verleitet, von Innovationen abzusehen. Hier ist im Hinblick auf die Marktsituation und die mit der Software anzustrebenden Ziele genau abzuwägen, welche Lösungen langfristig finanziell am günstigsten sind. Eingriffe in den Markt sind möglichst zu vermeiden, wenn die vom Markt gebotenen Bedingungen gegenüber den unmittelbar durch Behörden veranlassten Lösungen zumindest gleichwertig sind.

[21] *Bernhardt*, NJW 2015, 2778.

Eingriffe in den Markt wären zum Beispiel kaum als angemessen begründbar, wenn ein von der öffentlichen Hand getragenes Institut mit hohen Kosten eine eigene Software entwickelt, die dann „kostenfrei“ Kommunen zur Verfügung gestellt wird, obwohl diese Software im Wesentliche nur das leisten kann, was die privaten Anbieter schon seit Jahren bieten oder bereits existierenden privaten Softwarelösungen nachempfunden ist. Es mag aus der Sicht von Kommunen nachvollziehbar sein, wenn sie eine solche „kostenlose“ Software dann einer Lösung eines privaten Anbieters vorziehen, auch wenn der einzige Vorteil für die Kommunen darin besteht, für diese Leistung nicht bezahlen zu müssen. Unter dem Grundsatz digitaler Gewaltenteilung wäre es für ein solches Institut eher angemessen, klare Vorgaben für eine Lösung zu formulieren und die Leistungen auszuschreiben. Denn aus der Sicht des Steuerzahlers erwächst keine Ersparnis, wenn ein hoher Aufwand für die Erstellung einer staatlichen Softwarelösung und eventuelle kontinuierliche Fortentwicklungen finanziert werden muss. Für den Steuerzahler ist es auch irrelevant, ob er über die Steuerpflicht die Kommune oder den Bund finanziert.

Auch ist kritisch zu hinterfragen, ob die Vereinbarung der Finanzminister der Länder im Einvernehmen mit dem Bundesminister der Finanzen vom Juni 2005 über die Grundlagen zur Entwicklung einheitlicher Software für das Besteuerungsverfahren in dem Vorhaben **KONSENS** (die **Ko**ordinierte **n**eue **S**oftware-**En**twicklung der **S**teuerverwaltung) bzw. das am 1.1.2007 in Kraft getretene Verwaltungsabkommen von Bund und Ländern KONSENS auf Dauer die privatwirtschaftliche Entwicklung von Software in diesem Bereich ersetzen darf bzw. sollte. Die Kosten für die Entwicklung und den Betrieb von Behördensoftware in der Steuerverwaltung sind beträchtlich (jährlich im hohen zweistelligen Millionenbereich; ca 500 Beschäftigte des öffentlichen Dienstes werden hier tätig). Alternativ wäre daran zu denken, hier der Privatwirtschaft über die bisherigen Kooperationen (Dataport, Software AG) hinaus Raum zu geben und Probleme einer zu vielfältigen und heterogenen IT-Landschaft in den Steuerverwaltungen der Länder mit Standardvorgaben zu begegnen.

Eigenentwicklungen von Behördensoftware sind auch häufig im Bereich der von Polizei- und Umweltbehörden genutzten Informationstechnologie vorzufinden. Solche Eigenentwicklungen werden oft damit gerechtfertigt, dass die Anforderungen an die IT so spezifisch sind, dass nur Behördenmitarbeiter sie erfüllen könnten. Dies überzeugt nicht. Eigenentwicklungen binden oft in bedeutsamem Ausmaß personelle Ressourcen in den Behörden. Daraus ergibt sich auch ein erheblicher Fortbildungsbedarf für die betreffenden Mitarbeiter. Dabei könnte gerade externes Knowhow dafür sorgen, dass neueste Erkenntnisse und Marktentwicklungen direkt in die Soft-

wareentwicklung einfließen. So gibt es durchaus auf dem Markt erhältliche Software, die mit geringen Anpassungen (Customizing) an die Bedürfnisse des Aufraggebers kostengünstig zum Einsatz gelangen könnte.

Bei der Ausschreibung von Dienstleistungen zur Einführung neuer IT-Systeme ist z.B. zu prüfen, ob wirklich alle Mitarbeiter aller Behörden einer Gebietskörperschaft gleichzeitig in das neue System eingeführt werden müssen oder eine Abschichtung nach Behörden und Zeiträumen möglich ist, auch um kleineren und mittleren Unternehmen mit begrenzter Mitarbeiterzahl eine realistische Chance für einen Ausschreibungserfolg zu geben.

Die IT-Beschaffung des Staates ist nach den Grundsätzen zu den Leistungsbeschreibungen im Vergaberecht produktneutral, d.h. hersteller-, lieferanten- und vertriebsneutral zu halten. Etwas anderes kann nur dann gelten, wenn für bestimmte Technologievorgaben ein sachlich begründeter Bedarf besteht, der nur und gerade durch die vorgenommenen Spezifikationen zu erfüllen ist. Sachliche Gründe sind vor allem solche Argumente, die mit Nutzbarkeit und Wirtschaftlichkeit der Produkte in engem Zusammenhang stehen. Dazu zählen insbesondere die Interoperabilität der IT-Produkte, die gesteigerten Anforderungen des elektronischen Verwaltungsverfahrens an die IT-Sicherheit, die übergreifenden Anpassungs- und Wartungsmöglichkeiten, sowie die Nachhaltigkeit der Produkt- und Systementscheidung für die öffentliche Verwaltung, zuweilen auch über die Grenzen der Kommunen oder des Bundeslandes hinaus.

3. Marktverhalten: Unlauterer Wettbewerb

These 16: In wettbewerbsrechtlicher Hinsicht besteht zwar kein Schutz vor konkurrierender „Behördensoftware“. Der Staat ist aber – soweit kein zulässiges Verwaltungsmonopol errichtet wird – zu lauterem Verhalten gegenüber privaten Marktteilnehmern verpflichtet. Dazu zählt zum Beispiel Transparenz der Angebotssituation und die Unterlassung irreführender Informationen an die Kunden. Aus dem Verbot unlauteren Wettbewerbs in Verbindung mit dem Gleichbehandlungsgrundsatz folgt auch die Pflicht des Staates, alle Marktteilnehmer (also nicht nur einen etwaigen privaten Projektpartner) zeitgleich und in gleichem Umfang mit solchen (z.B. Schnittstellen-) Informationen zu versorgen, die für den sachgemäßen Einsatz der E-Government-Fachanwendung erforderlich sind. Unzulässig wäre es auch, die staatliche Machtstellung ausschließlich zur Arbeitsplatzsicherung eigener Behördenbeschäftigter zu nutzen und einen existierenden privaten Anbietermarkt für IT-Systeme aus dem Markt zu drängen.

Rechenzentren wurden vor Jahrzehnten auf kommunaler, Landes- und Bundesebene gegründet, um jeweils einer Vielzahl von Kommunen oder staatlichen

Behörden zentrale IT-Dienstleistungen anzubieten. Waren anfangs noch exorbitante Hardwareanforderungen bestimmend für die Konstruktion einer zentralen Infrastruktur für die Kommunen und staatlichen Behörden, so kam es angesichts einer dramatischen Veränderung der Hardwareinfrastruktur zu einem Bedeutungswandel der Rechenzentren hin zu zentralen Dienstleistern für die Entwicklung, Einführung, Betrieb und Pflege von IT-Verfahren und zur Datenhaltung. Teilweise wurden an diese Dienstleister (meist als Anstalten des öffentlichen Rechts oder als Staatsbetriebe organisiert) auch zentrale IT-Steuerungs- und Beschaffungsaufgaben delegiert, die zum Kern staatlicher Aufgabenwahrnehmung gehören. Um Kapazitäten auszulasten und ohnehin vorhandenes Personal sinnvoll beschäftigen zu können, wurden diese Dienstleister auch außerhalb der vorherigen kommunalen oder Landes-Zuständigkeitsgrenzen tätig und weiteten insoweit ihren Aktionsradius aus.

Gleichzeitig gibt es mittlerweile einen durchaus wachsenden privatwirtschaftlich geprägten Markt für Dienstleistungen von Rechenzentren, den die Kommunen und staatlichen Behörden für ihre Zwecke nutzen könnten.

Ein lauteres Verhalten des Staates würde hier gebieten, diesem privaten Markt zukünftig bei der Vergabe von Dienstleistungen faire Chancen zu lassen – notfalls durch Trennung von Aufgaben, die beim Staat/bei der Kommune verbleiben müssten (Steuerungs- und Beschaffungsmaßnahmen) von den Rechenzentrumsdienstleistungen sowie von der IT-Entwicklung, Einführung, Betrieb und Pflege von IT-Verfahren und der Datenhaltung.

Unangemessenes Besitzstandsdenken der Behörden und ihrer Mitarbeiter und die Sorge des Verlustes eines direkten Zugriffs auf IT-Dienstleistungen verhindern aber hier oft einen durchgreifenden Wandel hin zur gebotenen Marktöffnung.

Zuweilen wird auch die Sorge geäußert, durch Privatisierung des Rechenzentrumsbetriebes im Wege des Outsourcings und Vergabe an ein großes privatwirtschaftliches Unternehmen gerate der Staat in eine neue Abhängigkeit von eben diesem privaten Dienstleister, weil ein späterer Wechsel des Dienstleisters mit hohen finanziellen Risiken (Knowhow-Verlust, Migrationsaufwand) verbunden sein könnte. Um solche Risiken zu vermeiden, kommt es darauf an, für die beim Staat verbleibende Steuerungskompetenz hinreichende Ressourcen zu behalten. Im Übrigen ist durch die Vertragsgestaltung mit dem privaten Dienstleister dafür Sorge zu tragen, dass klare Pflichten zu einem ordnungsgemäßen Betriebsübergang auf ein Nachfolgeunternehmen vertraglich fixiert werden.

Ebenso mag die Organisationsprivatisierung – wie die Organisation des DVZ Mecklenburg-Vorpommern als GmbH mit dem Land als Gesellschafter – zeigen, dass sie gegenüber öffentlich-rechtlichen Organisationsformen (Staatsbetrieb, Anstalten des öffentlichen Rechts) die Vor-

teile des privatwirtschaftlichen Marktes besser nutzen und IT-Dienstleistungen in hochmoderner Form präsentieren kann.

4. Marktverantwortung: Idee einer IT-Marktverträglichkeitsprüfung

These 17: Der Staat hat eine Marktverantwortung für die Balance zwischen Sicherheit (Safety, Security) einerseits und freiem Wettbewerb andererseits. Stärker als in anderen Wirtschaftsbereichen besteht im Prozess der Digitalisierung sowohl die Notwendigkeit politischer Führung als auch die Notwendigkeit unternehmerischer Freiheit.

Dem wird die öffentliche Hand in ihrem Marktverhalten bislang zu wenig gerecht. Zwar gibt es normative Ansätze wie die Etablierung eines IT-Planungsrates durch Art. 91c GG und den IT-Staatsvertrag. In der Praxis entspricht dieser jedoch nicht den in ihn gesetzten Erwartungen. Er ist mangels Unterbaus bzw. einer operativen Ebene und mangels adäquater Ressourcen praktisch nicht fähig, seine Aufgaben und Kompetenzen aus dem IT-Staatsvertrag wahrzunehmen. Bewusst wurde der IT-Planungsrat als hochrangiges Entscheidergremium eingerichtet, in dem Bund und Länder in der Regel durch ihre für IT zuständigen Staatssekretäre bzw. CIOs vertreten sein sollten. Die Tagesordnung des in der Regel viermal im Jahr tagenden IT-Planungsrats ist jedoch oft mit Projektsteuerungsfragen und Finanzangelegenheiten überfrachtet, so dass die Herausforderungen der IT-Steuerung und Standardsetzung nicht bewältigt werden. Hinzukommt ein vom IT-Staatsvertrag vorgegebenes Verfahren zur Entscheidungsfindung, das – wegen des Einstimmigkeitsprinzips bzw. des Prinzips qualifizierter Mehrheiten für Standardisierungsentscheidungen – den Langsamsten im Entscheidungsprozess privilegiert und so bisher nur selten Entscheidungen von erheblichem Gewicht ermöglicht hat. In der nun bereits sechsjährigen Geschichte des IT-Planungsrats kam es bisher nur zu zwei Standardisierungsentscheidungen. Um die Schlagkraft des IT-Planungsrats zu erhöhen, wäre es sachgerecht, den IT-Staatsvertrag zu ändern und für zahlreiche Kompetenzfelder des IT-Planungsrats Mehrheitsentscheidungen zu ermöglichen. So sind die Rahmenbedingungen dafür zu schaffen, dass der Staat seine Koordinierungsaufgabe wahrnehmen und zumindest strategische Leitlinien vorgeben und konkrete Projekte in den Behörden anschieben kann. Andernfalls lässt sich der für Deutschland bekannte und dem Gemeinwohl abträgliche digitalen Flickenteppich nicht beseitigen. Auch das gefährdet die Konsistenz und Nachhaltigkeit der IT-Systeme, genauso wie zu detailintensive Festlegungen durch den Staat, wenn sie die Interessen, Kapazitäten, Kompetenzen und Potentiale der IT-Wirtschaft vernachlässigen. Wie gesehen agiert der Staat zum Beispiel durch eigene Softwareentwicklung oft in Bereichen, in denen der IT-Markt die notwendigen

Lösungen und Produkte selbst bereitstellen könnte.

Vor diesem Hintergrund bietet sich eine IT-Marktverträglichkeitsprüfung an. Sieht man in Art. 91c GG mehr als nur eine Kompetenznorm, sondern – wie es der IT-Beauftragte der Bundesregierung auf seiner Webseite formuliert – als Auftrag für den IT-Planungsrat im Sinne einer verbindlichen Zusammenarbeit von Bund, Ländern und Kommunen in der IT und im E-Government, dann begründet ein solcher Auftrag zur Zusammenarbeit in Verbindung mit der im IT-Grundrecht verfassungsrechtlich verankerten staatlichen Schutzpflicht zur Gewährleistung der Sicherheit und Funktionsfähigkeit informationstechnischer Systeme und der aus Art. 12 GG folgenden Pflicht zur Marktorientierung in Verbindung mit dem Zurückhaltungsgebot aus Wettbewerbs- und Haushaltsrecht auch die Pflicht zur Entwicklung und Veröffentlichung einer marktorientierten IT-Strategie. Aus dieser muss ersichtlich sein, welche IT zu welchem öffentlichen Zweck gebraucht wird und wer diese entwickeln und bereitstellen soll. Monopole bedürfen einer besonderen sachlichen Rechtfertigung und gesetzlichen Grundlage. Dabei sind Aspekte eines fairen Wettbewerbs, rechtskonformer IT-Beschaffung und wirtschaftlicher Haushaltsführung zu berücksichtigen.

Die aus dem geltenden Kommunalwirtschaftsrecht bekannten Grundsätze (vgl. Art. 95 BayGemO: *Gemeindliche Unternehmen dürfen keine wesentliche Schädigung und keine Aufsaugung selbständiger Betriebe in ... Handel, Gewerbe und Industrie bewirken.*) sind auf die wirtschaftliche Betätigung aller juristischer Personen des öffentlichen Rechts im Hinblick auf den IT-Markt anzuwenden. Auch Art. 106 AEUV bekräftigt den Wettbewerbsgedanken, dem auch öffentliche Unternehmen unterliegen.

In ähnlicher Weise sieht § 2b UStG-E eine Ausnahme von der generellen Umsatzsteuerbefreiung juristischer Personen des Öffentlichen Rechts vor, *sofern eine Behandlung als Nichtunternehmer zu größeren Wettbewerbsverzerrungen führen würde.* Das bedeutet zwar nicht, dass juristische Personen des Öffentlichen Rechts stets als Unternehmen zu behandeln sind, die der Umsatzsteuerpflicht unterliegen. Im Einzelfall ist jedoch zu prüfen, ob die privilegierte Stellung solcher staatlicher Unternehmen im IT-Markt aus wettbewerbsrechtlichen Gründen eine Gleichbehandlung auch in umsatzsteuerlicher Hinsicht erfordert. Dies schließt unmittelbar an die Leitentscheidungen von EuGH (2008) und BFH (2011) an, wonach keine Umsatzsteuerbefreiung bei größeren Wettbewerbsverzerrungen vorkommen dürfe. Auch diese Rechtsprechung trägt zur Konturierung einer „digitalen Gewaltenteilung“ bei.

Dass eine Verträglichkeitsprüfung staatlich festgelegter technischer Spezifikationen anhand übergeordneter Grundsätze durchaus auch kein Fremdkörper in der Rechtsordnung sein muss, zeigt die

durch die Richtlinie (EU) 2015/1535 ausgelöste Notifizierungspflicht, die Beeinträchtigungen des freien Warenverkehrs und auch z.B. des freien Verkehrs von Diensten der Informationsgesellschaft verhindern soll. Demnach müssen die Mitgliedstaaten die Kommission über jeden Entwurf einer technischen Vorschrift vor deren Erlass unterrichten (Notifizierungspflicht).

V. Fazit: Leitidee einer „Digitalen Gewaltenteilung“ und Leitbild des kooperativen, vertrauenswürdigen und nachhaltigen IT-Staates

These 18: Die Leitidee einer „Digitalen Gewaltenteilung“ überträgt den Gedanken von „checks and balances“ auf die Machtverteilung bei der IT-Steuerung. In Zeiten globaler Digitalisierung und ihrer Auswirkungen auf Steuerung und Kontrolle („Code is law“) sollte sich Gewaltenteilung nicht auf die staatlichen Gewalten der Gesetzgebung, Verwaltung und Rechtsprechung beschränken. Vielmehr sind die Kompetenzen und Kräfte der Privatwirtschaft mit ihren IT-Unternehmen, Softwareentwicklern und anderen Innovatoren in dieses Gefüge einzubeziehen. Das betrifft gleichermaßen Teilhabe als auch Machtbegrenzung bei der IT-Steuerung.

Damit soll auch der problematischen Tendenz entgegenwirkt werden, die sich aus der latent grenzenlosen Organisationshoheit und politischen Gestaltungsmacht des Staates ergibt. Vernachlässigt dieser in Bezug auf IT-Entwicklung und IT-Einsatz die Interessen, Kapazitäten, Kompetenzen und Potentiale der IT-Wirtschaft, entsteht eine kaum überschaubare Gefährdungslage für die Konsistenz und Nachhaltigkeit der IT-Systeme und ihrer Komponenten. So werden oft IT-Lösungen staatlicherseits veranlasst oder realisiert, die am Markt „nicht ankommen“, weil sie die Markentwicklungen missachten, oder unverhältnismäßig hohe Kosten verursachen, weil der Aufwand zur Erstellung spezifischer Lösungen falsch eingeschätzt wird. Staatliche Organisationen sind oft gar nicht in der Lage, die für das Bestehen am Markt erforderliche Agilität bei der Entwicklung von IT-Systemen zu zeigen.

Diese Einschränkung der staatlichen Gestaltungsmacht lässt sich im Kontext der Digitalisierung mit Blick auf das Demokratieprinzip rechtfertigen. Gesetzgeber und Verwaltung haben kein Mandat, die übergreifenden und marktrelevanten IT-Strukturen faktisch änderungsfest über eine Legislaturperiode hinweg einseitig zu bestimmen.

Das aus diesen Erwägungen folgende Zurückhaltungsgebot des Staates gegenüber den privaten Akteuren im IT-Markt lässt sich als „technical self-restraint“ der öffentlichen Hand bezeichnen. Es erinnert an den Grundsatz des judicial self-restraint. Diesen hat sich das Bundesverfassungsgericht in seiner Entscheidung zum Grundlagenvertrag auferlegt. Er be-

deutet in den Worten der Karlsruher Richter nicht eine „Verkürzung oder Abschwächung seiner Kompetenz, sondern den Verzicht ‚Politik zu treiben', d. h., in den von der Verfassung geschaffen und begrenzten Raum freier politischer Gestaltung einzugreifen. Er zielt also darauf ab, den von der Verfassung für die anderen Verfassungsorgane garantierten Raum freier politischer Gestaltung offen zu halten".[22]

Damit soll andererseits nicht die wichtige Standardisierungsrolle, die vor allem dem IT-Planungsrat und E-Justice-Rat zukommen, in Zweifel gezogen werden, im Gegenteil: Standards zur Sicherung von IT-Sicherheit, Qualität, Interoperabilität und Nachhaltigkeit sind erforderlich; staatliche Untätigkeit in diesem Bereich führt zu Abhängigkeiten von bestimmten Dienstleistern und erheblichen finanziellen Lasten. Solche Standards sind aber nicht gleichzusetzen mit einer detaillierten technischen Festlegung.

So wie es beim judicial self-restraint um das Verhältnis von Verfassungsrechtsschutz und Politik geht, beschreibt der Grundsatz des technical self-restraint das Verhältnis von staatlicher Organisationshoheit und IT-Markt. Der Staat soll sich bei seinen IT-Organisationsentscheidungen im Interesse von Innovation und Nachhaltigkeit im IT-Markt zurückhalten. Um eine konsistente technical self-restraint-Praxis zu begründen, sollten entsprechende Leitlinien erarbeitet werden, die staatliches Handeln auf verschiedenen Ebenen erfassen müssen: bei der Normsetzung, bei Planungsentscheidungen des IT-Planungsrats und schließlich bei konkreten Ausschreibungen.

Das Leitbild eines kooperativen, nachhaltigen und vertrauenswürdigen IT-Staates soll helfen, die vielfältigen Unwägbarkeiten der digitalen Transformation abzufedern und die Verantwortung für die Folgen der rasanten Technologieentwicklung interessengerecht zu verteilen.

[22] BVerfG, Urt. v. 31.7.1973, BVerfGE 36, 1 (14 f.).

Internetlinkverzeichnis

1) Zu Fn. 6:
http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10_Sitzung/Kieler_Beschl%C3%BCsse_EvaKB.pdf?__blob=publicationFile&v=2

sowie

http://www.it-planungsrat.de/DE/Projekte/AbgeschlosseneProjekte/Kieler_Beschl%C3%BCsse/kieler_beschluesse.html

2) Zu Fn. 9:
http://www.emr-sb.de/tl_files/EMR-SB/content/PDF/Telekommun%20-%20Beitraege/EMR-WiM_BB_Gutachten_final_2008.pdf

3) Zu Fn. 12:
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03138/index_htm.html

4) Zu Fn. 12:
http://www.project-consult.de/ecm/in_der_diskussion/tr_03138_resiscan_ger%C3%A4t_immer_mehr_die_kritik

5) Zu Fn. 16:
http://www.egovernment-computing.de/das-drei-partner-modell-ist-eineerfolgsgeschichte-a-392596/