Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Fachbereich Rechtspflege

Voraussetzungen für die Speicherung und Verarbeitung von Justizdaten bei externen Landesdienstleistern unter Berücksichtigung von datenschutz- und verfassungsrechtlichen Aspekten

Autorin: Helene Knoll
Herausgeber/in: Prof. Dr. Anastasia Baetge, Zweitkorrektor: Prof. Roland Böttcher

Beiträge aus dem Fachbereich Rechtspflege
Nr. 01/2017
Herausgeber der Reihe: Dekan des Fachbereichs Rechtspflege

Voraussetzungen für die Speicherung und Verarbeitung von Justizdaten bei externen Landesdienstleistern unter Berücksichtigung von datenschutz- & verfassungsrechtlichen Aspekten

Diplomarbeit

zur Erlangung des Grades einer Diplom-Rechtspflegerin (FH)

im Studiengang

Rechtspflege

an der

Hochschule für Wirtschaft und Recht Berlin

vorgelegt von Helene Knoll

Erstkorrektorin:	Frau Prof. Dr. Anastasia Baetge
Zweitkorrektor:	Herr Prof. Roland Böttcher
zusätzlicher Korrektor:	Herr Bernhard Brückmann
Vorgelegt am:	31. März 2017

Inhaltsverzeichnis

Literaturverzeichnis

I. Kommentare und Lehrbücher

Friauf/Höfling (Hrsg.)	Berliner Kommentar zum Grundgesetz, Loseblattwerk mit 51. Aktualisierung 2016, Band 5.
Gola/Schomerus	Kommentar zum BDSG, 12. Auflage 2015.
Heckmann *in: Bräutigam*	IT-Outsourcing der öffentlichen Hand, IT-Outsourcing und Cloud Computing, 3. Auflage 2013.
Hoffmann-Riem u.a.	Grundlagen des Verwaltungsrechts, 2. Auflage, Band I.
Jarass/Pieroth	Grundgesetz für die Bundesrepublik Deutschland: GG, 14. Auflage 2016.
Kissel/Mayer	Gerichtsverfassungsgesetz, Kommentar, 8. Auflage 2015.
Koch	Computer-Vertragsrecht, 7. Auflage 2009.
Maunz/Dürig	Grundgesetz, 78. Auflage 2016.
von Münch/Kunig	Grundgesetz-Kommentar, 6. Auflage 2012, Band 2.

Sodan Grundgesetz, 3. Auflage 2015.

Taeger/Gabel (Hrsg.) Kommunikation und Recht BDSG, 2. Auflage 2013.

Tinnefeld/Buchner/Petri Einführung in das Datenschutzrecht, 5. Auflage 2012.

Yildirim, Nuriye Datenschutz im Electronic Government, 1. Auflage 2004.

Schild, in Roßnagel (Hrsg.) Handbuch Datenschutzrecht, 2003.

Schmidt-Bleibtreu/ Hofman/Henneke (Hrsg.) Kommentar zum Grundgesetz, GG, 13. Auflage 2014.

Söbbing, Thomas in Handbuch IT-Outsourcing: Recht, Strategien, Prozesse, IT, Steuern und Cloud Computing, 4. Auflage 2015.

II. Aufsätze

Abel, Ralf B. Die neuen BDSG-Regelungen, RDV 2009, 147-154.

Arbeitsgruppe „Zukunft" der BLK für Datenverarbeitung „Welches Maß an IT-Zentralisierung verträgt die Dritte Gewalt", JurPC Web-Dok. 202/2009.

Berlit, Uwe E-Justice – Chancen und Herausforderungen in der freiheitlichen demokratischen Gesellschaft, JurPC Web.-Dok. 171/2007.

	eJustice, eAke und Richterschaft, Betrifft Justiz 2015, 15-26.
Bertrams, Michael	Eingriff in die Unabhängigkeit der Dritten Gewalt durch Zentralisierung der IT-Organisation unter dem Dach der Exekutive, NWVBl. 2010, 209-215.
	Zentralisierung der Informationstechnik in der Landesverwaltung Nordrhein-Westfalen unter Einbeziehung der Dritten Gewalt, NWVBl. 2007, 205-211.
Böttcher, Hans-Ernst	Weg von napoleonischen und wilhelminischen Modellen! Hin zu einer demokratischen Justizverfassung, auch in Deutschland, KritV 2008, 417 ff.;
Britz, Gabriele	Von der elektronischen Verwaltung zur elektronischen Verwaltungsjustiz, DVBl 2007, 993-1000.
Frank, Christoph	Abschaffung des externen Weisungsrechts – Die Zeit ist reif, ZRP 2010, 147-149; Selbstverwaltung der Justiz: Ein Model auch für Deutschland, KritV 2008, 405 ff.
Gola, Peter/Klug, Christoph	Die Entwicklung des Datenschutzrechts im zweiten Halbjahr 2016, NJW 2017, 604-607.
Groß, Thomas	Was bedeutet Fachaufsicht, DVBl. 2002, 793-800.

Gruber, Daniel — Das Selbstverwaltungsprojekt der Dritten Gewalt, ZRP 2009, 123 f.;

Häuser, Horst — Selbstverwaltung der Gerichte: vertikal versus horizontal, KritV 2008, 410 ff.

Heckmann, Dirk — Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen – Maßstäbe für ein IT-Sicherheitsrecht, MMR 2006, 280 ff.

Held, Karlheinz — „Vernunft“ und „Besonnenheit“ am vernetzen Richterarbeitsplatz, Betrifft Justiz 2015, 27-39.

Hochschild, Udo — Von den Möglichkeiten der deutschen Exekutive zur Beeinflussung der Rechtsprechung, ZRP 2011, 65-67.

Hoffmann-Riem, Wolfgang — Mehr Selbstständigkeit für die Dritte Gewalt, DRiZ 2003, 284-291.

Kramer, Barbara — Die Selbstverwaltung der Dritten Gewalt, NJW 2009, 3079-3084.

Köbler, Ralf — eJustice: Vom langen Weg in die digitale Zukunft der Justiz, NJW 2006, 2089-2091.

Mackenroth, Geert — Qualitätsdiskussion in der Justiz – Alter Wein in neuen Schläuchen, DRiZ 2000, 301-311.

Papier, Hans-Jürgen — Zur Selbstverwaltung der Dritten Gewalt, NJW 2002, 2585-2593;

Kein radikaler Systemwechsel in der Justiz, ZRP 2009, 125.

Radke, Holger — eJustice - Aufbruch in die digitale Epoche, JurPC Web-Dok. 46/2006;

Datenhaltung und Datenadministration der Justiz und richterliche Unabhängigkeit, jM 2016, 8-13.

Roßnagel, Alexander — Die Novellen zum Datenschutzrecht – Scoring und Adresshandel, NJW 2009, 2716-2722.

Roxin, Claus — Zur Rechtsstellung der Staatsanwaltschaft damals und heute, DRiZ 1997, 109-121.

Schaffer, Wolfgang — Die Unabhängigkeit der Rechtspflege und des Richters, BayVBl 1991, 641-648.

Schäfer, Hans Christoph — Die Staatsanwaltschaft im Rechtssystem, NJW 2001, 1396-1397.

Scholz, Bernhard Joachim — IT-Standardisierung und richterliche Unabhängigkeit, DRiZ 2011, 78-81;

Neustart des Systems, DRiZ 2013, 284-285.

Schulte-Kellinghaus, Thomas — Die begrenzte Macht der Dritten Gewalt – Zur Notwendigkeit der Selbstverwaltung der Gerichte, ZRP 2008, 205;

Die Gesetzesentwürfe des Deutschen Richterbundes und der Neuen Richtervereinigung zur Selbstverwaltung der Justiz – Ein Vergleich im Überblick, KritV 2010, 256-259.

Schulz, Sönke — Gemeinschaftsrechtliche Verpflichtung zur elektronischen Verfahrensabwicklung als Perspektive zur Etablierung eines Rechtsrahmens des eGovernment, DVBl 2009, 12-21.

Sendler, Horst — Politikermeinung und richterliche Unabhängigkeit, NJW 2001, 1909-1911.

Sennekamp, Christoph — Alle Staatsgewalt geht vom Volke aus, NVwZ 2010, 213-217.

Siegel, Thorsten — IT im Grundgesetz, NVwZ 18/2009, S. 1128-1131.

Steffen, Till — Selbstverwaltung der Justiz – Möglichkeiten der politischen Umsetzung, ZRP 2008, 208-211.

Strauch, Hans-Joachim — Wandel des Rechts durch juristische Datenbanken, DVBl 2007, 1000-1007.

III. Internetquellen

https://www.edvgt.de/engagement/gemeinsame-kommission-elektronischer-rechtsverkehr/ eingesehen am 29. März 2017.

https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/it_planungsrat_1.pdf?__blob=publicationFile eingesehen am 29. März 2017.

https://www.datenschutz-grundverordnung.eu eingesehen am 29. März 2017.

https://www.janalbrecht.eu/fileadmin/material/Dokumente/DPD_consolidated_LIBE-vote-2015-12-17.pdf eingesehen am 29. März 2017.

http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2017/02/datenschutz-grundverordnung.html eingesehen am 29. März 2017.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1001.pdf?__blob=publicationFile&v=1 eingesehen am 29. März 2017.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile&v=1 eingesehen am 29. März 2017.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=1 eingesehen am 29. März 2017.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1003_ergaenzung.pdf?__blob=publicationFile&v=1 eingesehen am 29. März 2017.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf;jsessionid=59BA5E12D78BBC4088ECD70F67452D3C.2_cid091?__blob=publicationFile&v=1 eingesehen am 29. März 2017.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile&v=1 eingesehen am 29. März 2017.

http://www.cio.bund.de/SharedDocs/Publikationen/DE/Bundesbeauftragter-fuer-Informationstechnik/it_planungsrat_geschaeftsordnung_download.pdf?__blob=publicationFile eingesehen am 29. März 2017.

Abkürzungsverzeichnis

Abs.	Absatz
AJUKA	Automation der Justizkasse
AöR	Anstalt öffentlichen Rechts
Art.	Artikel
Aufl.	Auflage
AULAK	Automation des Landgerichts, der Amtsgerichte und des Kammergerichts
AUMAV	Automation des gerichtlichen Mahnverfahren
BayDSG	Bayrisches Datenschutzgesetz
BayVBl	Bayrische Verwaltungsblätter
Bd.	Band
BDSG	Bundesdatenschutzgesetz
BeLa	Berliner Landesnetz
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofs
BlnDSG	Berliner Datenschutzgesetz
BRD	Bundesrepublik Deutschland
BremDSG	Bremisches Datenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs	Bundesdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
bzw.	beziehungsweise
DRiG	Deutsches Richtergesetz
DRiZ	Deutsche Richterzeitung

DSG M-V	Landesdatenschutzgesetz Mecklenburg-Vorpommern
DSG NRW	Datenschutzgesetz Nordrhein-Westfalen
DSG-LSA	Datenschutzgesetz Sachsen-Anhalt
DVBl	Deutsches Verwaltungsblatt
EDV	elektronische Datenverarbeitung
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
engl.	englisch
ERV	Elektronischer Rechtsverkehr
EUGH	Europäischer Gerichtshof
EUMAV	Europäisches Mahnverfahren
ff.	fortfolgende
FördEIRV	Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten
GBO	Grundbuchordnung
GG	Grundgesetz
ggfs.	gegebenenfalls
GVBl	Gesetz- und Verordnungsblatt Berlin
HDSG	Hessisches Datenschutzgesetz
HGB	Handelsgesetzbuch
HmbDSG	Hamburgisches Datenschutzgesetz
Hrsg.	Herausgeber
HZD	Hessische Zentrale für Datenverarbeitung
i.S.d.	im Sinne des
i.V.m	in Verbindung mit
IMOG	Informationsmanagement in der ordentlichen Gerichtsbarkeit
ISMS	Managementsystem für Informationssicherheit
IT	Informationstechnik
ITDZ	IT-Dienstleistungszentrum
ITDZAöRG BE	Gesetz über die Anstalt des öffentlichen Rechts IT-Dienstleistung
IuK	Informations- und Kommunikationstechnik

jM	juris – Die Monatszeitschrift
Kap.	Kapitel
KEJ	Kosteneinziehungsstelle der Justiz
KritV	Die kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
LDSG	Landesdatenschutzgesetz
LG	Landgericht
MMR	Multimedia und Recht
NAS	Network-Attached-Storage
NDSG	Niedersächsisches Datenschutzgesetz
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht, Neue Zeitschrift für Verwaltungsrecht
NWVBl	Nordrhein-Westfälische Verwaltungsblätter
OLG	Oberlandesgericht
Pdf	Portable Document Format
RDV	Recht der Datenverarbeitung
RPflG	Rechtspflegergesetz
Rn.	Randnummer
Rz.	Randziffer
S.	Satz
SächsDSG	Sächsisches Datenschutzgesetz
SAN	Storage Area Network
SBC	Server Based Computing
SDSG	Saarländisches Datenschutzgesetz
SenJus	Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung
SLAs	Service-Level-Agreements
StPO	Strafprozessordnung
ThürDSG	Thüringer Datenschutzgesetz
u.a.	unter anderem
v.	vom
v. Chr.	vor Christus

vgl.	vergleiche
VPN	Virtual Privat Network
VwVfG	Verwaltungsverfahrensgesetz
z.B.	zum Beispiel
ZBR	Zeitschrift für Beamtenrecht
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik

I. Vorwort

„Nichts ist so beständig wie der Wandel“ sagte bereits der griechische Philosoph Heraklit 520 - 460 v. Chr. im kleinasiatischen Ephesus.

Die Entwicklung der Informationstechnologie in den letzten Jahrzehnten prägt immer mehr unseren Alltag. In allen Bereichen der Gesellschaft erhält die elektronische oder technische Revolution mehr und mehr Einzug. Wir lesen die Zeitung auf unserem Tablet, können nahezu alles online bestellen, bezahlen unsere Rechnungen mit einem Mausklick, übermitteln unsere Steuererklärung online, verschicken Emails und können mittels unterschiedlicher Programme und Applikationen mit der ganzen Welt kommunizieren.

Die elektronische Informationstechnik und Datenverarbeitung ist ein großes Thema. Sie befindet sich immer noch im stetigen Wandel und umfasst weitaus mehr Bereiche als im ersten Moment vorstellbar.

Auch im beruflichen Alltag ist der Computer nicht mehr wegzudenken. Beginnend mit der Ausschreibung der zu besetzenden Stellen im Internet und der Online-Bewerbung, die in vielen Unternehmen mittlerweile selbstverständlich ist, über den Email-Kontakt mit Geschäftspartnern und Kunden sowie jegliche Recherche die der Arbeitsalltag erforderlich macht. Die stetige Innovation soll im Hinblick auf die Rationalisierung zum einen erleichtern und beschleunigen, aber auch effizient sein. Diese Entwicklung beschäftigt ebenfalls die Verwaltung und Justiz. Mittels der Informationstechnik soll mehr Transparenz geschaffen werden und dem rechtssuchenden Bürger die Möglichkeit einer schnellen und unkomplizierten Kommunikation geboten werden. Die Geschäftsabläufe sind zu modernisieren, um eine größere Effizienz von Gerichtsverfahren zu ermöglichen. Das klingt natürlich vielversprechend und zukunftsorientiert, wirft allerdings auch einige Fragen auf.

Wie genau soll das erfolgen? Wo werden unsere Daten gespeichert? Wer hat Zugriff auf die von mir verfassten Dokumente? Wer kann die Dokumente einsehen und Änderungen darin vornehmen? Gegen wen und in welchem Umfang sollen die erstellten Daten geschützt werden? Ist mein Entscheidungsprozess durch die Einsicht

anderer beeinträchtigt? Hierbei handelt es sich selbstverständlich um keine abschließende Aufzählung. In den nachstehen Ausführungen soll versucht werden die Antworten zu den aufgeworfenen Fragen zu finden.

Nach vielen Jahren des Einsatzes von Informationstechnik in der Justiz ist es wichtiger denn je, sich nicht nur auf die Rezeption von Anwenderprogrammen zu beschränken, sondern auch zu hinterfragen was hinter den Bildschirmen tatsächlich abläuft.

II. Einleitung

1. Ziel und Gliederung der Arbeit

Zu Beginn des Einzuges der Informationstechnologie in die Gerichte haben sich wahrscheinlich die wenigsten Sorgen um ihrer Daten gemacht, denn die Speicherung erfolgte entweder direkt auf dem genutzten Rechner oder auf einem Server der sich im Gerichtsgebäude befand. Die Datenhoheit verblieb in jedem Fall beim Gericht. Mittlerweile steht allerdings die wirtschaftliche Datenhaltung und effizientes Datenmanagement im Vordergrund.

Durch die elektronische Justiz werden Arbeitsabläufe der Justiz zweifelsohne umgestaltet. Die IT-Organisation der Gerichte hat damit eine herausragende Bedeutung. Sie tangiert nicht nur die Rahmenbedingungen der täglichen Arbeit der Gerichtsbarkeit, sondern auch die verfassungsrechtlich garantierte Unabhängigkeit der rechtsprechenden Gewalt.

Zum einen ist zu untersuchen, welche datenschutzrechtlichen Voraussetzungen Berücksichtigung finden müssen, um die Modernisierung umzusetzen. Sowohl das Bundesdatenschutzgesetz als auch die jeweiligen Landesdatenschutzgesetze sind heranzuziehen. Insbesondere wird die Fragestellung aus der Sicht der Berliner Justiz beleuchtet. Ferner ist auch zu prüfen, ob verfassungsrechtliche Aspekte der Digitalisierung entgegenstehen.

Der Schwerpunkt dieser Arbeit ist vor allem die Frage, ob durch den Einsatz von Informations- und Kommunikationstechnik die verfassungsrechtlich verankerte richterliche Unabhängigkeit und das Gebot der organisatorischen Selbstständigkeit der Gerichte betroffen sind. Diesbezüglich werden insbesondere die Entscheidung des Bundesgerichtshofs[1] und die im Verfahren vor-[2] und nachgehenden[3] Entscheidungen herangezogen. Die Gerichte haben die Frage behandelt, ob der Betrieb und die

---

[1] BGH Dienstgericht des Bundes, Urteil v. 06.10.2011 – RiZ (R) 7/10 = MMR 2012, 128.
[2] OLG Frankfurt, Urteil v. 20.04.2010 - DGH 4/08; LG Frankfurt, Urteil v. 11.07.2008 - 1 DG 5/2007.
[3] BVerfG, 17.01.2013 – 2 BvR 2576/11.

Administration des EDV-Netzes der Judikative bei externen Dienstleistern mit den Grundsätzen der richterlichen Unabhängigkeit kollidieren könnte und mit dem Gebot der organisatorischen Selbstständigkeit der Gerichte vereinbart werden kann. Der Gegenstand der Prüfung war die zentrale Verarbeitung von Daten bei der Hessischen Zentrale für Datenverarbeitung. Bei der HZD handelt es sich um eine Landesbehörde der Finanzverwaltung die alle Daten von Behörden, Gerichten und anderen öffentliche Stellen verwaltet.

Ohne die Gewährleistung von IT-Sicherheit[4] ist eine umfangreiche Digitalisierung der Justiz nicht möglich. Folglich sind auch die Anforderungen des Datenschutzes und der Datensicherheit an die eJustice zu analysieren. Diese werden unter anderem im Rahmen der BSI Grundsätze erläutert und geprüft. Für das Datenmanagement sind die Landesrechenzentren zuständig. Für die Berliner Justiz erfolgt dies beim IT-Dienstleistungszentrum (ITDZ) Berlin. Somit wird diese „Institution" beleuchtet.

Abschließend werden Abhilfemöglichkeiten erläutert und Verbesserungsvorschläge aufgeführt, die berücksichtigt werden können, um die digitale Berliner Justiz in Zukunft sowohl datenschutz- als auch verfassungskonform zu gestalten.

2. Modernisierung im öffentlichen Sektor

Die elektronische Justiz im heutigen Zeitalter führt Begriffe wie De-Mail, EGVP, elektronische Akte u.a. mit sich. Auch der Begriff eGovernment wird oftmals in Verbindung mit der eJustice gesehen.

Als Modernisierungsziele stehen hauptsächlich die Verfahrensbeschleunigung und die Kostenminimierung im Vordergrund.

a. eGovernment

Der Begriff Electronic Government bezeichnet nach der Speyerer Definition die Abwicklung von Geschäftsprozessen unter Zuhilfenahme von Kommunikations- und Informationstechnik. Dieser Ausdruck hat allerdings zwei unterschiedliche

[4] Allgemein zum Begriff IT-Sicherheit: Heckmann, MMR 2006, 280 ff. .

Bedeutungen. Zum einen gilt diese Begriffsbestimmung für den gesamten öffentlichen Sektor, folglich für die drei Gewalten und für öffentliche Unternehmen. Zum anderen wird damit eine öffentliche Verwaltung bezeichnet, die auf elektronischem Weg Bescheide erlässt und elektronische Auskunfts- und Antragsformen zu Verfügung stellt.

Electronic Government umfasst die Kommunikation zwischen Bürger und Verwaltung, zwischen Verwaltung und Wirtschaft sowie die geschäftlichen Prozesse zwischen dem gesamten öffentlichen Sektor. Das Ziel im eGovernment ist es, die Leistungen der Verwaltung auf interaktiver Kommunikationsbasis vollständig elektronisch abzuwickeln.[5] Aufgrund der stetigen technischen Entwicklung soll künftig eine vollständig elektronische Abwicklung möglich werden. Nach dem Gesetz zur Förderung der elektronischen Verwaltung, sowie zur Änderung weiterer Vorschriften vom 25.07.2013[6] ist am 30.05.2016 nach der Veröffentlichung im Gesetz- und Verordnungsblatt Berlin Nr. 14/16 das Gesetz zur Förderung des eGovernment vom 30.05.2016[7] in Kraft getreten. Im Vordergrund steht die moderne serviceorientierte Dienstleistung, denn die Verwaltung nimmt die Rolle des „Dienstleisters“ ein und der Bürger die des „Kunden“.[8]

b. eJustice

Unter Electronic Justice versteht man nach der abgewandelten Spreyer Definition die Abwicklung geschäftlicher Prozesse im Zusammenhang mit Rechtsprechung und Justiz mithilfe von Informations- und Kommunikationstechniken über elektronische Medien. Die unterschiedlichen Möglichkeiten des Einsatzes von Informations- und Kommunikationstechnologie im justiziellen Bereich können mit dem Sammelbegriff eJustice bezeichnet werden.[9]

Dazu gehört auch der Elektronische Rechtsverkehr (ERV). Nach der Definition der ERV-Kommission umfasst dieser die rechtsverbindliche elektronische

[5] Yildirim, Datenschutz im Electronic Government, 1. Aufl., S. 19.
[6] BGBl. I 2013, 3786.
[7] GVBl S. 282.
[8] Yildirim, Datenschutz im Electronic Government, 1. Aufl., S. 21.
[9] Berlit, JurPC Web.-Dok. 171/2007 Abs. 1; Radke, JurPC Web-Dok. 46/2006.

Kommunikation zwischen Verfahrensbeteiligten und den Gerichten.[10] Dabei geht es im engeren Sinne um die Übermittlung von gerichtlichen Entscheidungen, die Einreichung von prozessualen Erklärungen, die elektronische Aktenführung, Archivierung und die interne Sachbehandlung. Im weiteren Sinne geht es um die Auskunftssysteme wie das elektronische Handelsregister und Grundbuch. In den letzten Jahren haben eine Vielzahl der Bundesländer Pilotprojekte zum elektronischen Rechtsverkehr initiiert und teilweise flächendeckend eingeführt.

Das elektronisch geführte Grundbuch und Handelsregister, sowie das elektronische Mahnverfahren und die Bekanntmachungen der Insolvenzgerichte unter www.Insolvenzbekanntmachungen.de werden mit Hilfe der Informationstechnik möglich gemacht.

c. Gemeinsamkeiten zwischen eJustice und eGovernment

Gemeinsamkeiten zwischen eJustice und eGovernment finden sich bei der elektronischen Signatur. Dieses Verfahren ist die Grundlage für ein sicheres und rechtsverbindliches Handeln und gewährleistet die Authentizität der Betroffenen und die Integrität der übermittelten Daten. Der Datentransfer soll damit vor Manipulationen geschützt und der Kommunikationspartner eindeutig identifiziert werden. Zudem wird auch die Vertraulichkeit des elektronischen Dokumentes geschützt. Folglich können die gesendeten Daten aufgrund der Verschlüsselung nicht von Dritten eingesehen werden. Etwaige Veränderungen in dem Dokument können mit Hilfe der Signaturprüfung nachgewiesen werden. Die rechtliche Grundlage für das Signaturverfahren bildet das Gesetz über die Rahmenbedingungen für elektronische Signatur vom 16.05.2001.[11] Die Einführung und Nutzung dieser Schlüsseltechnologie erfolgt bereits für Justiz und Verwaltung. Weitere Gemeinsamkeiten finden sich auch bei der elektronischen Akte. Es werden immer mehr Datenbänke elektronisch bereitgehalten, um Arbeitsprozesse zu optimieren und den Weg zu der papierlosen Justiz und Verwaltung zu ebnen.

[10] https://www.edvgt.de/engagement/, 29.03.2017, 17:08 Uhr.
[11] BGBl. I 2001, 876.

In beiden Fällen handelt es ich um elektronische Kommunikation staatlicher Stellen mit Bürgern unter dem Einsatz von Informationstechnik, die den Grenzen des Art. 33 Abs. 4 GG unterworfen sind. Allerdings macht die verfassungsrechtliche Sonderrolle der Justiz den signifikanten Unterschied aus. Die Justizminister fungieren für die Justizverwaltung als Teil der vollziehenden Gewalt und sind organisatorisch verantwortlich für das Funktionieren der rechtsprechenden Gewalt.[12] Das Legalitätsprinzip und die richterliche Unabhängigkeit sind weitere justizspezifische Besonderheiten die Parallelen zwischen eGovernment und eJustice nur teilweise zulassen.

Obwohl eJustice nicht eGovernment ist, ist eine technische Abstimmung zwischen den Bereichen aus grundsätzlichen Systemüberlegungen heraus durchaus erforderlich. Beispielsweise enthält die Akte in Strafverfahren regelmäßig Dokumente, die durch die Polizei angelegt wurden (Einleitung des Ermittlungsverfahrens, polizeiliche Zeugenvernehmung u.a.). Die Vereinbarkeit mit den polizeilichen IT-Systemen ist somit sinnvoll, um eine reibungslose Datenübertragung an die Gerichte und Staatsanwaltschaften zu erreichen. Zumindest eine technische Abstimmung ist aus dieser Sicht unumgänglich.

3. Entwicklung der elektronischen Justiz

Die Justiz soll mit den Mitteln der Informationstechnologie transparenter gestaltet werden und mit den modernen Arbeitsmitteln soll eine Effizienzsteigerung der täglichen Arbeit in den Gerichten erreicht werden. Die Grundlagen für diese Entwicklung sind das Inkrafttreten des Justizkommunikationsgesetzes am 01.04.2005[13] und das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10.10.2013.[14] Durch die vorstehenden Gesetze sollen nicht nur die Geschäftsabläufe innerhalb der Justiz erleichtern und beschleunigen, sondern auch die Kommunikation zwischen den Gerichten und dem Bürger fördern.[15]

---

[12] Köbler, NJW 2006, 2089.
[13] BGBl. I 2005, 837.
[14] BGBl. I 2013, 3786.
[15] vgl. auch BT-Drs 17/12634, S. 20 ff.

Sowohl die Globalisierung als auch die Digitalisierung nehmen immer mehr Einfluss auf die öffentliche Hand. In einem herkömmlichen Wirtschaftsunternehmen geht dieser Wandel erfahrungsgemäß schneller vonstatten. Die Gründe dafür liegen nicht nur in der haushaltspolitischen Bindung und der verfassungsrechtlich verankerten Gewaltenteilung, sondern mithin auch in dem umfangreichen Aufgabenspektrum der hoheitlichen Staatstätigkeit, den speziellen Arbeitsabläufen und Organisationsstrukturen der einzelnen Gerichte. Durch die Modernisierung und Digitalisierung sollen diese allerdings eines Tages zur Wirtschaft aufschließen.

Durch die elektronischen Abläufe mit Rationalisierungspotenzial und Effizienzgewinnen wird die Leistungsfähigkeit der Dritten Gewalt gesichert und die durchgehende elektronische Kommunikationsbeziehung mit dem rechtssuchenden Bürger eröffnet. Fraglich ist, ob diese Erleichterung der Arbeitsabläufe in jedem Bereich realisiert werden kann.

III. Datenschutzrechtlicher Anwendungsbereich

1. Grundgesetz

Mit in Kraft treten des Art. 91 c GG am 01.08.2009[16] und des dazugehörigen IT-Netz-Gesetzes am 18.08.2009[17] sowie des IT-Staatsvertrages am 01.04.2010[18] wurden neue Strukturen im Bereich der Informationstechnologie gebildet. Bis zum Inkrafttreten existierte im Hinblick auf die Informationstechnologie keine Regelung im Grundgesetz. Auch aus europäischer Sicht war die Regelung notwendig, denn aus Art. 8 der EU-Dienstleistungsrichtlinien ergibt sich bereits ein Anspruch auf elektronische Verfahrensabwicklung.[19] Art. 91 c GG ermöglicht nunmehr das Zusammenwirken von Bund und Ländern bei der Planung, Errichtung sowie dem Betrieb der informationstechnischen Systeme, die für ihre Aufgabenerfüllung nötig sind. Weiterhin ermöglicht Art. 91 c Abs. 3 GG den Ländern untereinander einen gemeinschaftlichen Betrieb entsprechender Systeme. Die Harmonisierung und Schaffung von Interoperabilität im Bereich der Informationstechnik kann damit gefördert werden.[20]

Die Informationstechnik ist durch das rasante Wachstum und kurze Innovationszyklen geprägt. Bereits nach vier Jahren nutzen rund 50 Millionen Nutzer das Internet. Dabei dürfte es sich um die entscheidende Infrastruktur der nächsten Jahrzehnte handeln. Damit gewinnt auch die digitale Dimension der Grundrechte an Bedeutungszuwachs. Die Digitalisierung tangiert die Verfassung auf unterschiedliche Weise. Berührt wird unter anderem die Berufsfreiheit aus Art. 12 Abs. 1 GG durch gesetzliche Normen, die Vorgaben zur Nutzung bestimmter Kommunikationsdienste machen. Ein Beispiel dafür ist die Verpflichtung zur ausschließlichen Nutzung elektronischer Mittel für die Kommunikation mit den Gerichten spätestens ab dem 01.01.2022.[21]

---

[16] BGBl. I 2009, S. 2248.
[17] BGBl. I 2009, S. 2702.
[18] https://www.bmi.bund.de/SharedDocs/, 29.03.2017, 17:10 Uhr.
[19] Schulz, DVBl 2009, 12 ff.
[20] Siegel, NVwZ 18/2009, S. 1128 ff.
[21] Art. 26 Abs. 7 FördEIRV.

2. Bundesdatenschutzgesetz

Die Erstfassung des Bundesdatenschutzgesetzes wurde am 01.02.1977 im Bundesgesetzblatt verkündet[22] und ist am 01.01.1979 in Kraft getreten. Bereits vorher war bekannt, dass der fortschreitende Einsatz der Informationstechnologie Rahmenbedingungen erforderlich macht, um der Tatsache entgegenzuwirken, dass schutzwürdige Belange der Betroffenen bei der Verarbeitung ihrer Daten beeinträchtigt werden. Der Sinn und Zweck von Datenschutz ist, dass jeder Mensch die Möglichkeit haben soll, selbst zu bestimmen, wer bei welcher Gelegenheit welche Informationen über ihn erhält. Damit soll verhindert werden, dass Entscheidungen im Berufs- oder Alltagsleben durch eine verkürzte Nutzung von Daten oder durch eine falsche und unzulässige Verknüpfung von Daten negativ beeinflusst werden. Datenschutzgesetze schützen somit nicht die Daten selbst, sondern den Bürger vor Nachteilen durch die Datenverarbeitung. Das Volkszählungsurteil des Bundesverfassungsgerichts[23] erklärte die Rechtmäßigkeit staatlicher Datenverarbeitung und den daraus resultierten Anspruch auf Schutz des informationellen Selbstbestimmungsrechts des Bürgers. Somit bestand für den Gesetzgeber die Pflicht einen generellen umfassenden Schutz der Persönlichkeitsrechte zu sichern. Durch die Novellierung wurden die Datenschutznormen mit der Neufassung vom 20.12.1990 erweitert und konkretisiert.[24] Im Laufe der Jahre hat das Gesetz zahlreiche Änderungen und Erweiterungen erfahren und an Umfang und Regelungsdichte zugenommen. Die Neuerung betrafen Erweiterungen des Geltungsbereichs, der Datenschutzkontrolle und der Verarbeitungsbeschränkungen.

Mit der Überarbeitung im Jahre 2001[25] wurden die Anforderungen der EU-Datenschutzrichtlinien des Europäischen Parlaments umgesetzt.[26] Drei Reformgesetze

---

[22] BGBl. I 1977, 201.
[23] BVerfG, NJW 1984, 419.
[24] BGBl. I 1990, 2954.
[25] BGBl. I 2001, 904.
[26] Richtlinien zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, RL 95/46/EG.

brachten im Jahre 2009 weitere Änderungen für das BDSG.[27] Allerdings betrafen diese ausschließlich den Bereich des privaten Datenschutzrechts.[28]

Durch die Modernisierung des Datenschutzrechts wurde der Schutz der Betroffenen im öffentlichen und privaten Bereich stetig verbessert und vereinheitlicht. Das Gesetz besteht derzeit in der Fassung der Bekanntmachung vom 14.01.2003[29] mit der vorerst letzten Änderung vom 25.02.2015.[30] Anfang Februar 2017 hat die Bundesregierung angesichts des neuen EU-Datenschutzrechts, bestehend aus der Datenschutz-Grundverordnung[31] und der Datenschutz-Richtlinie[32] im Bereich Justiz und Inneres, den Entwurf zu einem neuen BDSG beschlossen.[33] Die EU möchte ein gleichmäßiges und hohes Datenschutzniveau in allen Mitgliedsstaaten erreichen und gewährleisten. Folglich ist das nationale Datenschutzrecht der Mitgliedsstaaten nunmehr bis Mai 2018 an die Verordnung anzupassen und die Richtlinien in nationales Recht umzusetzen. Die Umsetzung der DS-Grundverordnung wird dazu führen, dass das BDSG zahlreiche Änderungen erfährt und die Landesdatenschutzgesetze ebenfalls angepasst werden. Bis zur Einführung hat auch die öffentliche Hand ihre Datenverarbeitung DS-GVO-konform auszugestalten.[34]

Das BDSG ist ein Schutzgesetz und wirkt nach dem Konzept des Gesetzgebers präventiv. Die Rechtsgrundlage ist demnach ein Verbot mit Erlaubnisvorbehalt. Nach der klassischen Systematik regelt § 1 Zweck und sachlichen Anwendungsbereich. Es dient dem Schutz des Betroffenen vor Beeinträchtigung bei dem Umgang[35] mit seinen personenbezogenen Daten. Legaldefinitionen der Unterbegriffe finden sich in § 3 BDSG. Die verfassungsrechtlich verankerten allgemeinen Persönlichkeitsrechte aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dienen hierbei als Prüfungsmaßstab für das

---

[27] Taeger/Gabel (Hrsg.), Kommunikation und Recht BDSG, 2. Aufl., Einführung Rz. 11.
[28] zu diesen vgl. zum Beispiel Roßnagel, NJW 2009, 2716; Abel, RDV 2009, 147.
[29] BGBl. I 2003, 66.
[30] BGBl. I 2015, 162.
[31] https://www.datenschutz-grundverordnung.eu, 29.03.2017, 17:10 Uhr.
[32] https://www.janalbrecht.eu/fileadmin/material/, 29.03.2017, 17:10 Uhr.
[33] http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/, 29.03.2017, 17:10 Uhr.
[34] Gola/Klug, NJW 2017, 604 ff.
[35] Oberbegriff umfasst das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen und Nutzen; Gola/Schomerus, BDSG, 12. Aufl., Rz. 22 zu § 1.

BDSG. In Bezug auf die staatliche Datenverarbeitung handelt es sich jedoch auch um ein Eingriffsgesetz. Damit können Eingriffe in das Recht auf informationelle Selbstbestimmung legitimiert werden. Bei den Eingriffsnormen und den konkreten Eingriffen sind das Allgemeininteresse zu berücksichtigen und die Grundsätze der Verhältnismäßigkeit und Normklarheit.

Das Gesetz besteht aus dem Allgemeinen Teil mit den für alle Datenverarbeiter geltenden Normen, sowie aus den ergänzenden Regelungen für den öffentlichen und privaten bzw. nicht öffentlichen Bereich. Ein wichtiger Aspekt der Regelungssystematik zeigt, dass öffentliche Stellen grundsätzlich anderen Regeln unterworfen sind als nicht öffentliche Stellen. Die Normadressaten sind somit die datenverarbeitenden Stellen aus dem privaten Bereich gemäß § 2 Abs. 4 BDSG. Zu den nicht-öffentlichen Stellen gehören damit natürliche und juristische Personen, Gesellschaften und Personenvereinigungen. Werden allerdings öffentliche Aufgaben wahrgenommen, handelt es sich um öffentliche Stellen im Sinne des BDSG.

Weitere Normadressaten sind die öffentlichen Stellen. Unter diesen Begriff fällt der „gesamte Bereich der Betätigung der öffentlichen Hand“[36]. Hierbei handelt es sich unter anderem um Behörden[37] und die Organe der Rechtspflege, nämlich die Gerichte des Bundes und der Länder. Der persönliche Anwendungsbereich für die Gerichte des Bundes als öffentliche Stelle ergibt sich aus § 1 Abs. 2 Nr. 1 i.V.m. § 2 Abs. 1 BDSG. Soweit die Organe der Rechtspflege Aufgaben der öffentlichen Verwaltung wahrnehmen, fallen sie unter den Behördenbegriff. Dazu gehört folglich die Justizverwaltung.[38]

Das BDSG unterscheidet ferner zwischen öffentlichen Stellen des Bundes und der Länder. Zu den öffentlichen Stellen des Bundes gehören das BVerfG und die obersten Bundesgerichte (Bundesgerichtshof, Bundesarbeits-, Bundesverwaltungs- und Bundessozialgericht sowie der Bundesfinanzhof). Die öffentlichen Stellen der Länder, § 2 Abs. 2 BDSG, insbesondere die Organe der Rechtspflege, liegen nur im

[36] Gola/Schomerus, BDSG, 12. Aufl., Rz. 4 zu § 2.
[37] „jede Stelle die Aufgaben der öffentlichen Verwaltung wahrnimmt“, § 1 Abs. 4 VwVfG.
[38] Gola/Schomerus, BDSG, 12. Aufl., Rz. 10 zu § 2.

Anwendungsbereich des BDSG, sofern der Datenschutz nicht durch Landesrecht geregelt ist, § 1 Abs. 2 Nr. 2b BDSG. Fraglich ist somit, ob für die Berliner Justiz der Anwendungsbereich des BDSG eröffnet ist. Da jedes Bundesland der BRD bereits seit Mitte der 90er Jahre über ein entsprechendes Landesdatenschutzgesetz verfügt, findet für die öffentlichen Stellen der Länder das BDSG keine Anwendung. Soweit die Gerichte nicht in Verwaltungsangelegenheiten handeln und landesrechtliche Regelungen existieren, wird das BDSG im Anwendungsbereich verdrängt. Mit der landesrechtlichen Regelung in § 2 Abs. 1 BlnDSG wird für Berlin das BDSG durch das Landesdatenschutzgesetz in vollem Umfang verdrängt. Neben dem BlnDSG verdrängt auch das jeweilige Landesrecht der Bundeländer Hessen[39], Bayern[40], Rheinland-Pfalz[41], Baden-Württemberg[42], Hamburg[43], Niedersachen[44], Sachen[45], Sachen-Anhalt[46], Schleswig-Holstein[47] und Thüringen[48] das Bundesrecht.

Das jeweilige Landesdatenschutzgesetz ist in diesem Fall heranzuziehen. Zu beachten ist allerdings auch, dass die Definitionen des § 2, wie auch die des § 3 nur bei der Anwendung des BDSG gelten. Kommt nach § 1 Absatz 2 nicht das BDSG, sondern Landesrecht zur Anwendung, so ist die landesgesetzliche Definition der öffentlichen Stelle maßgeblich.

Die Landesdatenschutzgesetze der übrigen Bundesländer wie Bremen[49], Brandenburg[50], Mecklenburg-Vorpommern[51], Saarland[52] und Nordrhein-Westfalen[53] regeln dagegen nur den Bereich der Justizverwaltung. Folglich bleibt das BDSG auf den rechtsprechenden Teil in vollem Umfang anwendbar.

---

[39] § 2 Abs. 1 Nr. 1 HDSG.
[40] Art. 2 Abs. 1 BayDSG.
[41] § 2 Abs. 1 Nr. 2 LDSG.
[42] § 2 Abs. 3 LDSG.
[43] § 2 Abs. 1 Nr. 1 HmbDSG.
[44] § 2 Abs. 1 Nr. 1 NDSG.
[45] § 2 Abs. 1 SächsDSG.
[46] § 3 Abs. 1 DSG-LSA.
[47] § 3 Abs. 1 LDSG.
[48] § 2 Abs. 1 ThürDSG.
[49] § 1 Abs. 4 BremDSG.
[50] § 2 Abs. 1 BbDSG.
[51] § 2 Abs. 4 DSGM-V.
[52] § 2 Abs. 1 SDSG.
[53] § 2 Abs. 1 DSGNRW.

Die Verarbeitung von Daten ist stets die Einschränkung eines Grundrechts, damit bedarf es immer der Prüfung der Erforderlichkeit. Ferner sind die Auskunftsrechte des Betroffenen über Art, Zweck und Empfänger der Verarbeitung und Übermittlung zu beachten. Ob der Anwendungsbereich des BDSG für einen bestimmen Sachverhalt eröffnet ist bedarf zunächst der Prüfung dreier Kriterien. Unter den Anwendungsbereich fällt die Erhebung, die Verarbeitung oder die Nutzung personenbezogener Daten. Folglich müssen zunächst personenbezogene Daten vorliegen. Eine Definition ergibt sich aus § 3 Abs. 1 BDSG. Es muss sich demnach um Einzelangaben über persönliche oder sachliche Verhältnisse einer natürlichen Person handeln. Zu bemerken ist, dass das BDSG keine juristischen Personen schützt. Die Person muss ferner direkt oder indirekt identifizierbar sein. Eine bestimmte Person liegt vor, wenn die Daten unmittelbar einer natürlichen Person zugeordnet werden können. Nach dem BDSG wird eine Person als bestimmbar angesehen, wenn die betreffenden Daten durch spezifische Elemente zugeordnet werden können. Sofern ein Personenbezug mit verfügbarem Zusatzwissen herstellbar ist, handelt es sich folglich um eine bestimmbare Person. Die Abgrenzung, ob es sich um personenbezogene Daten handelt gestaltet sich jedoch meist schwierig. Grundsätzlich ist festzustellen, dass es sich bei allen Informationen über die ein Personenbezug gebildet werden kann, um personenbezogene Daten handelt. Beispiele dafür sind der Name, die Personalnummer, die Kontaktdaten und Kontodaten und selbst die Aufzeichnungen der Arbeitszeit[54], sowie zahlreiche andere Daten. Aus § 3 Abs. 9 BDSG ergeben sich ferner Daten, die besonders schützenswert sind und deren Verwendung besonderen Anforderungen unterliegt. Hierzu gehören beispielsweise Angaben über religiöse Überzeugung, rassische und ethische Herkunft und politische Meinungen. Das BDSG schützt folglich nur personenbezogene Daten. Der Anwendungsbereich ist eröffnet, sofern diese Daten über Betroffene gezielt beschafft (Erhebung) oder gespeichert, übermittelt, gelöscht und verändert (Verarbeitung) werden. Allerdings auch bereits bei jeder Verwendung dieser Daten (Nutzung), soweit es sich nicht um die Verarbeitung handelt. Diese beinhaltet u.a. die Auswertung und die Verwendung des Informationsgehalts für Entscheidungen. Die personenbezogenen Daten der Antragsteller, Antragsgegner, Rechtsanwälte, Notare, Beklagten, Kläger etc. die bei

[54] EuGH, Urteil v. 30.05.2013 – C-342/12 -, juris.

den Gerichten anfallen sind somit durch das BDSG geschützt. Dies gilt auch für die Mitarbeiter der Justiz. Somit unterliegen auch die Verfügungen und Beschlüsse, die personenbezogene Daten enthalten, dem Schutz des Bundesrechts. Handelt es sich jedoch um Entwürfe oder Vermerke, die keine Zuordnung zu bestimmten Personen ermöglichen, weder direkt noch indirekt, so ist das BDSG nicht anwendbar.

3. Berliner Datenschutzgesetz

Das informationelle Selbstbestimmungsrecht bildete ebenfalls die Grundlage für die Landesdatenschutzgesetze. Hessen verabschiedete bereits im Jahre 1970 als erstes Bundesland ein Landesdatenschutzgesetz. Das Berliner Datenschutzgesetz ist erstmals in der Fassung vom 17.12.1990 im Gesetz- und Verordnungsblatt bekanntgemacht worden.[55] Nunmehr regelt es die Voraussetzungen unter denen Berliner Behörden und Organe der Rechtspflege personenbezogene Daten verarbeiten dürfen. Die Verarbeitung der Daten von Bürgern ist grundsätzlich nur zulässig, wenn eine besondere Rechtsvorschrift es erlaubt oder der betroffene Bürger eingewilligt hat. Das BlnDSG beginnt mit Allgemeinen Vorschriften im ersten Abschnitt welche den Anwendungsbereich, die Wartung der Datenverarbeitungssysteme und zahlreiche Begriffsbestimmungen sowie technische und organisatorische Maßnahmen beinhalten, die die Ausführung des BlnDSG sicherstellen. Nachfolgende Vorschriften des zweiten Abschnitts regeln unter anderem die Voraussetzungen unter denen Datenverarbeitung erfolgen kann, die Datensparsamkeit und Datenübermittlung. Die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme wird ebenfalls durch das BlnDSG bestimmt.

Fraglich ist, ob sich unterschiedliche Voraussetzungen für Daten ergeben, welche durch die Beschäftigten der Justiz produziert werden. Sofern die Gerichte in richterlicher Unabhängigkeit tätig werden, unterliegen sie nicht der Kontrolle des Datenschutzbeauftragten. Eine Kontrolle durch den Berliner Beauftragten für Datenschutz erfolgt gemäß § 24 Abs. 2 BlnDSG bei Gerichten nur soweit sie in Verwaltungsangelegenheiten tätig werden. Verfassungsrechtlich ist eine Kontrolle wegen Art. 92, 97 GG, §§ 4 Abs. 1, 25 DRiG unzulässig.

---

[55] GVBl. 1991 S. 16, 54.

Um die umfangreichen Dokumentationspflichten die aus dem Volkszählungsurteil und der gesetzlichen Umsetzung erwachsen sicherzustellen, bedarf es eines Sicherheitskonzeptes. Dieses sollte Verfahrensverzeichnisse, technisch-organisatorische Maßnahmen und Verzeichnisse für alle Fälle der Auftragsdatenverarbeitung abdecken. Der Inhalt von Verfahrensverzeichnissen ergibt sich aus § 19 Abs. 2 BlnDSG. Die Verfahrensverzeichnisse sind nicht nur für jede einzelne Fachanwendung zu erstellen, sondern auch für alle anderen Programme wie beispielsweise das E-Mail-Programm. Es wird zwischen internen und öffentlichen Verfahrensverzeichnissen unterschieden. Der einzige Unterschied besteht darin, dass die internen Verzeichnisse zusätzlich eine allgemeine Beschreibung ausweisen müssen, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind. Ferner ist das öffentliche Verfahrensverzeichnis auf Antrag jedermann in geeigneter Weise verfügbar zu machen, § 19a Abs. 1 S. 4 BlnDSG. Die jeweiligen Verfahrensverzeichnisse für die Fachanwendungen werden in Berlin für die ordentliche Gerichtsbarkeit durch das Kammergericht geführt. Soweit es sich um Programme handelt, die nur bestimmte Gerichte nutzen, erfolgt die Führung der Verzeichnisse bei den jeweiligen Gerichten. Für alle Fälle der Auftragsdatenverarbeitung sind ebenfalls Verfahrensverzeichnisse anzulegen. Auftragsdatenverarbeitung gemäß § 3 BlnDSG liegt vor, wenn sich die verantwortliche Stelle einer anderen Stelle bedient, die im Auftrag und weisungsabhängig personenbezogene Daten erhebt, verarbeitet oder nutzt.

Die Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung entsprechen den datenschutzrechtlichen Schutzzielen aus § 5 Abs. 2 BlnDSG. Es sind unterschiedliche technisch-organisatorische Maßnahmen erforderlich. Oftmals werden zur besseren Verständlichkeit die Begrifflichkeiten aus der Anlage zu § 9 Abs. 1 BDSG herangezogen. Unter die 8 Gebote des Datenschutzes fallen die Zutritts-, Zugangs-, Zugriffs- und Weitergabekontrolle, sowie die Eingabe-, Auftrags-, Verfügbarkeitskontrolle und die Datentrennung. Um die Anforderungen zu erfüllen können technische, bauliche und organisatorische Maßnahmen getroffen werden.

4. Weitere datenschutzrechtliche Regelungen

Eine Vielzahl von datenschutzrechtlichen Erlaubnisnormen findet sich in den Verfahrensordnungen. Vorschriften wie zum Beispiel § 12 GBO, § 299 ZPO, § 9 HGB, § 915b Abs. 1 ZPO, welche Bestimmungen im Hinblick auf die Einsicht in Register und Akten treffen, gehen den Regelungen in den allgemeinen Datenschutzgesetzten vor. Unbeachtlich der Entstehung der jeweiligen Normen sind die Vorschriften aus den Verfahrensordnungen vorrangig und die Landesdatenschutzgesetze und das BDSG subsidiär anzuwenden. Datenschutzrechtliche Regelungen finden sich darüber hinaus in etlichen Spezialgesetzen, etwa dem Telekommunikationsgesetz und dem Telemediengesetz, diese enthalten jeweils speziellere Regelungen zum Datenschutz für ihren Anwendungsbereich und sind als bereichsspezifischere Regelungen ebenfalls vorrangig.

IV. Begriffsbestimmungen und Erläuterungen

Im Rahmen der Informationstechnologie werden unterschiedliche Begrifflichkeiten oftmals nicht richtig verwendet. Teilweise ist eine klare Abgrenzung und Definition nur schwer möglich. Allerdings unterscheiden sich die Begriffe innerhalb ihrer Schutzziele.

1. Datenschutz

In erster Linie verfolgt der Datenschutz das Ziel die Privatsphäre eines Jeden zu schützen. Damit wird jedem Bürger das Recht auf informationelle Selbstbestimmung garantiert und schützt vor der missbräuchlichen Verwendung seiner Daten. Unter welchen Umständen und in welcher Form personenbezogene Daten verarbeitet werden können regelt das BDSG und die jeweiligen Landesdatenschutzgesetze. Die Kernfrage des Datenschutzes ist somit, ob personenbezogene Daten überhaupt verarbeitet werden dürfen.

2. Datensicherheit und Datensicherung

Die Datensicherheit befasst sich dagegen mit dem Schutz von Daten im Allgemeinen, unabhängig davon, ob diese Personenbezug aufweisen oder nicht. Die Datensicherheit dient dem Schutz vor Manipulation, Verlust oder unberechtigter Kenntnis. Hier geht es in erster Linie um die technischen und organisatorischen Maßnahmen welche zum Schutz der Daten erhoben werden müssen. Im Hinblick auf die Erforderlichkeit solcher Maßnahmen ist gem. § 9 S. 2 BDSG der Verhältnismäßigkeitsgrundsatz heranzuziehen. Der angestrebte Schutzzweck und der Aufwand der Maßnahmen müssen demnach verhältnismäßig sein.[56] Zur Gewährleistung der Datensicherheit sind Maßnahmen der Datensicherung erforderlich. Hierzu gehören alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme. Datensicherung erfolgt durch das Erstellen von Sicherungskopien, damit diese im Fall eines Systemfehlers nicht in Verlust geraten. Ein erheblicher Datenverlust ist nur zu vermeiden, sofern eine regelmäßige Sicherung erfolgt. Im Fall der Datenbeschädigung oder des Datenverlustes dienen die Backups der Wiederherstellung der Originaldaten.

3. Verarbeiten und Speichern

Was genau versteht man unter Verarbeiten und Speichern? Der Begriff des Verarbeitens wird durch das BDSG seit der Umsetzung der Datenschutzrichtlinien nicht einheitlich verwendet. In § 3 Abs. 4 BDSG werden fünf Phasen des Verarbeitens zusammengefasst. Die Verarbeitung im engeren Sinne umfasst das Speichern, Verändern, Übermitteln, Sperren und Löschen. Der weite Begriff des automatisierten Verarbeitens wird in § 3 Abs. 2 BDSG geregelt und entspricht dem Verarbeitungsbegriff der Datenschutzrichtlinien. Das Speichern (Fixieren von Daten durch menschliche Tätigkeit bzw. mittels apparativer Aufzeichnungsmechaniken wie Festplattenaufzeichnungen) umfasst das Erfassen, Aufnehmen bzw. Aufbewahren personenbezogener Daten zum Zwecke ihrer weiteren Verarbeitung oder Nutzung (§ 3 Abs. 4 S. 2 Nr. 1 BDSG). Die Entgegennahme von bereits fixierten Daten zwecks Breithalten zur weiteren Verarbeitung und Nutzung entspricht auch dem Speichern.[57]

---

[56] Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, 5. Aufl., Teil II Kap. 2.1.4, S. 239

[57] Schild, in Roßnagel (Hrsg.), Handbuch Datenschutzrecht, Kap. 4.2 Rz. 58.

4. Grundwerte der Informationssicherheit

Aus § 5 Abs. 2 BlnDSG ergeben sich bereits die Grundwerte der Informationssicherheit. In erster Linie gehören hierzu die Vertraulichkeit, Integrität und Verfügbarkeit. Unter Vertraulichkeit versteht man den Ausschluss vertraulicher Informationen von der Kenntnis Unbefugter. Die Daten und Informationen sind ausschließlich befugten Personen in der zulässigen Weise zugänglich zu machen. Eine Verletzung der Integrität liegt vor, wenn die Unversehrtheit der Informationen und Funktionsweise von Systemen nicht mehr gegeben ist. Integrität bedeutet demnach in Zusammenhang mit Daten, dass diese vollständig und unverändert sind. Werden Daten unerlaubt verändert, so liegt folglich eine Verletzung der Integrität vor. Die Verfügbarkeit umfasst den Zugriff autorisierter Benutzer auf Systeme, Anwendungen, IT-Netze und Informationen in der vorgesehen Weise. In individuellen Anwendungsfällen gehören unter anderem auch Begriffe wie Authentizität und Nichtabstreitbarkeit, mithin Verbindlichkeit zur Informationssicherheit. Authentizität gewährleistet, dass der angegebene Kommunikationspartner auch der Ersteller der Daten ist. Die Begrifflichkeit wird sowohl bei Personen als auch bei Anwendungen und IT-Komponenten verwendet. Dazu gehört gewissermaßen auch die Nichtabstreitbarkeit. Der Empfang und der Versand von übermittelten Informationen können nachträglich nicht bestritten werden. Das Schutzziel der Verbindlichkeit fasst diese beiden Begriffe folglich zusammen. Bei der Übertragung von Informationen bedeutet dies, dass die übermittelnde Person ihre Identität bewiesen hat und der Empfang der Daten nicht in Abrede gestellt werden kann.

Diese Grundwerte sind bei einer Schutzbedarfsanalyse von tragender Bedeutung. Die Prüfung, welche technischen und organisatorischen Maßnahmen notwendig sind, um die Schutzziele zu gewährleisten erfolgt im Rahmen einer Schutzbedarfsanalyse. Der Schutzbedarf beschreibt demnach, welcher Schutz für die jeweiligen Geschäftsprozesse, die eingesetzte Informationstechnik und die zu verarbeitenden Informationen angemessen ist und ausreicht. Dazu ist zunächst zu bestimmen, welche Daten verarbeitet werden und wie hoch das jeweilige Schutzniveau dieser Daten ist. Es empfiehlt sich die Einteilung in drei Schutzbedarfskategorien (normal, hoch und sehr hoch). Dabei bedeutet die Kategorie „normal“ dass die Schadenauswirkungen im Falle der Verletzung der Grundwerte begrenzt und überschaubar sind. Bei der

Zuordnung zur Kategorie „hoch“ können die Schadenauswirkungen dagegen beträchtlich sein. Gehört das Schutzniveau von Daten zur Schutzbedarfskategorie „sehr hoch“, können Schadenauswirkungen ein existentiell bedrohliches, katastrophales Ausmaß erreichen. Auf Basis dieser Einschätzung wird sodann ermittelt, welche Maßnahmen minimal notwendig sind um die Verarbeitung von Daten im Rahmen des BSI Grundschutzes umzusetzen. Ausschlaggebend hierbei sind die zu erwartenden Schäden die bei einer Beeinträchtigung der Grundwerte eintreffen können. Möglichen Folgeschäden sind grundsätzlich für jede Anwendung gesondert und realistisch einzuschätzen.

5. Outsourcing[58]

Beim Outsourcing steht das Ziel im Vordergrund bestimmte Dienstleistungen nicht selbst zu erbringen, sondern zu übertragen. Diese Übertragung erfolgt an Dienstleistungsunternehmen bei denen die Leistungserbringung wirtschaftlicher erfolgt. Vom Outsourcing selbst ist die lediglich temporäre Fremdvergabe von unternehmensfremder Leistung zu unterscheiden. Bei der temporären Fremdvergabe, auch als Lösungsgeschäft oder Systemintegration bezeichnet, werden mit externer Unterstützung bestimmte Projekte umgesetzt, die zeitlich begrenzt sind. Die Umstellung eines Computerbetriebssystems kann beispielsweise im Rahmen der temporären Fremdvergabe erfolgen. Im Falle des Outsourcings selbst handelt es sich jedoch um die Übertragung von Aufgaben, die nicht zu den Kernkompetenzen gehören, aber dennoch den täglichen Regelbetrieb betreffen. Somit fällt der Betrieb von Rechenzentren und damit die Verarbeitung von Daten sowie die Betreuung unter den Begriff IT-Outsourcing. Unterschiedliche Gründe sprechen dafür bestimmte Dienstleistungen auszugliedern. Zum einen steht die Kostenreduzierung im Vordergrund. Die öffentlichen Haushalte können mit dem Ausgliedern an externe Dienstleister finanziell entlastet werden. Ferner erfolgt eine Reduzierung auf die Kernkompetenzen. Die Beschäftigten müssen sich nicht mehr mit Aufgabenbereichen beschäftigen für die ihnen die fachliche Kenntnis fehlt oder nicht ausreicht um z.B. ein technisches Problem zu lösen. Wichtige Punkte sind weiterhin die garantierten Service Level und das Know-How der Dienstleister. Die Rechenzentren bieten mit den

[58] Lt. Duden: „Outsourcing, das; -s <engl.> (Wirtsch. Übergabe von bestimmten Firmenbereichen an spezialisierte Dienstleistungsunternehmen)“.

Service-Level-Agreements einen gewissen Standard, der variabel ist und an die Anforderungen entsprechend angepasst werden kann. Allerdings sprechen auch Gründe gegen das Ausgliedern des IT-Betriebes. Auf der Contra Seite steht unter anderem der drohende Verlust von Entscheidungsspielräumen und die Abhängigkeit von dem externen IT-Dienstleister[59]. Mangels rechtlicher Definitionen[60] wird beim Thema Outsourcing häufig die Frage gestellt, ob ein Betriebsteil übergeht. In der öffentlichen Verwaltung und der Justiz geht allerdings kein Teilbereich der Tätigkeit über. Der Teilbereich der IT-Dienstleistungen bleibt als Querschnittsaufgabe eng mit den Behörden und Gerichten verzahnt, da es sich nicht um eine geschlossene Tätigkeit handelt. Dem steht auch nicht entgegen, dass andere öffentlich-rechtliche Einrichtungen diese Dienstleistungen erbringen.

6. Service-Level-Agreements

IT-Dienstleistungen werden durch Festlegung von Service-Level-Agreements dosiert. Es wird bestimmt mit welcher Qualität wiederkehrende Leistungen zu erbringen sind. Dadurch kann für bestimmte Dienstleistungen eine eingeschränkte Verfügbarkeit oder längere Reaktionszeit individuell vereinbart werden. Durch diese Agreements lassen sich die jeweiligen Anforderungen an die Servicequalität auch leichter überprüfen. Die vereinbarten SLAs müssen sich sinnvoll in ein Gesamtvertragswerk eingliedern und dürfen gesetzlichen Bestimmungen nicht entgegenstehen. Im Bereich der Informationstechnologie können SLAs beinhalten, in welchem Zeitraum der Zugang zu den unterstützenden Systemen gewährleistet werden muss. Ferner werden auch die sogenannten Service-Zeiten geregelt, in denen Störungsmeldungen entgegengenommen und bearbeitet werden. Hierzu gehören auch die Reaktions- und Widerherstellungszeiten im Falle von auftretenden Störungen. Weiterhin gehören die Problemlösungszeiten, die von der Einordnung in den jeweiligen Problemklassen abhängig sind, dazu. Der Zeitraum ist in den entsprechenden Vereinbarungen genau zu bestimmen, ebenso sollen die Rechtsfolgen konkret formuliert werden. Vorher bedarf es einer exakten Formulierung der jeweiligen messbaren Leistungen.

---

[59] Allgemein zu Vor- und Nachteilen: Söbbing, Handbuch IT-Outsourcing, 4. Aufl., Rn. 22 ff.

[60] Koch, Computer-Vertragsrecht, 7. Aufl., Rz. 1006.

7. BSI-Standards

Mit den BSI-Standards hat das Bundesamt für Sicherheit in der Informationstechnik einen Leitfaden geschaffen, der der fachlichen Unterstützung von Anwendern der Informationstechnik dienen soll. Sie sind als Empfehlungen in Bezug auf die Informationssicherheit zu sehen und erleichtern die sichere Nutzung. Behörden und Unternehmen können unter Anpassung an ihre eigenen Anforderungen auf die BSI-Standards zurückgreifen. Die allgemeinen Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) werden definiert.[61] In den IT-Grundschutz-Katalogen sind Bausteine für typische Anwendungen und Prozesse enthalten, die möglichen Gefährdungen sind beschrieben und Empfehlungen zu Sicherheitsmaßnahmen werden darin ausgesprochen. So können sich die Betroffenen Anwender gezielt auf die für sie relevanten Bereiche konzentrieren. Bei der regelmäßigen Erweiterung und Aktualisierung werden technische Entwicklungen berücksichtigt. Ferner finden sich dort auch Hinweise, Hintergrundinformationen und entsprechende Beispiele im Hinblick auf die Erstellung eines Sicherheitskonzepts und die Umsetzung auf der technischen Ebene.[62] Darauf aufbauend ergeben sich aus BSI-Standard 100-4 Erläuterungen zur Etablierung und Aufrechterhaltung eines behördlichen Notfallmanagements.[63] Sofern Sicherheitsanforderungen über das normale Maß hinausgehen, kann auf die Risikoanalyse zurückgegriffen und eine ergänzende Sicherheitsanalyse mit Hilfe der BSI-Standard 100-3[64] angeschlossen werden. Die genannten Vorgehen bilden erprobte und effiziente Möglichkeiten auf die bei Bedarf zurückgegriffen werden sollte.

---

[61] https://www.bsi.bund.de/SharedDocs/BSI-Standard_1001., 29.03.2017, 17:11 Uhr.
[62] https://www.bsi.bund.de/SharedDocs/BSI-Standard_1002., 29.03.2017, 17:11 Uhr.
[63] https://www.bsi.bund.de/SharedDocs/BSI-Standard_1004, 29.03.2017, 17:11 Uhr.
[64] https://www.bsi.bund.de/SharedDocs/BSI-Standard_1003, 29.03.2017, 17:14 Uhr.

V. Datenschutzbeauftragte

Ganz abstrakt ausgedrückt, ist die Aufgabe des Datenschutzbeauftragten darauf hinzuwirken, dass das BDSG und die Landesdatenschutzgesetze eingehalten werden, § 4g Abs. 1 S. 1 BDSG. Der Datenschutzbeauftragte kann lediglich darauf hinwirken, denn die Umsetzung der datenschutzrechtlichen Vorschriften kann durch ihn nicht erfolgen. Er kontrolliert und analysiert somit den Stand des Datenschutzes in dem Unternehmen und macht ggfs. Vorschläge zur Verbesserung oder Implementierung einer Datenschutzorganisation. Dem Datenschutzbeauftragten selbst steht demnach keine Entscheidungsgewalt zu. Die Datenverarbeitungsprogramme werden durch ihn überwacht und präventive Maßnahmen eingesetzt, um Datenschutzverstöße zu vermeiden. In bestimmten Fällen schreibt das BDSG die Bestellung eines Datenschutzbeauftragten vor. Widmen sich mindestens 10 Mitarbeiten regelmäßig und bestimmungsgemäß der automatisierten Verarbeitung personenbezogener Daten, so ist die Bestellung erforderlich. „Ständig“ beschäftigt ist die Person, wenn sie für diese Aufgabe, die nicht ihre Hauptaufgabe zu sein braucht, vorgesehen ist und sie entsprechend wahrnimmt. Ständig bedeutet daher, dass der Mitarbeiter immer dann mit der Verarbeitung personenbezogener Daten beschäftigt ist, wenn die Tätigkeit anfällt. Auf den Anteil dieser Arbeit kommt es nicht an. Etwas Anderes gilt nur, wenn der Mitarbeiter nur gelegentlich mit der Datenverarbeitung zu tun hat. Dies gilt allerdings nur für die nicht-öffentlichen Stellen. Gemäß § 19a BlnDSG haben öffentliche Stellen Datenschutzbeauftragte zu bestellen. Es handelt sich folglich um eine „Sollvorschrift“ die nicht umgangen werden kann. Die Bestellung erfolgt schriftlich. Der Datenschutzbeauftragte muss die erforderliche Fachkunde und Zuverlässigkeit mitbringen. Allerdings sind diese Begriffe im Gesetz nicht definiert. Die Fachkunde umfasst die Erforderlichkeit von technischem Sachverstand, organisatorischen Kenntnissen und die Rechtskunde zu einschlägigen Datenschutzgesetzen sowie Sozialkompetenz. Für die Vermeidung von Interessenkonflikten, Charakterfestigkeit und Durchsetzungsvermögen steht die Zuverlässigkeit. Der Geschäftsführer oder Gleichstellungsbeauftragte kann aufgrund einer möglichen Interessenkollision nicht gleichzeitig Datenschutzbeauftragter sein. Für den behördlichen Datenschutzbeauftragten ist das Bestehen eines öffentlichen Dienst-/Arbeitsverhältnisses weitere Voraussetzung, § 19a Abs. 2 BlnDSG. Externe Datenschutzbeauftragte dürfen nicht mehr bestellt werden. Der Vorteil eines internen

Datenschutzbeauftragten ist, dass diesem die Behörde und Arbeitsabläufe bekannt sind.

Der Datenschutzbeauftragte ist weisungsfrei und kann sich in Datenschutzangelegenheiten unmittelbar an die Behördenleitung wenden. Weiterhin verantwortlich für die Rechtmäßigkeit der Datenverarbeitung und die Beachtung datenschutzrechtlicher Bestimmungen bleibt die Behördenleitung. Diese Aufgaben können nicht auf den Datenschutzbeauftragten übertragen werden. Der behördliche Datenschutzbeauftragte kontrolliert somit als neutrale und unabhängige Stelle die Einhaltung der datenschutzrechtlichen Bestimmungen. Seine Unabhängigkeit wurde im Jahre 2010 durch den Europäischen Gerichtshof[65] gestärkt. In dieser Entscheidung wird betont, dass die Unabhängigkeit der Datenschutzaufsichtsbehörde eingeführt wurde „um die von ihren Entscheidungen betroffenen Personen und Einrichtungen stärker zu schützen, und nicht, um diesen Kontrollstellen oder ihren Bevollmächtigten eine besondere Stellung zu verleihen“[66]. Durch die Novellierung des BlnDSG vom 2. Februar 2011 wurde die Rechtsaufsicht des Senates über den Beauftragten für Datenschutz und Informationsfreiheit gestrichen. Der Dienstaufsicht des Präsidenten des Abgeordnetenhauses unterliegt er nunmehr nur soweit seine Unabhängigkeit nicht beeinträchtigt wird, § 22 Abs. 2 S. 2 BlnDSG.

Gem. § 19a Abs. 1 S. 2 BlnDSG kann für mehrere Behörden und öffentliche Stellen auch ein gemeinsamer Datenschutzbeauftragter bestellt werden. Sinnvoll wäre allerdings die Bestellung eines Datenschutzbeauftragten für jedes Gericht. Dieser könnte individuell die rechtmäßige Anwendung von Datenverarbeitungsprogrammen überwachen, den Mitarbeitern bei Fragen zur Verfügung stehen und im Hinblick auf die fortschreitende Entwicklung der Informationstechnologie Informationen und Schulungen der Beschäftigten im Hause anbieten. Im Rahmen der Auftragsdatenverarbeitung könnte der Datenschutzbeauftragte die technisch-organisatorischen Maßnahmen beim Auftragsnehmer, in diesem Fall beim ITDZ, überprüfen und bei datenschutzrechtlichen Fragen, Anliegen und Beschwerden interner Ansprechpartner sein.

---

[65] NJW 2010, 1265 ff.
[66] ebenda, S. 1266.

VI. IT-Landesdienstleister

Die elektronische Justiz bedarf einer professionellen Organisation. Dies kann nur mithilfe von leistungsstarken IT-Dienstleistern umgesetzt werden. Bislang war sowohl der Einsatz von privaten als auch öffentlich-rechtlichen IT-Dienstleistern möglich. Es ist allerdings zu unterscheiden, welche Aufgaben bei der Errichtung und dem Betrieb der Systeme auf private Unternehmen übertragen werden können und welche Bereiche von der Erledigung durch private Dienstleister ausgeschlossen sind. Den rechtlichen Ausgangspunkt bildet Art. 33 Abs. 4 GG (Funktionsvorbehalte der öffentlichen Hand) und Art. 12 Abs. 1 GG (Berufs- und Gewerbefreiheit privater IT-Dienstleister). Weiterhin ist das Vergaberecht zu berücksichtigen. Eine Auftragsdatenvereinbarung i.S.d. § 3 BlnDSG liegt vor, sofern der Landesdienstleister die Dienstleistung weisungsabhängig erbringt, ein entsprechender Auftragsdatenverarbeitungsvertrag konstituierend ist und die Verantwortlichkeit weiterhin beim Auftraggeber verbleibt.

Für die Justizbehörden in Berlin ist das IT-Dienstleistungszentrum seit dem Jahre 2003 im Rahmen einer strategischen Partnerschaft der IT-Dienstleister. Er unterstützt die Justiz fachlich im Bereich der IuK-Technik und IT-Anwendungen bei den zu bewältigenden Aufgaben und übernimmt zur Verwirklichung der vereinbarten Ziele die Verantwortung für einen möglichst störungsfreien Betrieb der eingesetzten Technik bei der ordentlichen Gerichtsbarkeit im Rahmen der Servicevereinbarungen. Das IT-Dienstleistungszentrum Berlin ist als Anstalt des öffentlichen Rechts (AöR) ein eigenständiges Unternehmen, welches per Gesetz[67] mit einer öffentlichen Aufgabe betraut wurde. Die vollrechtsfähige juristische Person des öffentlichen Rechts wurde durch das Land Berlin errichtet. Gem. § 2 ITDZAöRG BE stellt das ITDZ den Berliner Behörden die erforderliche Informations- und Kommunikationstechnik zur Verfügung und betreibt die entsprechende Infrastruktur. Die Organe des ITDZ werden durch den Verwaltungsrat und den Vorstand gebildet, § 3 Absatz 1 ITDZAöRG BE. Letzterer ist auch der gesetzliche Vertreter und führt die Geschäfte der AöR. Die Überwachung der Ordnungsmäßigkeit erfolgt durch den Verwaltungsrat. Der Senat von Berlin ist der Anstaltsträger, somit die Senatsverwaltung für Inneres und Sport die Aufsichtsbehörde. Gegenüber den Verwaltungsratsmitgliedern wird die AöR durch

[67] GVBl. 2004, 459.

den Senat vertreten, § 4 Absatz 3 ITDZAöRG BE. Die Rechtsaufsicht über das ITDZ obliegt der Senatsverwaltung, § 7 ITDZAöRG BE. Damit unterliegt das ITDZ der vollziehenden Gewalt. Dies ist im Hinblick auf die verfassungsrechtlich verankerte Gewaltenteilung zu berücksichtigen.

Das ITDZ bietet den Berliner Gerichten eine moderne Vollausstattung mit Informations- und Telekommunikationstechnik. Dazu zählen unter anderem die Bereitstellung von Servern zur Steuerung und die Vernetzung der Standorte über das Berliner Landesnetz mit schneller und moderner Datenübertragung. Die Betreuung umfasst unter anderem die zentrale Benutzerunterstützung und Softwareverteilung. Das ITDZ, genaugenommen das Informationssicherheitsmanagementsystem sowie die technische und bauliche Infrastruktur der Dienstgebäude inklusive des Hochsicherheitsrechenzentrums wurde auf Basis von IT-Grundschutz mit dem BSI-Zertifikat (ISO 27001) ausgezeichnet. In diesem Rahmen wurden unter anderem die Prozesse der Informationssicherheit, die Systemlandschaft und die Ausrichtung an den IT-Sicherheitsgrundsätzen geprüft. Folglich kann davon ausgegangen werden, dass die Datenhaltung im ITDZ unter Umsetzung der BSI-Standards erfolgt.

VII. Verfassungsrechtliche Bedenken

Auf dezentralen Servern werden die Dokumente der Rechtsprechung gehalten. Die Administratoren des ITDZ haben Zugriff auf die Systemdateien und Dokumente. Sie verfügen über die technische Möglichkeit, sämtliche Dokumente einzusehen und zu verarbeiten. Im ersten Moment löst dies vielleicht noch kein Unbehagen aus, allerdings kann man diese Problematik an folgendem Szenario veranschaulichen:

Man stelle sich vor, die Mitarbeiter des ITDZ könnten sich außerhalb der Dienstzeiten Zugang zu den Gerichten verschaffen und in den Räumlichkeiten des Gerichts die Akten einsammeln um diese im ITDZ zu lagern.[68] Justizexterne Beschäftigte hätten dann die Möglichkeit Einblick in die Verfahrensakten, nebst Inhalten wie Vermerk und Entwürfe der zur Entscheidung befugten Personen, zu nehmen. Dieses Beispiel ist nicht nur befremdlich, sondern spricht auch gegen das tragende Organisationsprinzip

[68] Bertrams, NWVBl. 2010, 209 ff.

des Grundgesetzes,[69] nämlich gegen die Gewaltenteilung. Dies verursacht zahlreiche Befürchtungen und Probleme die es zu bewältigen gilt.[70]

Der Zugriff der Mitarbeiter ist jedoch nicht die einzige Stelle bei der Bedenken angebracht sind. Das ITDZ verarbeitet als Landesrechenzentrum nicht nur die Daten der Berliner Justiz. Zu den Kunden zählen auch unter anderem die Bezirksverwaltung, die Deutsche Rentenversicherung Bund sowie die Charité Berlin. Dementsprechend bedarf es aufgrund der besonderen Stellung der Justiz spezifische Vorkehrungen, auch gegen den unbefugten Zugriff durch sogenannte „Binnentäter". Folglich sind bestimmte Binnenschottungsmaßnahmen zu treffen und zusätzliche spezielle Kontrollmechanismen erforderlich, damit die Unabhängigkeit der Judikative gewahrt bleibt.

VIII. Rahmenbedingungen der Landesdienstleister

1. Bestehende Vereinbarungen in Berlin

Die Leistungen, die das ITDZ für die ordentliche Gerichtsbarkeit in Berlin erbringt, sind in einer entsprechend Servicevereinbarung und der Rahmenvereinbarung IMOG geregelt. Die Rahmenvereinbarungen IMOG stammen aus dem Jahre 2004 und sollen in diesem Jahr fortgeschrieben werden. Gegenstand der Vereinbarungen sind IT-Service einschließlich der standardisierten Service-Dienstleistungen und Service Level. Zu den IT-Dienstleistungen gehören unter anderem der geschützte Anschluss der Gerichte an das Berliner Landesnetz durch das VPN Justiz, der Betrieb der zentralen AULAK-Systeme und der IT-Betrieb in den jeweiligen Standorten auf Grundlage der SBC Technologie. Das ITDZ ist dabei verantwortlich für die sachengerechte Auswahl und Anwendung der Arbeitsmethoden durch qualifiziertes Personal und hat die Ermächtigung Subunternehmen zu beauftragen. Das Land Berlin, vertreten durch die Senatsverwaltung für Justiz ist gemäß § 3 BlnDSG jedoch weiterhin für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Diese hat somit für eine reibungslose Integration des Informationsmanagements zu sorgen. Die Datenverarbeitung erfolgt ausschließlich nach den Weisungen der Senatsverwaltung

[69] BVerfGE 3, 225 ff. = NJW 1954, 65.
[70] Held, Betrifft Justiz 2015, 27 ff.

der Justiz auf Grundlage der erstellten Sicherheitskonzepte unter Einsatz von informationstechnischer Hard- und Software. In der Vereinbarung werden der Senatsverwaltung entsprechende Kontrollrechte eingeräumt und bestimmt, dass Unbefugten der Zugang zu schutzwürdigen Daten zu verwehren ist, ferner die Verarbeitung und Einsicht zu versagen ist. Um dies zu gewährleisten, werden Zugriffsrechte auf die Systeme, Software und die Daten durch das ITDZ dokumentiert und vor einem Verarbeitungsprozess die Berechtigung der jeweiligen Person geprüft. Jegliche Veränderungen durch die Administratoren werden protokolliert und vier Wochen aufbewahrt. Aus diesen Protokollen sind die ausführende Person und der Zeitpunkt ersichtlich, an dem die Veränderung erfolgt ist. Ferner ergeben sich aus dem technisch erstellten Protokoll auch die Art und der Ablauf der Änderung.

Das ITDZ erbringt die vereinbarte Leistung derzeit für 11 Amtsgerichte, das Landgericht sowie für das Kammergericht. In den Dienstgebäuden werden die Leistungen des ITDZ an den jeweiligen Arbeitsplätzen überwiegend über die sogenannten Thin-Clients bezogen. Der Client stellt die Schnittstelle zwischen dem IT-System und dem Endanwender dar. Dazu gehören auch die Ein- und Ausgabe-Komponenten wie die Maus, der Monitor oder die Tastatur. Das Rechenzentrum stellt der ordentlichen Gerichtsbarkeit Software bzw. Anwendungen für die IT-Grundfunktionen bereit. Dazu gehören beispielsweise das Emailprogramm, das Intranet, das Windows Betriebssystem, MS-Office, Virenschutz u.a. Die erforderlichen Sicherheits-Updates und Servicepacks für die jeweiligen Anwendungen werden ebenfalls im Rahmen der vertraglich vereinbarten Leistung bereitgestellt. Zu weiteren Anwendungen gehören auch individuelle Software und die IT-Fachverfahren, wie beispielsweise AULAK. Der Verfahrensbetrieb der Fachverfahren ist jedoch in separaten Servicevereinbarungen geregelt und nicht Gegenstand der Rahmenvereinbarung.

Die Dienstleistung des ITDZ beinhaltet auch den ServiceDesk, über den Störungsmeldungen entgegengenommen und in einem Ticketsystem erfasst werden. Die Bearbeitung dieser Meldungen erfolgt wiederrum in einer dreistufigen Organisation nach den Regelungen des Service Level Agreements. Die Störungsmeldungen werden innerhalb der jeweiligen Servicezeiten der entsprechenden Service Level bearbeitet. Die Störungen wie Ausfall,

Einschränkungen oder Einzelfall-Störungen werden Problemklassen von 1 bis 3 zugeordnet. Bei einer besonderen Ausnahmesituation z.B. einem Totalausfall der vertraglich geschuldeten Nutzungsmöglichkeit handelt es sich um einen Katastrophenfall. In solchen Situationen ist eine uneingeschränkte Erreichbarkeit des ITDZ vereinbart und die erforderlichen Veranlassungen zur Widerherstellung der vertraglichen Nutzungsmöglichkeit der Leistung.

2. Datenspeicherung und Datensicherung

Die Datenspeicherung wird in drei Speicherklassen eingeordnet. Je nach Art und Einsatzgebiet der Daten erfolgt die Einordnung in die Kategorie A, B oder C. Von den Speicherklassen ist auch abhängig wie die Datensicherung erfolgt. Bei den Kategorien A und B erfolgt die Datenspeicherung im SAN (Storage Area Network). Hierbei handelt es sich um ein Datenspeicher-Netzwerk, in dem große Datenmengen gespeichert und bewegt werden können. Im SAN wird der gesamte Speicher unabhängig vom Standort und Betriebssystem zentral verwaltet und zu virtuellen Einheiten zusammengefasst. Der Zugriff auf diesen Speicher erfolgt über den Server im Data-Center (Hochsicherheitsrechenzentrum) des ITDZ. Die Kategorien A und B unterscheiden sich in der Verfügbarkeit und Performance. Hochverfügbar ist ein System, dass im Falle eines Ausfalles einer Komponente den IT-Betrieb mit einer ziemlichen hohen Wahrscheinlichkeit unterbricht. Performance ist gleichzusetzen mit Leistungsfähigkeit. In der Speicherplatzkategorie B erfolgt keine Performancezusage. Um die Funktionalität des Systems aufrechtzuerhalten wird außerdem ein vierteljährliches Wartungsfenster benötigt. Dieses Wartungsfenster wird benötigt, um Wartungsarbeiten am System durchzuführen oder Software-Updates einzuspielen. Dies sichert die Funktionsfähigkeit des Systems. Die Datensicherung in diesen Kategorien erfolgt an jedem Werktag, jedoch ohne Langzeitarchivierung.

In der Kategorie C wird der Speicherplatz über NAS bereitgestellt. Dabei handelt es sich um ein Gegenkonzept zu SAN, dass über eine breitere Angebotsbasis verfügt. Dieser einfach zu verwaltende Dateiserver wird grundsätzlich eingesetzt um ohne hohen Aufwand unabhängige Speicherkapazität bereitzustellen. Über diese Speicherplatzkategorie erfolgt die Langzeitspeicherung. Durch das Duplizieren des gesamten Plattenbereichs in ein getrennt aufgestelltes zusätzliches Plattensubsystem

werden die Daten gesichert. Ein wichtiger Vorteil von NAS besteht darin, unterschiedliche Clients am Netz Zugriff auf dieselben Dateien zu ermöglichen. Auch hier ist für die Aufrechterhaltung der Funktionalität ein vierteljährliches Wartungsfenster einzuräumen.

Vereinbart ist ebenfalls ein IT-Grundschutzkonformes Sicherheitsmanagement-System mit definierten Prozessen nach dem BSI 100-2[71]. Die Vorgehensweise nach IT-Grundschutz ist so gestaltet, dass möglichst kostengünstig ein angemessenes Sicherheitsniveau erreicht werden kann. Etwaige Vereinbarungen zu Sicherheitskonzepten sind nicht Bestandteil des Rahmenvertrages. Es wird lediglich bestimmt, dass dies im Rahmen eines gesonderten Vertrages zu regeln ist. Wie ein solches Sicherheitskonzept erstellt werden kann, die Auswahl angemessener Sicherheitsmaßnahmen und die entsprechende Umsetzung wird im BSI-Standard 100-2 erläutert.

Vertraglich vereinbart ist auch die regelmäßige Durchführung von sogenannten Management Reviews die eine Betriebsanalyse von Arbeitsabläufen ermöglichen. Dabei wird die qualitative und quantitative Ausführung und Umsetzung des Vertrages bewertet.

3. Vertragliche Bindung

Eine dauerhafte Gebundenheit der Justiz an den IT-Dienstleister ergibt sich aus dem Dienstleistungsvertrag nicht. Die Rahmenvereinbarung wurde zwar für einen längeren Zeitraum geschlossen, wie es im Falle des Outsourcings auch üblich ist, allerdings beinhaltet der Vertrag auch die Möglichkeit der Beendigung. Es werden Möglichkeiten der ordentlichen und außerordentlichen Kündigung eingeräumt und ein entsprechendes Beendigungsmanagement definiert. Die Justizverwaltung soll in der Lage sein, bei Bedarf einen anderen Dienstleister in Anspruch zu nehmen oder die IT-Leistungen wieder selbst zu erbringen. Inhalt der Rahmenvereinbarung IMOG ist jedoch auch die Möglichkeit die Vereinbarung zu ergänzen, soweit notwendige Regelungen festgestellt werden die bislang nicht berücksichtigt wurden. Gleiches gilt

[71] https://www.bsi.bund.de/SharedDocs/BSI-Standard_1002, 29.03.2017, 17:15 Uhr.

bei der Änderung von rechtlichen oder wirtschaftlichen Rahmenbedingungen oder bei Änderung der Datenverarbeitungstechnik. Die Rahmenvereinbarung bzw. die jeweilige Servicevereinbarung ist in diesem Fall entsprechend anzupassen. Dabei müssen in erster Linie selbstverständlich die Verfahrensverfügbarkeit und der IT-Betrieb für die ordentliche Gerichtsbarkeit gesichert bleiben.

IX. Verfassungsrechtliche Gebote

1. Rechtsschutz

Die Funktion der Justiz in einem Verfassungsstaat besteht in erster Linie in der Gewährleistung effektiven Rechtsschutzes. Dieses Recht wird durch Art. 19 Abs. 4 GG garantiert. Um diesen Rechtsschutz wirkungsvoll und zeitnah zu gewährleisten braucht die Justiz moderne, komfortable und schnelle Arbeitsabläufe. Der Einsatz moderner Informationstechnologie ist folglich mittelfristig funktional notwendig. Ein wichtiger Punkt im Rahmen der Modernisierung ist das Vertrauen des rechtssuchenden Bürgers in das elektronische System. Bei der elektronischen Kommunikation mit den Gerichten darf dieser nicht befürchten einer staatlichen Kontrolle zu unterliegen und aus diesem Grund den elektronischen Kontakt meiden.[72] Ferner gilt es bereits den Anschein einer befangenen Justiz zu vermeiden. Eine räumliche und organisatorische, für die Öffentlichkeit erkennbare Trennung, ist erforderlich um das Vertrauen in die Unabhängigkeit der Rechtsprechung zu stärken. Der Befürchtung der staatlichen Kontrolle kann nur durch die lückenlose Gewährleistung von IT-Sicherheit begegnet werden. Die Grundlage dafür bildet somit die Vertraulichkeit und Integrität der Kommunikation mit den Gerichten.

Sofern dies gewährleistet wird, kann davon ausgegangen werden, dass die Einführung von eJustice-Strukturen verfassungsrechtlich als geboten anzusehen ist. Ein dahingehendes Gebot kann mit dem Beschleunigungsgrundsatz begründet werden, demnach ist Rechtsschutz in angemessener Zeit zu gewähren. Nun ließe sich argumentieren, dass dieser Anforderung nur genügt wird, wenn der Staat Verfahren innerhalb der Zeit beendet, die im Falle der Existenz einer entsprechenden elektronischen Infrastruktur erforderlich wäre. Dass sich der

[72] Britz, DVBl 2007, 993 ff.

Justizgewährleistungsanspruch in zeitlicher Hinsicht derart verdichten kann und eine Handlungspflicht des Gesetzgebers anzunehmen ist, erkannte bereits das BVerfG: Der Staat habe die Gerichte so auszustatten, „wie es erforderlich ist, um die anstehenden Verfahren ohne vermeidbare Verzögerung abzuschließen."[73]

2. Gewaltenteilung

Die Staatsgewalt wird nach Art. 20 Abs. 2 S. 2 GG durch die vollziehende Gewalt, die Rechtsprechung und die besonderen Organe der Gesetzgebung ausgeübt. Damit wird der Grundsatz der Gewaltenteilung im Grundgesetz verankert[74] und beinhaltet ein tragendes Organisationsprinzip der Verfassung.[75] Das Gebot zielt insbesondere auf eine organisatorische Trennung der Judikative von den Behörden der Exekutive.[76] Die Speicherung verfahrensbezogener Daten in einer Untergliederung des Innenministeriums könnte den Grundsatz der Unabhängigkeit der Judikative verletzen.

Die Judikative wird durch Art. 92 GG als sachlich, persönlich und institutionell unabhängige Staatsgewalt konkretisiert.[77] Dadurch wird die rechtsprechende Gewalt zwar von jeglichen Einwirkungen abgeschirmt, allerdings ist eine Gewaltenverschränkung oftmals unumgänglich. So ist die Judikative personell weitestgehend abhängig von der Exekutive[78], denn die Justizverwaltung ist im herkömmlichen Sinne Exekutivverwaltung und weitgehend der Organisationsmacht der zuständigen Minister unterstellt.[79] Daraus resultiert in jüngster Zeit die verstärkte Forderung nach einer sogenannten richterlichen Selbstverwaltung.[80] Der Deutsche Richterbund sowie die Neuen Richtervereinigungen erbrachten dabei detaillierte Vorschläge zur Ablösung der Judikative von der Exekutive.[81] Beispielsweise schlägt

---

[73] BVerfG, Beschluss v. 12.12.1973 – 2 BvR 558/73.
[74] Papier, NJW 2002, 2585 ff.; Sennekamp, NVwZ 2010, 213-217.
[75] Sodan, GG, 3 Aufl. , Rz. 28 zu Art. 20 GG.
[76] BVerfG, Beschluss v. 17.12. 1969 - 2 BvR 271/68 –, BVerfGE 27, 312- 325.
[77] BGHZ 67, 184; BVerwGE 78, 216.
[78] Sodan, GG, 3. Aufl., Rz. 32 zu Art. 20 GG.
[79] Arbeitsgruppe „Zukunft" der BLK für Datenverarbeitung, JurPC Web-Dok. 202/2009, Abs. 79.
[80] Frank, KritV 2008, 405 ff.; Häuser, KritV 2008, 410 ff.; Böttcher, KritV 2008, 417 ff.; Schulte-Kellinghaus, ZRP 2008, 205 ff.
[81] Hochschild, ZRP 2011, 65 ff.; Gruber, ZRP 2009, 123 f.; Kramer, NJW 2009, 3079 ff.

der Deutsche Richterbund für die Selbstverwaltung ein „Zwei-Säulen-Modell“ vor, mit einen Justizverwaltungsrat an der Spitze, der aus Staatsanwälten und Richtern besteht die von einem Justizverwaltungsausschuss in den Verwaltungsrat gewählt werden. Mit einer solchen Änderung der Organisationsstrukturen würden gewiss die Bedenken hinsichtlich der Einflussnahme der Exekutive auf die Rechtsprechende Gewalt ausgeräumt werden, allerdings stößt dies an verfassungsrechtliche Grenzen. Eine autonome Dritte Gewalt führt zu einer Legitimationslücke. Zur Herauslösung aus der Ministerverantwortlichkeit der Verwaltung bedarf es demnach einer demokratischen Legitimation, an der es einer richterlichen Selbstverwaltung mangelt. Eine Anbindung an die Verwaltung bzw. an eine ununterbrochene auf das Volk zurückzuführende Legitimationskette ist unumgänglich.[82] Aus verfassungspolitischer Sicht besteht bei einer Selbstverwaltung der Justiz die Gefahr einer unerwünschten Binnenpolitisierung.[83] Dies spricht gegen eine justizielle Selbstverwaltung durch gewählte Mitglieder in Gestalt eines Justizverwaltungsrates.

Die Judikative ist somit weiterhin abhängig von organisatorischen Rahmenbedingungen, die durch die Justizverwaltung gestaltet und gesichert werden. Die Verwaltung stellt demnach die sachlichen Arbeitsgrundlagen der Gerichte zur Verfügung. Dies beinhaltet sowohl die Errichtung und Instandhaltung von Gerichtsgebäuden als auch alle zur Verbesserung der Arbeitsabläufe erforderlichen Maßnahmen. Damit auch die Ausstattung mit Informations- und Computertechnik. Der Einsatz von IT bleibt somit in weiten Teilen alleinige Angelegenheit der Justizverwaltung.

Fraglich ist, welche Auswirkungen dieser verfassungsrechtliche Grundsatz auf die Verarbeitung von Justizdaten beim ITDZ hat. Als Anstalt des öffentlichen Rechts unterliegt das ITDZ der Aufsicht der Senatsverwaltung für Inneres und Sport. Die Datenverarbeitung erfolgt jedoch auf Grundlage von Vereinbarungen mit der Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung. Die organisatorische Selbstständigkeit und Unabhängigkeit der rechtsprechenden Gewalt von der Exekutive könnte somit nicht hinreichend gewährleistet sein, da Daten der

[82] Papier, NJW 2002, 2588; Sennekamp, NVwZ 2010, 213 ff.
[83] Papier, ZRP 2009, 125.

Gerichte auf zentralen Servern gespeichert werden, die durch die Exekutive betrieben werden. Bei dem ITDZ handelt es sich somit um eine Einrichtung der Exekutive und nicht um eine justizeigne Betriebsstelle, welche Bestandteil der rechtsprechenden Gewalt oder dieser unterworfen ist. Der Betrieb des ITDZ erfolgt im Geschäftsbereich der vollziehenden Gewalt, somit im organisatorischen bestimmten Verantwortungsbereich des Innenministeriums. Bei der Zuordnung zu einem „justizfremden" Ressort könnte ein Verstoß gegen den Gewaltenteilungsgrundsatz vorliegen. Durch diese organisatorische Delegation verfügen die Administratoren des ITDZ technisch über die Möglichkeit sämtliche Daten der Berliner Gerichte einzusehen. Es stellt sich die Frage, ob dies ein Verstoß gegen das Gebot zur Wahrung der organisatorischen Selbstständigkeit der Gerichte darstellt. Aus den Entscheidungen des Bundesverfassungsgerichts[84] ergibt sich eindeutig, dass die Gerichte organisatorisch hinreichend von den Verwaltungsbehörden getrennt sein müssen.

Der Betrieb des Rechenzentrums im Geschäftsbereich des Innensenators erscheint allerdings nicht von vornherein verfassungswidrig. Beispielsweise liegt eine IT-Zentralisierung unter ressortfremder Führung bereits bei der Abwicklung der Justizkommunikation über das elektronische Gerichts- und Verwaltungspostfach (EGVP) vor. Das EGVP wurde unter anderem durch das Bundesverwaltungsgericht und den Bundesfinanzhof mit dem Bundesamt für Sicherheit in der Informationstechnik konzipiert. Bei der Software des elektronischen Gerichts- und Verwaltungspostfaches handelt es sich um einen erweiterten Briefkasten, welcher von den angemeldeten Teilnehmern zum Versand und Erhalt von Nachrichten genutzt werden kann. Die versandten Nachrichten werden mittels einer Signatureinrichtung signiert und mit dem erfolgreichen Versand liegt bereits ein Zugangsnachweis vor. Die rechtsverbindliche Unterschrift wird durch die Signatur ersetzt und bewirkt, dass nachträglich erfolgte Änderungen an dem Dokument sofort sichtbar sind.

Dagegen wurde die Speicherung von Verfahrensdaten auf Serversystemen, deren Betrieb durch die Exekutive erfolgt, in Nordrhein-Westfalen erheblich kritisiert.[85] Der

---

[84] BVerfG, Beschluss v. 17.12.1969 – 2 BvR 271, 342/68; BVerfG 27, 312, 321 und v. 03.06.1980 – 1 BvL 114/78 – BVerfGE 54, 159, 166.

[85] Bertrams, NWVBl. 2007, 205 ff.; 2010, 209 ff.

Verlust der Datenhoheit und der strategischen Entscheidungshoheit über die Grundsatzfragen der IT-Strukturen gefährdet demnach die Unabhängigkeit der Justiz als dritte Staatsgewalt.

Der Dienstgerichtshof Frankfurt[86] hat in seiner Entscheidung festgestellt, dass es sich bei dem Betrieb des EDV-Netzes der Justiz durch eine Institution der Exekutive nicht um einen Verstoß gegen das Gebot zur Wahrung der organisatorischen Selbständigkeit der Gerichte handelt. Es wurde jedoch ein entsprechendes Konzept entwickelt, welches verbindliche konkrete Regeln im Hinblick auf den Umgang mit richterlichen Dokumenten voraussetzt und die Kontrollmöglichkeiten der Richtergremien beinhalten muss. Sofern die Einhaltung dieser Regeln zur ordnungsgemäßen Administration transparent überwacht werden kann, ist es unerheblich in welchem Geschäftsbereich der zentrale IT-Betrieb organisatorisch eingegliedert ist. Soweit die Möglichkeit besteht soll die Verwaltung allerdings dennoch durch die Justiz selbst erfolgen.

Verwaltungsaufgaben haben die Gerichte als Teil der Staatsorganisation zu erfüllen. Diese stehen weder unmittelbar, noch mittelbar sachlich und organisatorisch in Zusammenhang mit Rechtsschutz und Rechtsprechung.[87] In Justizverwaltungsangelegenheiten handeln Gerichte als Behörden und können insoweit hierarchisch organisiert sein. Geht man davon aus, dass es sich bei der technischen Verwaltung des EDV-Netzes um eine gerichtliche Hilfsverwaltung handelt, ist kein Verstoß gegen die organisatorische Selbstständigkeit der Judikative gegeben. Das aus Art. 20 Abs. 2 S. 2, 92, 97 GG abgeleitete Gebot organisatorischer Selbstständigkeit gilt allein für den zentralen Bereich der Rechtspflege, zu dem die Hilfsverwaltung nicht gehört.[88] Zu den Aufgaben der Gerichtsverwaltung gehört die Bereitstellung von persönlichen und sachlichen Mitteln für die Tätigkeit der Gerichte. Zu den persönlichen Mittel zählen unter anderem die Bestellung der Beschäftigten der Gerichte und die anschließende Bearbeitung der Personalangelegenheiten. Der Bau und die Unterhaltung von Gerichtsgebäuden, sowie die Ausstattung mit Büromaterial und Mobiliar, jedoch auch die Bewirtschaftung mit den bereitgestellten

[86] OLG Frankfurt, Urteil v. 22.04.2010 – DGH 4/08.
[87] BGH NJW 1987, 1198 ff.
[88] von Münch/Kunig, GG 6. Auflage 2012, Art. 92 Rz. 8, 12.

Haushaltsmitteln umfassen die erforderlichen Sachmittel. Die Gerichtsverwaltung organisiert somit den gesamten Dienstbetrieb in den Gerichten. Heutzutage kann man durchaus davon ausgehen, dass die Ausstattung der Arbeitsplätze mit Computertechnik ebenfalls zu den notwendigen Sachmitteln zählt, da die Tätigkeit der Beschäftigten mittlerweile ohne eine Verwendung von Informationstechnik nicht möglich wäre. Im Bereich der Hilfsverwaltung ist die hinreichende Selbstständigkeit bereits dadurch gewährleistet, dass der Justizminister die Fachaufsicht über die Daten der Rechtspflege hat und bindende Anordnungen erteilen kann. Die Tatsache, dass die Ausstattung der Gerichte mit entsprechender Computertechnik im Bereich der Hilfsverwaltung liegt, ist nicht gleichzusetzen mit der Verarbeitung der auf dem Computer erzeugten Daten. Fraglich ist also, ob es sich bei der Verwaltung und Pflege von zentralen Servern um vergleichbare Verwaltungshandlungen handeln könnte. Die bereitgestellte Hard- und Software wird ebenfalls zur Erledigung der täglichen Arbeit verwendet. Der Unterschied besteht allerdings darin, dass die Produkte und Inhalte der richterlichen Arbeit bei der zentralen Datenhaltung in die Obhut der Exekutive gelangen. Folglich werden Verfahrensinhalte durch die zentrale Speicherung an eine andere Einrichtung transportiert. Dagegen erhält die Justizverwaltung als Exekutive das beschriebene Papier, welches der Richter für seine Tätigkeit nutzt, nicht zurück.[89] Die Datenhaltung geht somit über die übliche „Justiz-Hilfsverwaltung“ hinaus und erfordert in jedem Fall klare Mitsprache- und Kontrollmöglichkeiten der Justiz.

Die Arbeitsgruppe „Zukunft“ der Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz geht davon aus, dass es unerheblich ist, ob die Organisation dem Justizministerium oder dem Innenministerium obliegt.[90] Diese Schlussfolgerung ergibt sich daraus, dass es sich bei der IT-Organisation um eine reine Verwaltungstätigkeit der vollziehenden Gewalt handelt. Da die Justizverwaltung selbst dem Justizministerium untersteht, ist es unerheblich welche Institution der Exekutive nunmehr die Steuerung dieser Tätigkeiten übernimmt. Ferner wird davon ausgegangen, dass der Gewaltenteilungsgrundsatz dynamisch an den staatlichen

[89] Bertrams, NWVBl 2010, 209 ff.
[90] Arbeitsgruppe „Zukunft“ der BLK für Datenverarbeitung, JurPC Web-Dok. 202/2009, Abs. 94.

Wandel und die Informationstechnik anzupassen ist.[91] Dieser Ausführung ist zuzustimmen, zumal die Entwicklung der Informationstechnologie die Festlegung und Umsetzung von Zugriffsbeschränkung ermöglicht und die Schaffung von „datensicherem Raum“ technisch durchaus möglich ist.

Die Datenpflege und –haltung könnte verfassungsrechtlich ein weiteres Problem mit sich bringen. In der Zivilgerichtsbarkeit könnte in einem Gerichtsverfahren das ITDZ selbst beteiligt sein. Dies gestaltet sich äußerst problematisch, da das Rechenzentrum oder die Aufsichtsbehörde sowohl Beteiligter im Verfahren ist, als auch gleichzeitig die Hoheit der Daten innehat. Auch dieses Problem könnte mit entsprechenden Verschlüsselungen, datenschutzrechtlichen Sicherungen und mit der Vergabe von Zugriffsrechten behoben werden.

Auf die Revision der Vorsitzenden Richter hat der BGH[92] in den Gründen lediglich die Frage behandelt, ob die richterliche Unabhängigkeit durch die Überlassung des gerichtlichen EDV-Netzes an externe Dienstleister betroffen ist. Hinsichtlich des verfassungsrechtlichen Gebotes organisatorischer Selbstständigkeit der Gerichte erfolgten keine abschließenden Ausführungen, da die Prüfungskompetenzen sich auf angegriffenen Maßnahmen der Dienstaufsicht beschränken, § 26 Abs. 3 DRiG. Ob die Überlassung des gerichtlichen EDV-Netzes an externe Dienstleister mit Art. 20 Abs. 2 S. 2 GG und anderen Rechtsvorschriften vereinbar ist, hat das Richterdienstgericht nicht zu entscheiden gehabt. Diese Frage und die datenschutzrechtliche Prüfung der Maßnahme hat der BGH den Verwaltungsgerichten vorbehalten.[93] In der Verfassungsbeschwerde wurde gerügt, dass der BGH diese Prüfung fehlerhaft unterlassen hat. Mangels hinreichender Substantiierung betrachtet das BVerfG diese Rüge allerdings als unzulässig.[94] Eine abschließende Entscheidung des Bundesgerichts liegt dahingehend nicht vor.

---

[91] Arbeitsgruppe „Zukunft“ der BLK für Datenverarbeitung, JurPC Web.-Dok. 202/2009, Abs. 96.
[92] BGH Dienstgericht des Bundes, Urteil v. 06.10.2011 – RiZ (R) 7/10 = MMR 2012, 128.
[93] BGH, Urteil v. 24.11.1994 – RiZ (R) 4/94 –, juris = NJW 1995, 731 ff.
[94] NJW 2013, 2102.

Die Präsidenten der Verwaltungsgerichte in Nordrhein-Westfalen haben sich zu diesem Thema dahingehend positioniert, dass durch die Aufhebung der Datenhoheit und die Einschränkung der organisatorischen Selbstständigkeit der Gerichte ein wesentlicher Bestandteil des unabhängigen Rechtsprechungsbereichs nach Art. 20 Abs. 2 S. 2 GG beseitigt wird.[95] Soweit alle Bereiche der Informationstechnologie für die richterliche Tätigkeit als Maßnahmen der Hilfsverwaltung eingestuft werden, liegt in jedem Fall eine reine Verwaltungstätigkeit vor. In Bezug darauf, dass sich die Daten in der Obhut der Exekutive befinden ist die Transparenz durch Einräumung von Kontrollrechten zwingend erforderlich.

Nicht außer Betracht zu lassen ist die dienende Funktion der IT-Tätigkeit gegenüber der rechtsprechenden Gewalt. Sofern die inhaltliche Hoheit der Richter über ihre Tätigkeit gewahrt bleibt, widerspricht ein Rechenzentrum welches der Justizverwaltung zugeordnet ist genauso wenig dem Gewaltenteilungsgrundsatz wie die herkömmliche Verwaltung und Organisation der Justizbehörden.

Selbst wenn man davon ausgeht, dass durch das Hosten[96] der Justizdaten in Landesrechenzentren der öffentlichen Verwaltung das Gebot der organisatorischen Selbstständigkeit der Gerichte verletzt wird, folgt daraus nicht automatisch auch die Verletzung der richterlichen Unabhängigkeit. Diese verfassungsrechtlichen Aspekte konkretisieren sich zwar untereinander, sind dennoch getrennt zu betrachten. Für die Verletzung der Unabhängigkeit der Richter kommt es unter anderem darauf an, ob bestimmte Organisationseinheiten der Gerichte auf externe Dienstleister der Executive Abläufe mit sich bringen, die geeignet sind den richterlichen Entscheidungsprozess zu beeinträchtigen.

3. Ausübung hoheitsrechtlicher Befugnisse

Verfassungsrechtliche Bedenken könnten sich aus dem Funktionsvorbehalt des Art. 33 Abs. 4 GG ergeben. Demnach können hoheitliche Befugnisse nicht als ständige Aufgabe an private Dienstleister übertragen werden, sondern müssen in der Regel dem öffentlichen Dienst vorbehalten bleiben. Dennoch hat der Gesetzgeber in

[95] BDVR-Rundschreiben 2012, 87-88; beck-link 1020726.
[96] engl. betreiben, beherbergen, unterbringen.

unterschiedlichen Gesetzen für hoheitliche Maßnahmen Öffnungsklauseln vorgesehen.

Die Justiz muss weiterhin der verantwortliche Herr der Daten bleiben und hat für die Einhaltung datenschutzrechtlicher Bestimmungen Sorge zu tragen. Das Datenschutzkonzept ist somit im entsprechenden Rahmenvertrag zu regeln. Die Weisungsbefugnisse sind festzulegen und es ist zu bestimmen, welche Sensibilitätskriterien für die einzelnen Verfahren anzuwenden sind. Damit sind auch Bestimmungen hinsichtlich der Zugriffsrechte der Mitarbeiter des Dienstleisters zu treffen. Die datenschutzrechtlichen Bestimmungen sind nicht nur für die Fachverfahren zu treffen, sondern auch für die Verarbeitung und Speicherung von Daten in allgemeinen Standardverfahren wie z.B. den Textverarbeitungsprogrammen.

4. Richterliche Unabhängigkeit

Inwieweit ein Eingriff in die richterliche Unabhängigkeit vorliegen könnte ist fraglich. Die richterliche Unabhängigkeit wird durch Art. 97 GG garantiert. Art. 97 Abs. 1 GG verbietet jede vermeidbare Einflussnahme der Exekutive auf die spruchrichterliche Tätigkeit. Somit richtet sich diese Vorschrift gegen alle Versuche der Staatsgewalt auf Entscheidungen der Gerichte Einfluss zu nehmen, eine solche Einflussnahme zu ermöglichen oder die Rechtsstellung der Richter zu beeinflussen. Betrachtet man Art. 97 GG historisch, so umfasst die richterliche Unabhängigkeit die Unzulässigkeit von Weisungen gegenüber der rechtsprechenden Gewalt und dient „ausschließlich der Erfüllung der Justizgewährleistungspflicht, die sich aus dem Rechtspflegemonopol des Staates ergibt“[97]. Die Entscheidungen ergehen ohne jegliche Einflussnahme durch die Exekutive. Allerdings dient sie auch dem Schutz vor Eingriffen der Legislative.

Fraglich ist, ob für Staatsanwälte gleiches gilt. Es ist nicht unumstritten welcher Staatsgewalt die Staatsanwaltschaft zuzuordnen ist. Die Staatsanwaltschaft ist als Organ der Rechtspflege zur Objektivität verpflichtet und kann Verfahren unter Gesichtspunkten der Opportunität einstellen (§§ 153 ff. StPO). Bei diesen Einstellungen handelt es sich jedoch um Ermessensentscheidungen der Staatsanwälte

[97] Schaffer, BayVBl 1991, 641 ff.

und nicht um solche die in Rechtskraft erwachsen können. Entscheidungen mit dieser Fähigkeit zu treffen ist gerade das Wesenhafte der Rechtsprechung.[98] Somit bildet die Staatsanwaltschaft eine Institution sui generis im Bereich der Strafrechtspflege.[99] Auch nach dem Wortlaut des Art. 92 GG ist die Rechtsprechung den Richtern anvertraut. Demnach kann die Staatsanwaltschaft kein Teil der rechtsprechenden Gewalt sein. In der herrschenden Lehre wird der Staatsanwaltschaft aufgrund ihrer Gesetzesbindung eine Zwitterstellung zugeteilt. Es wird jedoch auch die Ansicht vertreten, dass sie ausschließlich der Exekutive zuzuordnen ist.[100] Zu welcher Staatsgewalt sie zuzuordnen ist, kann hier dahingestellt bleiben. In jedem Fall sollte die Tätigkeit der Staatsanwälte im Interesse des Rechtsstaates von externen Weisungen frei sein.[101]

Es stellt sich ferner die Frage, wie es sich mit der sachlichen Unabhängigkeit der Rechtspfleger verhält, die sich aus § 9 RPflG ergibt. Danach sind Rechtspfleger sachlich unabhängig und nur an das Gesetz gebunden. Rechtspfleger erledigen Aufgaben, die ihnen durch das Rechtspflegergesetz übertragen wurden, § 1 RPflG. Dann müsste ihnen bei der Erfüllung der nach § 3 RPflG übertragenen richterlichen Aufgaben die gleiche sachliche Unabhängigkeit wie den Richtern zukommen. Rechtspfleger haben aufgrund der Ausgestaltung ihres Aufgabenbereichs nicht die gleiche Rechtsstellung im Sinne des Verfassungsrechts wie Richter, denn Rechtspfleger sind Beamte und unterliegen Einschränkungen gemäß §§ 4 ff. RPflG.[102] Soweit sich bei der Bearbeitung einer Sache rechtliche Schwierigkeiten ergeben, hat der Rechtspfleger die Akte dem Richter vorzulegen, § 5 Abs. 1 Nr. 2 RPflG. Demzufolge steht die gewährleistete Selbstständigkeit der Rechtspfleger von vornherein unter einem Vorbehalt und entspricht nicht der verfassungsrechtlichen

---

[98] Jarass/Pieroth, GG, 14. Aufl. , Rz. 4 zu Art. 92.
[99] Roxin, DRiZ 1997, 109 ff.
[100] BVerfG, Urteil v. 20.02.2001 – 2 BvR 1444/00 -, BVerfGE 103, 142-164; Kissel/Mayer, GVG, 8. Aufl., § 141 Rn. 8; kritisch: Schäfer, NJW 2001, 1396-1397.
[101] Frank, ZRP 2010, 147.
[102] BVerfGE 54, 159 (172); 101, 397 (405); 56, 87 (127); Schmidt-Bleibtreu/Hofman/Henneke, GG, 13. Aufl., Rn. 41 zu Art. 92.

Unabhängigkeit der Richter.[103] Berücksichtigt man hier jedoch das Wesen der Rechtsprechung ist festzustellen, dass auch die Entscheidungen der Rechtspfleger der Rechtskraft fähig sind und die Verfahrensdaten der Rechtspfleger gleichermaßen einer zusätzlichen Sicherung bedürfen, denn die sachliche Unabhängigkeit der Rechtspfleger verbietet ebenfalls jede vermeidbare Einflussnahme durch die Exekutive.

Im weiteren Verlauf der Ausführungen wird aufgrund der eingehenden Schwerpunktsetzung lediglich von der richterlichen Tätigkeit und der Unabhängigkeit der rechtsprechenden Gewalt ausgegangen. Zu unterscheiden ist zunächst zwischen der sachlichen und der persönlichen Unabhängigkeit, die die Wesensmerkmale eines Richters bilden.

[103] BVerfG, Beschluss v. 20.01.1981- 2 BvL 2/80 = BVerfGE 56, 110- 128; BVerwG, Beschluss v. 14.01.1988 - 2 B 112/87 -, juris; BVerwG, Beschluss v. 15.02.1991 – 2 B 19/91 -, juris; BGH, Urteil v. 16.10.2008 – RiZ (R) 2/08 -, juris.

a. Sachliche Unabhängigkeit

Die sachliche Unabhängigkeit beinhaltet, dass Richter bei der Ausübung der judikativen Aufgaben nicht an Weisungen gebunden sind. Die Gewährleistung bezieht sich ausschließlich auf die „richterliche Tätigkeit", folglich nicht auf die einem Richter übertragenen Aufgaben der Gerichtsverwaltung. Dies ergibt sich aus dem Sinn und Zweck der Unabhängigkeitsgewähr, denn durch diese soll eine gerechte und von sachenfremden Einflüssen freie Rechtsprechung ermöglicht werden. Davon werden somit Justizverwaltungsaufgaben nicht erfasst.[104]

Die Unabhängigkeit des Richters von der Legislative soll verhindern, dass die gesetzgebende Gewalt unmittelbar Einfluss auf Entscheidungen in Gerichtsverfahren hat. Durch die Unabhängigkeit von der Exekutive können Entscheidungen frei von vermeidbarer Einflussnahme der Verwaltung getroffen werden. Einzelweisungen oder Verwaltungsvorschriften nehmen keinen Einfluss auf den Entscheidungsausspruch und alle diesem vorgehenden Verfahrensentscheidungen wie die Fristsetzung, Ladung, Terminsbestimmung u.a. Alle Schritte die zur Entscheidungsfindung erforderlich sind, werden durch den Begriff der Rechtsprechung miteingeschlossen. Folglich fallen in den Schutzbereich der richterlichen Unabhängigkeit alle der Rechtsfindung auch nur unmittelbar dienenden Verfahrensentscheidungen.[105] Richter können die Arbeitsprozesse damit eigenverantwortlich und frei von jeglicher Kontrolle gestalten. Somit richtet sich die sachliche Unabhängigkeit auch gegen die eigene Gerichtsverwaltung. Arbeitsabläufe können individuell und flexibel gestaltet werden. Dem Richter steht es folglich frei, wann und wo er seine Arbeit verrichtet.[106]

Die Dienstaufsicht ist hiervon zu unterscheiden. Sie erstreckt sich unter anderem auf eine offensichtlich fehlerhafte Amtsausübung.[107] Jegliche Maßnahmen, die den Inhalt der richterlichen Entscheidung betreffen, sind unzulässig soweit sie den „äußeren

---

[104] BVerfGE 38, 139-154.
[105] BGH, Urteil v. 24.11.1994 – RiZ (R) 4/94 -, juris = NJW 1995, 731; BGH, Urteil v. 10.01.1985 – RiZ (R) 7/84 -, BGHZ 93, 238-245; BGH, Urteil v. 31.01.1984 – RiZ (R) 3/83 -, BGHZ 90, 41-52; Friauf/Höfling (Hrsg.), GG, Bd. 5, Rn. 34 zu Art. 92.
[106] Schmidt-Bleibtreu/Hoffmann/Henneke, GG, 13. Aufl., Rz. 58 zu Art. 92.
[107] BGHZ 67, 184-190.

Ordnungsbereich“[108] überschreiten. Damit sind Tätigkeiten umfasst, die den Kern der Rechtsprechung betreffen und weitere übertragende Aufgaben die im Zusammenhang mit der Rechtsprechung stehen.

Die sachliche Unabhängigkeit beinhaltet auch die Unabhängigkeit gegenüber der Judikative selbst. Richter können somit unabhängig von den Entscheidungen übergeordneter Gerichte urteilen und auch ihre bisherige Rechtsprechung ändern. Nach dem Sinn und Zweck des Art. 97 GG sind Richter auch vor gesellschaftlicher Einflussnahme zu schützen.[109]

Durch die sachliche Unabhängigkeit soll ferner sichergestellt werden, dass die Richter bei ihrer Entscheidungsfindung nur durch das Gesetz, welches den maßgeblichen Richt- und Orientierungspunkt für die Entscheidung bildet, geleitet werden. Die sachliche Unabhängigkeit fungiert somit nicht nur als Abwehrrecht gegen unzulässige Eingriffe.

b. Persönliche Unabhängigkeit

Die persönliche Unabhängigkeit des Richters ist zwar für das vorstehende Thema nicht von erheblicher Bedeutung, soll jedoch nicht unerwähnt bleiben. Von der persönlichen Unabhängigkeit des Art. 97 Abs. 2 GG sind grundsätzlich nur die hauptamtlich und planmäßig angestellten Richter erfasst. Somit z.B. nicht die ehrenamtlichen Richter und die Richter auf Probe. Allerdings wird die sachliche Unabhängigkeit durch die persönliche Unabhängigkeit bedingt und letztere muss so weit gesichert sein, dass ersteres gewährleistet bleibt.[110] Für die nicht von Art. 97 Abs. 2 GG erfassten Richter ergibt sich das Mindestmaß an persönlicher Unabhängigkeit aus Art. 33 Abs. 5 GG, da zu den hergebrachten Grundsätzen des richterlichen Amtsrechts insbesondere die sachliche und persönliche Unabhängigkeit gehört.[111] Die persönliche Unabhängigkeit schützt die Richter vor Maßnahmen der Entlassung, Versetzung oder Amtsenthebung. Nach dem Grundsatz der Inamovibilität können solche Maßnahmen nur erhoben

[108] BGHZ 42, 163-176.
[109] Maunz/Dürig, GG, 78. Aufl., Art. 97 Rz. 93; a.A. Sendler, NJW 2001, 1909 ff.
[110] BVerfGE 14, 57.
[111] BVerfGE 55, 372.

werden, wenn ihnen eine richterliche Entscheidung zugrunde liegt, welche auf einer gesetzlichen Grundlage beruht.

c. Beeinträchtigung der Unabhängigkeit

aa. Kontrolle

Die Datenkontrolle bei den Rechenzentren erfolgt letztlich durch die Justizverwaltung bzw. durch die IT-Mitarbeiter und nicht durch die Richterschaft selbst. Die Richterschaft ist im Grund genommen abhängig von der Exekutive. Inwieweit auch eine Beeinflussung der Rechtsprechung stattfindet ist nicht unumstritten. Eine gewisse Abhängigkeit der Judikative von der gesetzgebenden Gewalt findet sich in vielerlei Hinsicht. Der Finanzminister entscheidet über Personal- und Sachmittel je nach Haushaltslage und vielerorts entscheidet der Justizminister über Beförderung und die Einstellung von Richtern. Folglich spielen für die Entscheidungen oftmals auch politische Einflüsse eine Rolle. Die Gewaltenteilung ist zwar ein tragendes Organisationsprinzip des Grundgesetzes,[112] allerdings kann die Verfassungswirklichkeit hiervon abweichen. Fraglich ist, ob die Exekutive tatsächliche Macht gegenüber der rechtsprechenden Gewalt inne hat und damit in der Lage ist die Richter dazu zu veranlassen, eigene Handlungsziele umzusetzen bzw. zu unterstützen. Davon unabhängig ist die Frage zu sehen, ob von dieser Machtausübung auch Gebrauch gemacht wird. Eine verbotene Einflussnahme liegt nach dem BVerfG[113] vor, wenn ein besonnener Richter wegen dem Gefühl des unkontrollierbaren Beobachtetwerdens von der Verwendung der zur Verfügung gestellten Arbeitsmittel absieht. Hierzu gehört auch eine mittelbare subtile und psychologische Einflussnahme. Die richterliche Unabhängigkeit kann durch Maßnahmen verletzt werden, die dazu bestimmt und geeignet sind, die Rechtsfindung durch psychischen Druck oder sonstige Weise zu beeinflussen. Es stellt sich nunmehr die Frage, wann es sich nach dem vom Verfassungsgericht gewählten Maßstab um einen „besonnen Richter“ handelt und wann dieser Richter salopp gesagt einfach „paranoid“ ist. Hochschild[114] verdeutlicht diese Problematik in seinem Beitrag an einem angenommenen Beispiel. Dies zeigt, dass eine Einflussnahme über den

[112] BVerfGE 3, 225 = NJW 1954, 65.
[113] NJW 2013, 2102-2103.
[114] Hochschild, ZRP 2011, 65 f.

Justizminister und den Gerichtspräsidenten auf die Richter möglich ist und auch bis in den Kernbereich der richterlichen Tätigkeit eingreifen könnte. Im ausgeführten Beispiel bewirken knappe Ressourcen, eine Steigerung der Arbeitsbelastung, personelle Knappheit im Hinblick auf die dienstliche Beurteilung und mögliche Beförderungen, dass Quantität der Arbeit vor Qualität steht. Schlussfolgernd daraus findet ein Eingriff in die Entscheidungsfindung statt, da die Verfahren möglicherweise nur noch „oberflächlich" bearbeitet werden um Verzögerungen des Falles zu vermeiden und hohe Erledigungszahlen vorzuweisen. Durch den Einsatz von Informationstechnik steigt die Möglichkeit einer solchen Kontrolle der Erledigungs- bzw. Bearbeitungszahlen ins Unermessliche. Die Richter haben ihre Tätigkeit jedoch nicht an Statistiken und Vorgaben der vollziehenden Staatsgewalt auszurichten, sondern nach dem Gesetz. Mit der elektronischen Bearbeitung von Verfahren besteht die Möglichkeit nachzuvollziehen, wann und wer die betreffenden Verfahren bearbeitet hat, sowie in welchem Umfang dies geschehen ist. Eine Leistungskontrolle ist allerdings gleichermaßen unzulässig wie untauglich, da die Qualität der einzelnen richterlichen Entscheidungen und damit die der Rechtsprechung nicht messbar sind. Leistungskontrollen dürfen und können nicht an quantitative Erledigungsleistungen gemessen werden. Zur Wahrung der richterlichen Unabhängigkeit ist folglich sicherzustellen, dass die Kontrolle die durch den Einsatz von Informationstechnik möglich ist, nicht durch die Gerichtsverwaltungen ausgeschöpft wird um die Arbeitsprozesse zu „überwachen".[115] Die technischen Möglichkeiten sind zwar nicht dazu bestimmt, jedoch geeignet das Verhalten und die Arbeitsleistung der Richter zu überwachen. Die auswertbare Protokollierung ist aus Sicherheitsgründen unumgänglich. Es muss somit gewährleistet werden, dass das Ausmaß der Kontrollen der Protokolle verhältnismäßig bleibt. Dies hat unter anderem unter Zuhilfenahme der notwendigen technisch-organisatorischen Maßnahmen nach dem BlnDSG zu erfolgen. Das Ausmaß der Protokollierung kann durch entsprechende Konfiguration der Technik bis auf das Erforderlichste eingeschränkt und der Rahmen der Verhältnismäßigkeit durch Dienstvereinbarungen bestimmt werden.

[115] Berlit, Betrifft Justiz 2015, 15 ff.

bb. Homeoffice

Mit dem Einzug der Informationstechnologie in die Justiz obliegt die Entscheidung, wann und wo die Richterschaft die anfallende Arbeit verrichtet teilweise nicht mehr alleine der Entscheidung der Richter. Auf individuelle Gestaltungswünsche kann im Vergleich zur Bearbeitung einer Papierakte immer weniger eingegangen werden. So ist die Möglichkeit der mobilen Arbeit bzw. Heimarbeit nicht mehr ohne einen strengen Blick auf die Datenschutzvorkehrungen möglich. Zu Berücksichtigen ist die Tatsache, dass die meisten Arbeitsplätze mit Thin-Clients ausgestattet sind und bei diesen die Nutzung eines USB-Sticks nicht möglich ist, da schlichtweg das entsprechende Laufwerk fehlt. Sofern jedoch eine USB-Schnittstelle vorhanden ist, ist im Hinblick auf die IT-Sicherheitsvorkehrungen zum Datenaustausch eine zentrale „Datenschleuse“ mit einem Virenschutzprogramm aufzusuchen. Der Datenaustausch zwischen dem dienstlichen Computer und dem privaten Endgerät erfordert somit einen entsprechenden Aufwand. Ausweichreaktionen, nämlich den Versand sensibler Daten per Email an den „Heimarbeitsplatz“, gilt es zu vermeiden. Der Versand von sensiblen Daten außerhalb des Landesnetzes bringt erhebliche Risiken mit sich, die es zu umgehen gilt. Zum einen besteht die Möglichkeit für den Datenaustausch einen gesicherten USB-Stick zu verwenden. Dieser wird von den meisten Justizverwaltungen für Mitarbeiter zur Verfügung gestellt, die die Möglichkeit der Heimarbeit in Anspruch nehmen. Zum anderen ist auch die Verschlüsselung von Word und Pdf-Dateien unproblematisch möglich. Anhänge können in einer Email kennwortgeschützt übersandt werden. Das Öffnen dieser Anhänge ist nur mit dem entsprechenden Kennwort möglich. So kann verhindert werden, dass Daten im Versand abgefangen werden und an Unbefugte gelangen. Mithin schützt eine obligatorische Verschlüsselung nur vor externen Angriffen und solchen Binnentätern, die nicht die erforderlichen Administrationsrechte zur Einsicht besitzen. Die Verschlüsselung ist auch während der Erstellung einer Datei auf dem Dienstcomputer möglich. Jedoch wird selbstverständlich nicht etwa der Arbeitsspeicher des Computers verschlüsselt. Der Systemadministrator hat trotz Verschlüsselung die Möglichkeit durch Entschlüsselung auf die Dateien zuzugreifen.

Zur Integration privater mobiler Endgeräte hat der IT-Planungsrat eine offene Arbeitsgruppe eingerichtet, um Möglichkeiten aufzuzeigen, unter welchen

Rahmenbedingungen der Einsatz privater Endgeräte in der Verwaltung sinnvoll sein kann.[116] Der IT-Planungsrat wurde als oberstes Koordinationsgremium nach der Einführung des Art. 91 c GG gebildet. Es ist jedoch zu bemerken, dass den Vertretern der Justiz auch nach zahlreichen Gesprächen kein Sitz in diesem Gremium einräumt wurde. Es wurde lediglich in § 10 der Geschäftsordnung festgestellt, dass „die aus verfassungs- und einfachrechtlichen garantierten Positionen der unabhängigen Rechtspflegeorgane resultierenden Besonderheiten“ durch das Koordinationsgremium beachtet werden.[117]

cc. Ausstattung der Arbeitsplätze

Der den Richtern übertragene Justizgewährungsanspruch kann nur dann effektiv und sachgerecht erfüllt werden, wenn die hierfür notwendige Ausstattung zur Verfügung gestellt wird und die richterliche Unabhängigkeit garantiert wird. Der BGH[118] hat in seiner Entscheidung in Bezug auf die richterliche Beurteilung deutlich betont, dass die richterliche Unabhängigkeit kein Grundrecht bzw. Privileg der Richter ist. Überdies haben die Richter nur einen Anspruch darauf, bei der Zuteilung der für ihre Tätigkeit erforderlichen sachlichen und personellen Mittel in ermessensfehlerfreien Weise berücksichtigt zu werden.[119] Ihre Rechtsstellung wird nicht um ihrer selbst Willen garantiert, sondern soll sie gegen jegliche sachfremde Einflussnahme von außen absichern. Der Justizgewährleistungsgrundsatz der Bürger ist nur auf diese Weise gesichert. Bei dem Gebot aus Art. 92 GG handelt es sich mithin um ein objektives und kein subjektives Recht, das dem einzelnen Richter zusteht.[120] Die Beeinträchtigung der Unabhängigkeit kann freilich auch durch Anordnungen erfolgen, die im Zusammenhang mit der Benutzung von Hilfsmitteln stehen, die für die tägliche Arbeit benötigt werden. Dies resultiert daraus, dass alle der Entscheidung mittelbar dienenden Handlungen bereits in den Schutzbereich des Art. 97 GG fallen. Maßnahmen wie die IT-Ausstattung fallen grundsätzlich in den äußeren Ordnungsbereich und können die richterliche Unabhängigkeit nur tangieren, wenn sie dazu bestimmt oder geeignet sind

---

[116] „Bring Your Own Device“, Beschluss 2015/25 des IT-Planungsrates v. 26.06.2015, BAnz AT v. 19.08.2015, B1.
[117] http://www.cio.bund.de/it_planungsrat, 29.03.2017, 17:20 Uhr.
[118] BGH, Urteil v. 10.08.2001 – RiZ (R) 5/00 -, juris =
[119] BGH, Urteil v. 25.09.2002 – RiZ (R) 2/01-, juris = NJW 2003, 282.
[120] BGH, Urteil v. 21.10.2010 – RiZ (R) 5/09 –, juris.

die Entscheidungsfindung mittelbar oder unmittelbar zu beeinflussen. Wird die bereitgestellte Technik folglich nicht von den Richtern genutzt, weil sie beispielsweise veraltet ist oder ergonomische Nachteile befürchtet werden, liegt keine Verletzung der Unabhängigkeit vor. Ebenfalls schützt Art. 97 GG „nicht die Papierakte oder den Arbeitsplatzdrucker“[121]. Anders verhält es sich dagegen, wenn den Richtern keine Möglichkeit der alternativen Bearbeitung eingeräumt wird, als die Arbeit mit dem Dienstcomputer. Dies würde den relativen Anspruch gegen die Justizverwaltung auf entsprechende Ausstattung zumindest beschränken. Befürchtet der „besonnene Richter“ in diesem Fall eine unzulässige Kontrolle seiner Arbeit und greift deshalb eher zu Stift und Papier, liegt eine verbotene Einflussnahme und damit möglicherweise eine Verletzung der richterlichen Unabhängigkeit vor.[122] Selbst wenn Verfügungen und Entscheidungen von dem Richter handschriftlich verfasst werden, landen sie spätestens mit der Abfassung durch die Geschäftsstellenmitarbeiter schlussendlich mit den übrigen Daten auf dem zentralen Server. Letztlich wird es mit der Einführung der elektronischen Akte nicht mehr möglich sein die Nutzung der Computertechnik zu umgehen, folglich sind Vorkehrungen zu treffen die selbst einen „besonnenen Richter“ nicht zu der Annahme verleiten seine Daten wären nicht sicher. Der Anspruch auf eine angemessene IT-Ausstattung des richterlichen Arbeitsplatzes ist trotz der knapp bemessenen Mittel in den öffentlichen Haushalten bestmöglich zu erfüllen. Denn der Mangel an angemessener Hard- und Software und fehlende Fortbildungen für die Anwender gefährden das wesentliche Ziel der Modernisierung, nämlich die Steigerung der Effizienz.

d. Richterliche Unabhängigkeit als Grenze

Die richterliche Tätigkeit ist rechtlich und tatsächlich organisationsgebunden, allerdings bildet die rechtsprechende Tätigkeit die Grenze der Organisationsgewalt der Justizverwaltung sobald eine Rückwirkung auf die richterliche Entscheidungsfindung gegeben ist.

[121] Berlit, Betrifft Justiz 2015, 15 ff.
[122] NJW 2013, 2102-2103.

In einer Literaturmeinung[123] wird vertreten, dass die richterliche Unabhängigkeit nicht berührt ist, wenn es sich um Maßnahmen der Justizverwaltung handelt die keine unmittelbare Rückwirkung auf den richterlichen Entscheidungsprozess haben und solche, die der Verbesserung der Organisation dienen. Die verfassungsrechtlich garantierte Unabhängigkeit soll nicht der „Modernisierungsabwehr" dienen. Hier ist ein pragmatischer Weg einzuschlagen. Die Verfassungsgarantie wird als organisatorisch rechtlich-gestaltende eingestuft. Danach ist die Optimierung gerichtsinterner Verfahrensabläufe originärer Teil der richterlichen Verantwortung für die Systemleistungen und damit mit der richterlichen Unabhängigkeit kompatibel.[124] Zu dem Kernbereich der richterlichen Tätigkeit gehören diejenigen Aufgaben, die das Grundgesetz ausdrücklich den Richtern bzw. den Gerichten zugewiesen hat. Sieht der Gesetzgeber also ein gesetzförmiges Verfahren hoheitlicher Streitbeilegung vor und verleiht solchen Entscheidungen eine Rechtswirkung, die nur ein unabhängiges Gericht herbeizuführen vermag, dann handelt es sich funktional immer um Rechtsprechung. Im Widerspruch zur richterlichen Unabhängigkeit stehen auch solche Maßnahmen, die indirekt künftige Verfahren zu beeinträchtigen vermögen.[125] Eine Trennung der technischen Unterstützungstätigkeit der IT-Dienstleister von der rechtsprechenden Tätigkeit gestaltet sich immer schwieriger. Als Beispiel ist der Einsatz elektronischer Literatur- und Rechtsprechungsdatenbanken aufzuführen. Dadurch werden Arbeitsinhalte und –ergebnisse vorgeprägt, denn die moderne Technik ist nicht nur in der Lage die richterliche Arbeit durch inhaltliche Vorgaben zu unterstützen, sondern auch im Stande sie zu lenken. Der Zugriff auf juristische Datenbanken verändert die Rechtskultur. Heutzutage wird nicht mehr nur auf die herkömmliche Subsumtionstechnik zurückgegriffen, denn die Rechtsprechung beruht auch zunehmend auf Referenzentscheidungen. Durch die Online Datenbanken erlangt man schneller viele aktuelle Informationen, orientiert sich bei der Recherche aber auch an ähnlich gelagerten Fällen. Dadurch kommt es zu einem Richterrecht und zur Rechtsgleichheit.[126] Der erweitere Zugang zu Rechtsinformationen und die Vielfalt der Informationen ändert auch die methodische Herangehensweise an die Lösung von Fällen. Im Hinblick darauf ist es von großer Bedeutung, dass die vorformulierten

[123] Heckmann in: Bräutigam, IT-Outsourcing und Cloud Computing, 2. Aufl.
[124] Mackenroth, DRiZ 2000, 301 ff.
[125] BGH, NJW 2002, 359 ff. (361).
[126] Strauch, DVBl 2007, 1000 ff.

Verfügungen und Entscheidungen in den jeweiligen IT-Anwendungen nur als Alternative angeboten werden und eine schnelle Änderung durch den Anwender unproblematisch erfolgen kann. Standardisierte Vorgaben sind oftmals sicher eine Arbeitserleichterung, sie dürfen freilich nicht dazu führen, dass eine bestimmte Verfahrensweise zwingend gewählt werden müsste damit die Änderung nicht zu erheblicher Mehrarbeit führt und dadurch zumindest einen mittelbaren Druck auf den Anwender ausüben.[127] Die Anwendungen müssen weiterhin die eigenverantwortliche und individuelle Arbeitsweise der Richter ermöglichen und diese unterstützen.

Gegen die Einstufung der Verfassungsgarantie des Art. 97 GG als inhaltlich-abwehrende spricht in jedem Fall, dass die richterliche Unabhängigkeit nicht als Modernisierungsbremse fungieren darf und damit Strukturveränderungen verhindert werden.[128]

Es ist zu unterscheiden zwischen justizsensiblen Bereichen wie der elektronischen Aktenführung einerseits und exekutiven Dienstleistungsgegenständen wie das elektronische Handelsregister andererseits. Die Führung von elektronischen Registern als Verwaltungsaufgabe bringt keine Einschränkungen aufgrund Art. 92, 97 GG mit sich. Die justizsensiblen Bereiche erfordern jedoch eine starke Verschlüsselung und die eindeutige Festlegung von Rechten und Rollen der Datenverarbeiter. Sofern es um Justizdaten geht ist eine Festschreibung der Dienst- und Fachaufsicht der SenJus über das ITDZ bzw. deren Mitarbeiter erforderlich. Damit ist gewährleistet, dass der Judikative eine ausreichende Einwirkungs- und Gestaltungsmacht zukommt, um die gebotenen Schutz- und Kontrollstandards für den Datenschutz und die Datensicherheit zu bestimmen. Es stellt sich die Frage, was von dem Begriff der Fachaufsicht umfasst ist. Die Begrifflichkeit umfasst grundsätzlich sämtliche Mittel einer Verwaltungs-steuerung mithin Weisungen zur Verwirklichung von Zweckmäßigkeitserwägungen, Konzepten und Strategien sowie die Befugnis zur Rechtskontrolle.[129] Die Fachaufsicht

[127] Scholz, DRiZ 2011, 78 ff.; Scholz, DRiZ 2013, 284 ff.
[128] Hoffmann-Riem, DRiZ 2003, 284 ff.
[129] Groß DVBl. 2002, 793 ff.

geht über die Rechtsaufsicht hinaus, welche sich nur auf eine Kontrolle der Rechtmäßigkeit der Verwaltung beschränkt.[130]

Die Richterschaft ist in die Konzeption zwingend einzubeziehen. Eine IT-Kontrollkommission sollte wegen der sachlichen Unabhängigkeit der Rechtspfleger, die eine Einflussnahme durch die Exekutive ebenfalls verbietet, allerdings nicht nur gewählte Vertreter der Richterschaft enthalten, sondern auch Vertreter der Rechtspfleger. Dazu kann ein Vertreter des Personalrates herangezogen werden der nach § 2 RPflG mit den Aufgaben eines Rechtspflegers betraut ist.

[130] Hoffmann-Riem/Schmidt-Aßmann/Vosskuhle, Grundlagen des Verwaltungsrechts, 2. Aufl., Bd. I, § 10 Rz. 23 und § 14 Rz. 60.

X. Abhilfemöglichkeiten und Verbesserungsvorschläge

1. Lokale Speicherung

Um der zentralen Verarbeitung durch Justizexterne zu entgehen könnte eine lokale Speicherung in Betracht kommen. Zunächst ist festzustellen, dass ein Eingriff in die richterliche Unabhängigkeit nur denkbar ist, wenn es sich um Daten handelt, die vor Rechtskraft einer Entscheidung gespeichert werden. Genaugenommen sind nur die Daten betroffen, deren Speicherung vor der Verkündung erfolgt. In diesem Stadium des Verfahrens könnte die Einsichtnahme durch Dritte beeinflussend wirken. Die Kenntnisnahme durch Dritte könnte in den Entscheidungsprozess des Richter eingreifen, so dass gewisse Verfahrenshandlungen nicht dergestalt erfolgen, wie ohne die erlangte Kenntnis des Außenstehenden. Nach der Verkündung einer Entscheidung kann der Richter selbst eine Änderung grundsätzlich nicht mehr vornehmen. Dies wäre nur im Rahmen des Rechtsmittelverfahrens denkbar. Nach Rechtskraft berührt die Speicherung der Daten somit lediglich den Datenschutz und nicht mehr verfassungsrechtliche Aspekte. Zugriffsbefugnisse haben in diesem Verfahrensstadium nur noch Verfahrensbeteiligte und die Personen, deren Zugriff gesetzlich legitimiert ist. Ein Eingriff in die richterliche Unabhängigkeit ist folglich nicht mehr denkbar. Eine strikte Trennung zwischen Daten vor Verkündung und Daten bei denen keine Beeinflussung mehr in Betracht kommt könnte folglich verfassungsrechtliche Bedenken ausräumen. Die Datenhaltung müsste in diesem Fall an unterschiedlichen Orten erfolgen. Allerdings ist dies technisch kaum umsetzbar. Verfahrenshandlungen die die Entscheidung vorbereiten, werden unter Nutzung der Fachanwendungen erstellt. Eine interne Verarbeitung dieser Daten und die Übermittlung an den jeweiligen Server beim ITDZ nach Verkündung der Entscheidung, bedürfte zunächst eine Möglichkeit der Datenhaltung bei den einzelnen Gerichten bzw. der datenverarbeitenden Stelle.

Die Möglichkeit der lokalen Datenhaltung besteht jedoch nur sofern die bereitgestellte Hardware noch über integrierte Speichermedien verfügt. Notizen, Entwürfe und Vermerke, die die Entscheidungsfindung vorbereiten, können so im Machtbereich des jeweiligen Bearbeiters bleiben. Werden die Dokumente in dieser Form gespeichert, sind sie allerdings nicht vor Verlust oder technischer Beschädigung gesichert. Ferner

ist zu bemerken, dass gerade die eingeschränkte Nutzung des Systems einen Verstoß gegen die richterliche Unabhängigkeit darstellt, da eben nicht die Erleichterungen der modernen Infrastruktur genutzt werden und der Richter von der optimalen Nutzung der zur Verfügung gestellten Arbeitsmittel abgehalten wird. Die garantierte Gewährung effektiven Rechtsschutzes im Sinne des Art. 19 Abs. 4 GG wäre damit ebenfalls betroffen, soweit dies zu Effizienzeinbußen bei der richterlichen Arbeit führen würde.

2. Persönliche Ablage

Es stellt sich die Frage, ob eine Speicherung in der persönlichen Ablage die Zugriffe anderer umgehen würde. Jedem Nutzer ist in der SBC-Umgebung ein Home-Verzeichnis zugeordnet, welches zur Ablage solcher Daten bestimmt ist, die der Bearbeiter ausschließlich seinem Zugriff vorbehalten muss oder möchte. Die Speicherung erfolgt vielfach in diesem Laufwerk um die Daten vor jedem anderweitigen Zugriff zu sichern. Dateien oder Entwürfe, die nicht von unberechtigten Dritten gelesen werden sollen, können in diesem Verzeichnis abgelegt werden. Die Größe dieses Verzeichnisses ist jedoch beschränkt und die Anwender werden oftmals gebeten die Datenmenge auf das unbedingt Erforderliche zu reduzieren. Allerdings liegen die Zugriffsrechte für dieses Laufwerk nicht ausschließlich bei dem betroffenen Anwender. Der Administrator des ITDZ hat ebenfalls Zugriff auf die abgelegten Daten. Der administrative Zugriff der Mitarbeiter des ITDZ sollte hier ausgeschlossen sein. Soweit sich in der internen Handhabung Defizite durch fehlerhafte Benutzung durch Anwender ergeben sollten, müsste deren Behandlung der Dienstaufsicht der Behördenleitungen unterliegen und ist demnach dem lokalen Systemverwalter vorzubehalten. Ein absoluter Zugriffsschutz auf die in der persönlichen Ablage gespeicherten Daten lässt sich jedoch auch dann nicht realisieren, da administrative Zugriffe auf Dateiablagen oder Aufschaltungen auf die Computer der Anwender im Rahmen von Support- oder Migrationsfällen unverzichtbar sind.

3. Justizinterne Datenhaltung

Eine andere Ausweichmöglichkeit wäre die justizinterne Datenhaltung. Die Forderung nach einer Selbstverwaltung der Justiz[131] wird seit einiger Zeit von unterschiedlichen Seiten erhoben. Dies würde es ermöglichen rasch und flexibel auf die vor Ort bestehenden IT-Bedürfnisse einzugehen. Anregungen aus den Kreisen der Richter und anderer Justizbediensteter könnten unmittelbar und in enger Abstimmung mit den Anwendern umgesetzt werden. Eine direkte Einflussnahme auf die Arbeitsbedingungen wäre damit gewährleistet. Bei einer internen Datenhaltung wäre ein Verstoß gegen die organisatorische Selbstständigkeit der Judikative ausgeschlossen. Fraglich ist, ob gleiches auch hinsichtlich der richterlichen Unabhängigkeit gilt. Die Datenhaltung würde prinzipiell durch die Justizverwaltung erfolgen. Diese würde im Rahmen der Organisationsstruktur eines jeden Gerichts die erforderlichen Leistungen bereitstellen. Die Richterschaft und die übrigen Justizmitarbeiter könnten eine Kontrolle durch ein gewähltes Gremium sicherstellen. Es würden zwar lediglich die entsprechenden Mitarbeiter der Gerichte Zugriff auf die Daten haben, allerdings könnte sich im Falle einer dezentralen Datenhaltung bei den einzelnen Gerichten auch eine Verschlechterung der technischen Entwicklung ergeben. Aufgrund der Schnelllebigkeit der technischen Entwicklung besitzt die öffentliche Hand alleine nicht die notwendigen Kompetenzen und es bedürfe einer Hinzuziehung von qualifizierten Mitarbeitern die den Gerichten unterstehen. Es steht außer Frage, dass eine zentrale Bereitstellung und Pflege der Programme durch große Rechenzentren eine optimale Ausstattung der Gerichte bedeutet, da die Erfahrung und Qualifikation der dort beschäftigten Mitarbeiter nicht gleichermaßen dezentral erfolgen kann und zugleich wirtschaftlich ist. Sicherlich darf die IT-Sicherheit der Justiz nicht von nur haushaltspolitischen Aspekten abhängig gemacht werden. Allerdings kann die Gewährleistung von richterlicher Unabhängigkeit auch nicht der Grund für unverhältnismäßigen Kosteneinsatz und veraltete technologische Rahmenbedingungen sein.[132]

---

[131] unter anderem: Steffen, ZRP 2008, 208; Schulte-Kellinghaus, KritV 2010, 256.
[132] Radke, jM 2016, 8.

4. Länderübergreifendes IT-Dienstleistungszentrum

Die Arbeitsgruppe der Bund-Länder Kommission für Informationstechnik hat bereits im Jahre 2009 eine länderübergreifende Lösung veröffentlicht.[133] Diese beinhaltet die Bereitstellung von IT-Diensten für alle 16 Bundesländer. Auf Grundlage des Art. 91 c GG wäre auch die Beteiligung des Bundes an einem „IT-Dienstleistungszentrum Justiz“ möglich. Damit könnte ein professioneller Betrieb unter Berücksichtigung der verfassungsrechtlich verankerten organisatorischen Selbstständigkeit der Justiz gewährleistet werden. Jegliche verfassungsrechtlichen Bedenken wären damit aus dem Weg geräumt. Zudem wäre diese Lösung sowohl wirtschaftlich, als auch ressourcenschonend. Eine solche Umsetzung ist jedoch nicht geplant und es verblieb lediglich bei einem Vorschlag.

5. Gemischt externe Datenhaltung

Um die externe zentrale Datenhaltung weiterhin zu ermöglichen und die richterliche Unabhängigkeit zu wahren ist sicherzustellen, dass die Justiz entweder für den Betrieb und die Konzeption der IT-Ausstattung selbst verantwortlich ist oder zumindest maßgeblichen Einfluss darauf hat. Bei einer externen Organisationsstruktur müssten weiterhin die Zugriffsrechte klar geregelt sein und kontrolliert werden. Die Richtervertretung ist bei den Kontrollmöglichkeiten zu beteiligen. Wie bereits ausgeführt wäre die Beteiligung eines Vertreters der Rechtspfleger ebenfalls sinnvoll. Zum einen um die Transparenz zu schaffen und zum anderen aber auch um die Akzeptanz zu fördern. Eine Lösungsmöglichkeit könnte darin bestehen beim ITDZ eine interne Justizgruppe einzurichten, die bestimmte administrative Aufgaben übernimmt. Bei diesen Personen sollte es sich um Mitarbeiter handeln, die dem Justizresort unterstehen und deren Dienstaufsicht der Behördenleitung obliegt. Ferner haben Beschäftigte aus der Justiz Kenntnisse über Verfahrensabläufe die zur schnellen und praxisnahen Administration beitragen könnten. Es stellt sich die Frage, welche Fachverfahren und Dienstleistungen von dieser Arbeitsgruppe übernommen werden sollten. Nachstehende Überlegungen sind vor dem Hintergrund erfolgt, dass die Datenhaltung und der Betrieb der entsprechenden Server in erster Linie nicht in die

[133] Arbeitsgruppe „Zukunft“ der BLK für Datenverarbeitung, JurPC Web-Dok. 202/2009, Abs. 1-126.

richterliche Unabhängigkeit eingreifen und wirtschaftlich für die Berliner Justiz ist. Zudem ist unter Hinweis auf die vereinbarten Kündigungsfristen zu bemerken, dass die Berliner Justiz die nächsten Jahre vertraglich an das Landesrechenzentrum gebunden ist und sich die ausschließlich justizinterne Datenhaltung in Bezug auf die Haushaltsmittel schwierig gestalten könnte.

a. Firewall

Der Betrieb der zentralen Justizfirewall sollte weiterhin durch die Mitarbeiter des ITDZ erfolgen. Dadurch wird das gesamte Rechnernetz vor unerwünschten Netzwerkzugriffen geschützt. Die Firewall bildet demnach ein Teil des Sicherheitskonzeptes. Datenpakete können so zusammenhängend analysiert und Anfragen entsprechend gefiltert werden. Hierbei handelt es sich um eine ressourcenschonende Lösung, denn durch eine zentrale Bereitstellung der Firewall für die gesamte Justiz können Kosten geringgehalten werden. Ferner besitzt das Landesrechenzentrum sowohl das notwendige Know-How als auch die technischen Mittel unerlaubten Zugriff von Anwendungen auf das Netz zu unterbinden.

b. SBC-Umgebung

Mit der SBC-Umgebung werden Anwendungsprogramme zentral bereitgestellt. Die Bereitstellung erfolgt über ein Client-Server-System. Der Server als zentrales System stellt die Anwendungen für die angeschlossenen Clients bereit. Die Anwendungen laufen nicht über die jeweiligen Arbeitsspeicher, sondern über den zentralen Anwendungsserver. Unterschiedliche Applikationen wie Office-Anwendungen können so bereitgehalten werden. Auch die Fachverfahren werden den Anwendern über die SBC-Umgebung zur Verfügung gestellt. Der Betrieb der SBC-Umgebung bedeutet folglich auch den Zugriff auf die einzelnen Fachanwendungen. Folglich ist die Übernahme durch die Justizgruppe höchstwahrscheinlich erforderlich. Dies hängt von den Fachverfahren ab, die in der Berliner Justiz genutzt werden.

c. AULAK und forumSTAR

Die IT-Anwendung AULAK ist in der Berliner Justiz als Fachverfahren für die gesamte ordentliche Gerichtsbarkeit im Einsatz. Der Betrieb der Anwendung, die

Datenspeicherung und –sicherung sowie der Systemsupport für diese Anwendung sollte durch die Justizgruppe beim ITDZ erfolgen. In den vorgenannten Verfahren handelt es sich überwiegend um Verfahren in denen richterliche Entscheidungen getroffen werden, folglich ist der „justizinterne“ Betrieb in jedem Fall erforderlich. Berlin ist Ende des Jahres 2009 dem Länderverbund forumSTAR beigetreten und beabsichtigt nunmehr AULAK in den nächsten Jahren durch die IT-Anwendung forumSTAR abzulösen. Die Basistechnik des bestehenden Fachverfahrens entspricht nicht mehr den zeitgemäßen Anforderungen und ist wegen der fehlenden Zukunftssicherheit abzulösen. Die Einführung von forumSTAR erfordert zwar einen erheblichen Einsatz von personellen und finanziellen Ressourcen, jedoch ist nach entsprechender Umsetzung eine finanzielle Entlastung des Landes Berlin zu erwarten. Beispielsweise wird die Anpassung der Fachanwendung zukünftig nicht alleine vom Land Berlin finanziert, sondern im Länderverbund mit Bayern, Brandenburg, Hamburg, Sachsen und anderen. Bis zur vollständigen Einführung wird in einigen Gerichten weiter das Fachverfahren AULAK genutzt und teilweise besteht ein Dualbetrieb mit AULAK für Altverfahren und forumSTAR für neue Verfahren. Die Betreuung von forumSTAR müsste somit ebenfalls durch die einzurichtende Justizgruppe beim ITDZ erfolgen.

d. AUMAV und EUMAV

Die Fachanwendungen AUMAV und EUMAV werden durch das Amtsgericht Wedding als zentrales Mahngericht genutzt. Die Bearbeitung erfolgt überwiegend maschinell. Die Anträge werden lediglich formell geprüft. Eine rechtliche Prüfung unterbleibt. Folglich handelt es sich um keinen Bereich indem richterliche Unabhängigkeit greifen würde. Gleiches gilt für die europäischen Mahnverfahren, für die das Amtsgericht Wedding zentral in Deutschland zuständig ist. Die Bereitstellung und Pflege dieser Fachanwendungen können somit beim ITDZ verbleiben.

e. AJUKA

Der Betrieb des Servers und die damit einhergehenden Aufgaben für die Anwendung AJUKA könnte ebenfalls weiterhin durch die Mitarbeiter der ITDZ erfolgen. Diese Anwendung wird von der Kosteneinziehungsstelle der Justiz für Zahlungsverfahren genutzt. Über AJUKA erfolgen beispielsweise Sollstellungen der KEJ zur Einziehung

von Gerichtskosten. Daneben wird für die Haushaltsplanaufstellung und die Bewirtschaftung der Haushaltsmittel das landesweite Kassenverfahren ProFiskal genutzt. Mit dieser Anwendung werden in den Gerichten auch die anfallenden Zahlungsvorgänge erledigt.

Für die weiteren Anwendungen der jeweiligen Fachverfahren könnte die Einordnung unter diesem Gesichtspunkt erfolgen. Im Hinblick auf eine „gemischt externen Datenhaltung“ ist anzumerken, dass sich eine Verschlechterung der Service-Level ergeben könnte und die technische Nutzung für den Endanwender nicht unbedingt verbessert wird. Dies resultiert daraus, dass zurzeit mehr Mitarbeiter beim IT-Dienstleister zur Verfügung stehen, die administrative Aufgaben für mehrere Behörden und andere Auftraggeber des Rechenzentrums erledigen. Fachverfahren werden beispielsweise gebündelt betreut, diese Maßnahme ist freilich mit geringeren Personalzahlen verbunden als die Betreuung einzelner. Die Verwaltung der Server aller Auftraggeber ermöglichen kürzere Wartungsfenster und schnellere Wiederherstellungszeiten. Erfolgt die Administration nur durch die Justizgruppe bzw. werden die administrativen Rechte auf ein geringes Maß beschränkt, so führt dies zwangsläufig zu Einbußen im Falle von Systemausfällen.

6. Änderungsvorschläge

Zur Sicherung der richterlichen Unabhängigkeit werden folgende Regelungen, auch im Hinblick auf die Entscheidung des Dienstgerichts Frankfurt am Main, als mindestens geboten angesehen:

a. Ein inhaltlicher Zugriff auf richterliche Dokumente durch die Mitarbeiter des ITDZ bedarf der vorherigen Mitteilung an die datenverarbeitende Stelle und den Betroffenen und ist nur im Falle einer notwendigen Reparatur zulässig. Alltägliche technische Fehler sind soweit möglich durch gerichtsinterne Administratoren zu beheben.

b. Richterliche Dokumente und die dazugehörigen Metadaten dürfen nicht an die Exekutive und sonstige Dritte weitergegeben werden. Ausnahmen können mit Zustimmung der datenverarbeitenden Stelle bei einem konkreten Verdacht des Missbrauchs des Netzes zu dienstfremden Zwecken zugelassen werden. Allerdings kann auch hier eine formlose Einsichtnahme nicht erfolgen. Wird beispielsweise ein Missbrauch des Internetzugangs oder eine Straftat vermutet, ist die Einsichtnahme disziplinar- oder strafrechtlich zu rechtfertigen.

c. Grundsätzlich ist weder ein dienstaufsichtlich zu begründende, noch die organisationsrechtlich begründete Auswertung der gespeicherten Daten, die auf die richterliche Tätigkeit zurückgehen, zulässig. Durch die Zugriffe auf den Server darf keine Erledigungskontrolle der Verfahren stattfinden.

d. Das sogenannte Masterpasswort und damit den Zugang zu allen Dateien sollte lediglich einer Person der Justizgruppe zur Verfügung stehen und ggfs. einem Vertreter dieser Person. Die Weitergabe ist streng zu untersagen. Der Zugriff der weiteren Administratoren ist entsprechend den vorherigen Überlegungen einzuschränken.

e. Technische und organisatorische Maßnahmen sind im Rahmen der institutionalisierten Kontrollbefugnis zu überprüfen. Die Prüfung hat durch die datenverarbeitende Stelle unter gleichberechtigter Mitwirkung der IT-Kontrollkommission zu erfolgen. Der

Umfang der Kontrolltätigkeit dieser Kommission und ihre genauen Befugnisse sind hinreichend klar zu regeln.

f. Jegliche Zugriffe auf richterliche Dokumente sind durch die Mitarbeiter entsprechend zu protokollieren und im Rahmen der regelmäßigen Kontrollen durch die Kommission vorzulegen. Aus dieser Dokumentierung muss sich ergeben, wann der Zugriff erfolgt ist, aus welchem Grund und wer die Zustimmung hierfür erteilt hat.

g. Durch die Schutzbedarfsanalyse ist festzulegen, dass die Daten der Justiz beim ITDZ auf „eigenen“ Servern gehostet werden und nicht auf gemeinschaftlich genutzten Servern mit den Daten der weiteren Auftraggeber des Landesrechenzentrums. Der jeweilige Server soll demnach ausschließlich für die Justizdaten verwendet werden. Damit kann verhindert werden, dass bei einem Systemupdate oder Systemreparaturen eine Datenvermengung erfolgt und Justizdaten versehentlich für Unbefugte einsehbar sind.

XI. Fazit

Die Entwicklung der Informationstechnologie birgt auch für die Berliner Justiz einen stetigen Wandel. Vor allem im Hinblick auf die Einführung der elektronischen Akte ist der Weg zu einer vollständig elektronischen Justiz in den nächsten Jahren zu ebnen. Die justizinterne Datenhaltung mag unter Berücksichtigung der verfassungsrechtlich verankerten Gewaltenteilung und Unabhängigkeit der Richter jegliche Bedenken aus dem Weg räumen, allerdings handelt es sich hierbei um eine Lösung die an anderer Stelle zu Einbußen führen würde. Die Inanspruchnahme von externen Landesdienstleistern ist technisch und datenschutzrechtlich die bessere Lösung, da die Kernkompetenzen der Justiz nicht im Bereich der Datenhaltung liegen und der Aufbau eigener Zusatzkompetenzen organisatorisch und haushaltspolitisch einen Aufwand erfordert, der durch die Auftragsdatenverarbeitung umgangen werden kann.

Um dennoch die Akzeptanz aller Beschäftigten der Justiz und auch der Richterschaft zu fördern, ist die Schaffung von Transparenz unumgänglich. Im Hinblick auf die Sonderstellung der Justiz ist bei der Inanspruchnahme von externen IT-Dienstleistern ein besonderes Augenmerk auf die verfassungsrechtlichen Grundsätze zu legen. Auch wenn diese aufgrund des stetigen Wandels in gewissem Maße anpassungsfähig sind, ist vor allem zu beachten, dass ein Zugriff Unberechtigter auf Justizdaten dennoch nicht zulässig ist. Die Daten der Justiz sind bei der Datenhaltung deshalb strikt von den Daten anderer Auftraggeber des jeweiligen Dienstleisters zu trennen, sodass die Verarbeitung auf gemeinsamen Servers ausgeschlossen ist. Alleine die Möglichkeit der Exekutive auf richterliche Dokumente, die die Entscheidung vorbereiten, ist auszuschließen. Um einen Zugriff und damit eine unzulässige Kontrolle der Exekutive, auch in Gestalt der Justizverwaltung, zu verhindern ist eine regelmäßige Prüfung der protokollierten Daten durch eine ausgewählte Kommission unabdingbar. Die Aufgaben einer solchen Kontrollkommission sind unter Berücksichtigung von Schutzbedarfsanalysen ausdrücklich festzuschreiben. Es gilt insbesondere jeglichen Anschein der Überwachung der Judikative durch die Exekutive zu vermeiden. Im Falle der Datenhaltung unter dem Dach der gesetzgebenden Gewalt, wie dem Innenministerium, ist ausdrücklich klarzustellen, dass die Fachaufsicht der Justizdaten ausschließlich dem Justizminister obliegt. Trotz Auftragsdatenverarbeitung hat immer die datenverarbeitende Stelle die Hoheit über die betreffenden Daten.

Um die verfassungsrechtlichen Anforderungen zu erfüllen, ist eine interne Justizgruppe mit der Verarbeitung solcher Daten zu betrauen, bei denen ein Eingriff in die richterliche Unabhängigkeit möglich wäre. Justizdaten bei denen ein derartiger Eingriff ausgeschlossen ist, können weiterhin durch das Landesrechenzentrum verarbeitet werden.

Der technologische Fortschritt ist nicht aufzuhalten und im Zeitalter rasanter technischer Entwicklung kann die Justiz nicht in der analogen Welt stehen bleiben. Dabei liegt es in der Natur der Dinge, dass die Entwicklung zunächst mit Skepsis sowie einer holprigen Einführungsphase mit Problemen und Verzögerungen verbunden ist. Die Vorteile der Technik werden nach einer gewissen Zeit jedoch für die meisten selbstverständlich und unverzichtbar.

Impressum

Herausgeber der Reihe
Dekan des Fachbereichs Rechtspflege

Auflage
35

Druck
HWR Berlin

Berlin, September 2017

www.hwr-berlin.de