Schleswig-Holsteinischer Landtag
Umdruck 18/5238

Prof. Dr. Berlit Leipzig, den 27. November 2015

Stellungnahme zu dem Entwurf eines
IT-Gesetzes für die Justiz des Landes Schleswig-Holstein (IT-Justizgesetz – ITJG)*

A. Allgemeines

I. Der Vorstoß der Landesregierung Schleswig-Holstein, die Datenhaltung (in) der Justiz Schleswig-Holstein durch Gesetz zu ordnen, ist richtig und wichtig. Mit dem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten (vom 10.10.2013, BGBl. I, 3786) hat der elektronische Rechtsverkehr (in) der Justiz einen wesentlichen Schritt voran gemacht. Inzwischen zweifelt niemand mehr ernsthaft an der zunehmenden Bedeutung der elektronischen Kommunikation auch für die justizielle Aufgabenerledigung. Das Positionspapier des Deutschen Richterbundes zum Elektronischen Rechtsverkehr und zu E-Akten (September 2015) und die „Gemeinsame Erklärung des Deutschen Richterbundes und des Deutschen Anwaltvereins zur Umsetzung des elektronischen Rechtsverkehrs“ (Oktober 2015) unterstreichen: In zentralen Berufsgruppen der Justiz die Erkenntnis angekommen ist, dass eine effektive und zeitgemäße Justiz in einer Informationsgesellschaft die Vorteile und Chancen der Digitalisierung nutzen muss, ohne damit deren langfristige Risiken und die bei der Einführung erwartbaren Probleme und Schwierigkeiten zu leugnen.

II. Der Gesetzentwurf betritt regelungstechnisch weitgehend Neuland. Nach dem Gesetz zur Errichtung der Informationstechnik-Stelle der hessischen Justiz (IT-Stelle) und zur Regelung justizorganisatorischer Angelegenheiten sowie zur Änderung von Rechtsvorschriften (v. 16.12.2011, HessGVBl. I, 778) ist es der zweite Vorstoß, den (flächendeckenden) Einsatz der Informations- und Kommunikationstechnik in der Justiz gesetzlich zu regeln, um den (auch verfassungsrechtlichen) Besonderheiten der Justiz Genüge zu tun.

Im Vergleich zu Hessen und einer Vielzahl weiterer Bundesländer kann das Land Schleswig-Holstein mit Dataport auf einen öffentlich-rechtlich organisierten, aber institutionell gesonderten Datenverarbeitungsdienstleister zurückgreifen. Der Gesetzentwurf entscheidet sich zu Recht dafür, die hierin liegenden Sicherheits-, Betriebs- und Performancevorteile einer professionellen, zentralisierten Betriebsstruktur zu nutzen, die zugleich unter Kontroll- und Überwachungsaspekten in Bezug auf eine rechtmäßige, unabhängigkeitswahrende Datenverarbeitung durch ihre besondere Umsetzungsstruktur spezifische Vorteile bietet.

III. Die institutionelle Sonderung der Justiz als Dritter Staatsgewalt, die aus dem Gewaltenteilungsgrundsatz folgt, verbietet eine Eingliederung der Datenhaltung (in) der Justiz in die sonstige (zentrale) Datenverarbeitung der öffentlichen Verwaltung. Die genaue Reichweite der aus dem Gewaltenteilungsgrundsatz folgenden Anforderungen an die Verselbstständigung der Datenhaltung (in) der Justiz ist umstritten.[1] Die im Gesetzentwurf herangezogene

---

* Stellung genommen wird aufgrund der Vorbefassung mit den Themen des Gesetzentwurfes u.a. als vom geschäftsführenden Vorstand beauftragtes Mitglied des Vorstandes des EDV-Gerichtstages e.V. Sie erfolgt nicht in dienstlicher Funktion als Richter am Bundesverwaltungsgericht.

1 S. etwa Bertrams, Eingriff in die Unabhängigkeit der dritten Gewalt durch Zentralisierung der IT-Organisation unter dem Dach der Exekutive, NWVBl. 2010, 209; Positionspapier der Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz „Welches Maß an IT-Zentralisierung verträgt die dritte Gewalt?“, CR 2009, Beilage zu Heft 8; Berlit, Rechtliche Rahmenbedingungen einer strategischen Neuausrichtung der IT- Struktur aus Sicht der Justiz (Kurzgutachten 2002), JurPC Web.-Dok. 201/2009.

Rechtsprechung der Richterdienstgerichte und der hierzu ergangene Beschluss des Bundesverfassungsgerichts schaffen insoweit keine abschließende Klarheit, weil sie das Problem ausschließlich aus der Perspektive der Anforderungen haben behandeln können, die sich aus der richterlichen Unabhängigkeit ergeben. Nicht entschieden ist hierdurch, ob daneben die institutionelle Sonderung der Justiz andere oder weitergehende Forderungen der Verselbstständigung der Datenhaltung (in) der Justiz oder deren Kontrolle durch die Gerichtsverwaltung (nicht: der ministerialen Justizverwaltung) fordert. Hier wird teils gefordert, dass die Justizrechenzentren nicht nur im Geschäftsbereich des Justizministeriums und unter dessen Aufsicht betrieben werden müssen, sondern dass Betrieb und Aufsicht – quasi „ministerialfrei“ - durch die Gerichtsverwaltung(en) zu erfolgen hat. Verfassungsrechtlich halte ich diese Auffassung nicht für zwingend. Institutionelle Sonderung (bei) der Datenhaltung ist kein Selbstzweck; sie soll die funktionsgerechte Aufgabenerledigung der Dritten Gewalt organisatorisch absichern. Entscheidend ist mithin die Wahrung von Schutz- und Sicherungszielen, nicht die institutionelle Sonderung als solche; sie ist nicht Selbstzweck.

In dem Spannungsfeld von Unabhängigkeit der Justiz und sicherheitsgewährender Professionalität großer Datenzentren halte ich es dann für die Erreichung der verfassungsgesetzlich vorgegebenen Schutzziele für effektiver, statt auf die institutionelle Zuordnung der physikalischen Datenhaltung auf die Beachtung eines definierten Sicherheitsniveaus zu setzen und bei externer Datenhaltung klar und rechtssicher die Aufsichts-, Kontroll-, Zugriffs- und Weitergaberechte so zu regeln, dass die Justiz selbst wirksam mit über eine mit ihren Anforderungen konforme Datenhaltung wachen kann.[2] Die Auftragsstruktur, die bei der Beauftragung von Dataport als öffentlich-rechtlichen Bindungen unterliegendem Dritten besteht, schafft hier einen flexiblen, strukturell tauglichen Rahmen.

IV. Bei allen Besonderheiten, die Justiz kennzeichnen, bleibt Justiz Ausübung öffentlicher Gewalt. Es bestehen Gemeinsamkeiten mit der Informations- und Kommunikationstechnik insb. der Exekutive. Die Grundentscheidung des Gesetzes, die IT-Infrastruktur der Gerichte und Staatsanwaltschaften nicht vollständig von derjenigen der Landesverwaltung zu lösen und weiterhin anzukoppeln an den ressortübergreifenden Einsatz von Informations- und Kommunikationstechnologien ist als solche fachlich sinnvoll. Sie ist nicht nur dem in der allgemeinen Begründung wiedergegebenen Aspekt geschuldet, dass zum Aufbau eines justizeigenen IT-Betriebs die erforderliche Anzahl von Stellen für qualifiziertes IT-Personal vor dem Hintergrund des landesweit anstehenden Personalabbaus nicht zu erwirtschaften sei. Diese Begründung wäre nicht geeignet, weitergehende verfassungsrechtliche Anforderungen auch an die Ausstattung der Justiz mit Personal und Mitteln zu verdrängen. Justiz ist eine notwendige Staatsgewalt, deren Mittelausstattung nicht im freien Belieben der anderen Staatsgewalt entsteht.

V. Der Titel des Gesetzes „IT-Gesetz für die Justiz des Landes Schleswig-Holstein“ ist zu weit gefasst. Der Gesetzentwurf widmet sich im Kern der Organisation der Datenhaltung (in) der Justiz. (s.a. § 1 E-IT JG: „organisatorische Rahmenbedingungen der zentralen Ausstattung der Gerichte und Staatsanwaltes des Landes Schleswig-Holstein mit der erforderlichen Information-und Kommunikationstechnik (IT) und deren Betreuung“) und dem Schutz der gespeicherten Justizdaten vor unbefugtem Zugriff. Dies ist notwendig und wichtig, aber für eine „elektronische Justiz“ nicht hinreichend.

- Weitergehender Regelungsbedarf besteht etwa in Bezug auf die Mitbestimmung im Bereich der IT-Entwicklung. Angesichts der Komplexität und Prozesstätigkeit der Entwicklung und Einführung von IT-Programmen und IT-Infrastruktur und der faktischen Unumkehrbarkeit von Entwicklungsergebnissen sind - nicht nur in der Justiz -

[2] Berlit, eJustice, eAkte und Richterschaft, BJ 2015, 15 (20); s. bereits ders., Richterliche Unabhängigkeit und elektronische Akte, JurPC Web.-Dok 77/2012, Abs. 37 ff., 43 ff.

neue Formen der stufenweisen entwicklungsbegleitenden, aber verbindlichen Mitbestimmung/-wirkung vorzusehen.[3]

- Zumindest nützlich ist auch, sich im Rahmen des bundesgesetzlich Möglichen auch klar für die Einführung einer (führenden) elektronischen Akte zu entscheiden und hierfür einen klaren, wenngleich hinreichend flexiblen Zeitplan vorzugeben. Dies schaffte für die Justiz (und die in ihr Tätigen) Handlungsgewissheit und Planungssicherheit und wäre geeignet, die weiteren Anstrengungen auf die Ausgestaltung der elektronischen Justiz und die Weiterentwicklung der elektronischen Kommunikation zu konzentrieren.
- Sinnvoller Regelungsgegenstand eines IT-Justizgesetzes ist auch, die wesentlichen technischen und organisatorischen Anforderungen zu benennen, die an die IT (in) der Justiz als Dritter Staatsgewalt zu stellen sind (z.B. Schaffung hinreichender Leitungskapazitäten, Verfügbarkeitsanforderungen, Gebot funktionsgerechter Unterstützung der spezifischen Arbeitsweisen der Justiz), übergreifende Ziele zu fixieren, die mit der (weiteren) Einführung elektronischer Prozesse in der Justiz verbunden sind, und (zumindest deklaratorisch und aus Akzeptanzgründen) die „Schutzziele" zu benennen, die bei jeder Datenhaltung (in) der Justiz zu beachten sind (Wahrung der richterlichen Unabhängigkeit; Beachtung der institutionellen Sonderung der Justiz als Dritter Staatsgewalt).

B. Zu den einzelnen Vorschriften

I. Geltungsbereich (§ 1)

1. § 1 E-ITJG bestimmt nicht den Geltungsbereich, sondern den Regelungsgegenstand. Unklar ist, warum Bezug genommen wird lediglich auf die „zentrale" Ausstattung der Gerichte und Staatsanwaltschaften mit der erforderlichen Informations- und Kommunikationstechnik, zumal in § 4 E-ITJG auch die dezentralen IT-Stellen angesprochen werden.

2. § 1 Abs. 2 E-ITJG stellt klar, dass die Bestimmungen des Dataport-Staatsvertrages unberührt bleiben. Dies erscheint selbstverständlich, weil der Landesgesetzgeber nicht einseitig einen mehrseitigen Staatsvertrag ändern kann. Die Kernaussage, dass Dataport auch für die Justiz der zentrale IT-Dienstleister des Landes ist, geht so unter. Sie mag ausdrücklich (klarstellend) in den Gesetzestext aufgenommen werden.

3. § 1 Abs. 2 E-ITJG lässt auch die bereits zu Dataport begründeten Benutzungsverhältnisse unberührt. Soweit es um bestehende Vertragsverhältnisse geht, ist auch dies lediglich deklaratorisch. Insoweit mag § 1 Abs. 2 E-ITJG indes auch als „Versteinerungsklausel" selbst für den Fall missverstanden werden, dass sich aus dem E-ITJG oder anderen Bestimmungen Abweichendes ergibt und sich so Anpassungsbedarfe in den vertraglichen Beziehungen zu Dataport ergeben.

II. Besondere Belange der Justiz (§ 2)

1. § 2 E-ITJG benennt einerseits Schutzziele, die sich aus den Besonderheiten der Justiz und der in ihr Tätigen ergeben, und regelt andererseits Vorkehrungen hierfür. Eine klarere Trennung dieser beiden Regelungsbereiche erscheint sinnvoll. Bei den „Schutzzielen" des § 2 Abs. 1 E-ITJG werden zudem die Umschreibung der Schutzziele und die Adressaten der

[3] S.a. Berlit, Elektronischer Rechtsverkehr – eine Herausforderung für die Justiz, JurPC Web.-Dok. 173/2013, Abs. 27 ff.

Regelung verbunden. Dies führt zu Unklarheiten. Satz 1 nennt neben den in § 1 Abs. 1 genannten obersten Landesbehörden auch die Unterstützung durch Data Port und andere IT-Dienstleister, ohne deutlich zu machen, ob diese gesetzesunmittelbar Adressat der gesetzlichen Berücksichtigungs- und Schutzpflichten oder lediglich – nach Maßgabe des § 2 Abs. 1 Satz 2 E-ITJG – vertraglich zu binden sind.

2. Die „Funktionsfähigkeit der Justiz" steht systematisch neben der richterlichen Unabhängigkeit, der sachlichen Unabhängigkeit der RechtspflegerInnen und den sich aus dem Legalitätsprinzip ergebenden besonderen Belange der Justiz, die insoweit keine „sonstigen" Belange sind. Die aus der richterlichen Unabhängigkeit folgenden Schutzziele werden pauschal vorausgesetzt, aber nicht ausdifferenziert (z.B. eigenständige und eigenverantwortliche Arbeitsweise; Ausschluss der Datennutzung zur Verhaltens- und Leistungskontrolle [mit klar definierten Ausnahmen im Bereich statthafter Dienstaufsicht]; „Abschirmung" der Justizdaten, insb. gegen die unbefugte Einsichtnahme durch Dritte und namentlich bei den öffentlichrechtlichen Fachgerichtsbarkeiten [auch jenseits des datenschutzrechtlich gebotenen Schutzes personenbezogener Daten]).

Erwogen werden mag, in einem § 2 Abs. 1/1 abstrakt die Schutzziele zusammenzufassen und – auch aus Akzeptanzgründen – auszudifferenzieren und in einem § 2 Abs. 1/2 die „Gewährleistungsverantwortlichen" zu benennen; in dem Umfang, in dem Dataport nach dem zu Grunde liegenden Staatsvertrag unmittelbar durch Landesgesetz rechtlich gebunden werden kann, sollte dies klargestellt werden.

Soweit bei der Einschaltung Dritter (hier sollte auf die sonst verwendete Terminologie „Dataport und andere externe IT-Dienstleister" zurückgegriffen werden, um klarzustellen, dass es sich nicht um sonstige Dritte handelt, die nicht in § 2 Abs. 1 Satz 1 E-ITJG genannt sind) die Einhaltung des Gesetzes (nur) vertraglich sicherzustellen ist, mag – aus Akzeptanzgründen – auch als Fehlerfolge erwogen werden, neben entsprechenden Vertragsanpassungspflichten auch die Nichtigkeit des Vertrages bei unzureichender vertraglicher Regelung anzusprechen.

Die Funktionsfähigkeit der Justiz sowie die sich aus der Unabhängigkeit „ergebenden besonderen Belange" sind nicht nur „zu berücksichtigen"; sie sind „sicherzustellen".

3. § 2 Abs. 2 E-ITJG formt den Gewaltenteilungsgrundsatz durch ein Trennungsgebot aus. Die „IT-Strukturen" der Gerichte und Staatsanwaltschaften sind von denen der Landesverwaltung „technisch" zu trennen. Dies ist im Ansatz zu unterstützen. Die weiteren Ausformungen dieses Ansatzes bedürfen aber der zumindest redaktionellen Überarbeitung, um das Gewollte klarzustellen.

Mir unklar ist z.B. der Begriff der „IT-Strukturen". Erfasst er nur die für die Datenhaltung (in) der Justiz erforderliche Hardware, die Nutzung der Hardware oder das Zusammenspiel von Hard- und Software bei der Datenhaltung? Eine „technische Trennung" kann sich nach meiner Vorstellung als „Nichttechniker" nur auf zu Grunde liegende Technik (Hardware) beziehen. Dies scheint mir ungewollt auch logische Trennungsvorkehrungen auszuschließen.

Das Gebot der „technischen" Trennung lässt offen, ob/in welchem Umfange diese Trennung durchgängig physikalisch erfolgen muss oder eine logische Trennung ausreicht. Der Begründung ist zu entnehmen, dass eine durchgängig auch physikalische Trennung wohl nicht angestrebt wird, wenn auf die „Schaffung geschlossener, voneinander abgeschotteter Benutzergruppen" abgestellt wird. Das Trennungsgebot wird nicht funktional bezogen auf das Schutzziel in § 2 Abs. 2 Satz 2 Halbs. 1 „Ausschluss unbefugter Einblicke in die richterliche, rechtspflegerische oder staatsanwaltschaftliche Tätigkeit".

Die einschränkende Formulierung in § 2 Abs. 2 Satz 2 E-ITJG, „soweit die in den Gerichten und Staatsanwaltschaften zum Einsatz kommende IT von den in § 1 Absatz 1 genannten Stellen bereitgestellt und betreut wird“, suggeriert, dass es in relevanten Umfange auch durch andere, nicht den Schutzgeboten des § 2 Abs. 2 E-ITJG unterliegende Stellen bereitgestellte und betreute IT gibt.

4. § 2 Abs. 2 Satz 2 E-ITJG untersagt grundsätzlich jeglichen Einblick in die richterliche, rechtspflegerische oder staatsanwaltschaftliche Tätigkeit, formuliert aber in den nachfolgenden Maßgaben hiervon zahlreiche Ausnahmen, die nicht der inhaltlichen Reichweite nach, wohl aber systematisch über reine „Maßgaben“ hinausgehen. Dies dient nicht der Regelungsklarheit. Vorzugswürdig ist ein Verbot jeglichen Einblicks in die richterliche, rechtspflegerische oder staatsanwaltschaftliche Tätigkeit, die nicht ausdrücklich durch oder aufgrund Gesetzes zugelassen ist. Dabei könnte auch klargestellt werden, ob ein Einblick in die „Tätigkeit“ bereits jeder Zugriff auf/Einblick in eine im Rahmen dieser Tätigkeit erstellte einzelne Datei bedeuten soll.

Diese Regelungsstruktur ermöglichte dann auch, in den jeweiligen Ausnahmeregelungen klarer die Adressaten und Ausnahmezwecke zu bestimmen. Die Regelungen des § 2 Abs. 2 Satz 2 Nrn. 1 bis 6 scheinen sich überwiegend an die Administratoren/die Betreiber von Dataport zu richten, enthalten partiell aber auch Regelungen, die eine Datenverwendung Dataport-externer Dritter (z.B. das für Justiz zuständige Ministerium oder die ihm nachgeordneten Stellen der Dienstaufsicht) erfassen. Hier wäre deutlich zwischen den jeweiligen Adressaten (und der Schutzrichtung der Regelungen gegen „Binnentäter“ im Rechenzentrum einerseits, gegen die Datennutzung zum Zwecke der Dienstaufsicht oder sonstigen Kontrolle durch die Justizverwaltung und gegen externe Dritte [bei unbefugtem Datenzugriff]) und der Art der Datenverwendung (interne Zugriffe; Weitergabe an Dritte/Externe) zu unterscheiden.

5. In Fällen einer unbefugten Einsichtnahme oder – vor allem – Weitergabe von Dokumenten oder Metadaten ist klarzustellen, dass die so unbefugt „genutzten“ Informationen einem strikten, umfassenden Verwertungsverbot unterliegen.

6. § 2 Abs. 2 E-ITJG zielt auf den Schutz vor Einblicken in die richterliche, rechtspflegerische oder staatsanwaltschaftliche Tätigkeit. Nicht ausdrücklich angesprochen wird indes die Frage einer verschlüsselten Ablage bestimmter Dokumente, die im Rahmen dieser Tätigkeit erstellt werden, ohne bereits Gegenstand der „offiziellen“ Gerichtsakte geworden zu sein (z.B. vorbereitende Notizen, Voten oder Urteilsentwürfe, die noch nicht in den Umlauf gegeben worden sind). Sachlich, aber auch als „vertrauensbildende Maßnahme“ scheint mir angezeigt, jedenfalls im Bereich der (vorbereitenden) richterlichen, rechtspflegerischen oder staatsanwaltschaftlichen Tätigkeit außerhalb der elektronischen Akte eine verschlüsselte Ablage mit einem allein durch den jeweiligen Akteur zu verwaltenden kryptographischen Schlüssel zumindest als Option verpflichtend anzubieten.

Eine obligatorische verschlüsselte Ablage der Gerichtsakten selbst sollte jedenfalls so lange nicht vorgesehen werden, als Performanceeinbußen nicht sicher und dauerhaft ausgeschlossen werden können.

7. § 2 Abs. 2 Satz 2 Nr. 1 Halbs. 1 E-ITJG sieht die Bestimmung „berechtigter InhaberInnen“ administrativer Zugänge vor. Auch aus der Begründung erschließt sich nicht eindeutig, wer in diesem Sinne „externe IT-Dienstleister“ sind. Werden auch die Dataport-internen AdministratorInnen erfasst? Oder sind nur die AdministratorInnen externer IT-Dienstleister erfasst, die weder zu Dataport gehören noch zu dezentralen IT-Stellen (§ 4 E-ITJG)? Wenn zusätzlich die Bedingungen einer „darüber hinaus erforderlichen Öffnung für weitere administrativ berechtigte Personen“ festzulegen sind, bleibt unklar, was mit „Öffnung“ gemeint ist, wie sich der Kreis der „administrativ berechtigten Personen definiert“ und vor allem – wer in welcher Form und in welchem Verfahren - die Bedingungen für diese Öffnung festlegt. Umschrieben

wird der Sache nach ein gestuftes Rechtekonzept, das Gegenstand der mit Dataport (oder einem anderen externen Dienstleister) zu treffenden Vereinbarungen zu sein hat und vorab in einer entsprechenden Dienstvereinbarung geregelt sein könnte.

§ 2 Abs. 2 Satz 2 Nr. 1 Halbs. 2 E-ITJG schreibt für den Fall einer unbefugten Öffnung eine Information der IT-Kontrollkommission (§ 5) und der betroffenen Gerichte und Staatsanwaltschaften sowie ein Verfahren zur Änderung der Zugangsgewährung vor. Systematisch vorzugswürdig scheint, Benachrichtigungs- und Unterrichtungspflichten in einer gesonderten Regelung zusammenzufassen und klar zu benennen, wer hiernach binnen welcher Fristen „berichtspflichtig" ist. Dann wäre auch das Verhältnis zu der in § 2 Abs. 2 Satz 2 Nr. 6 E-ITJG vorgesehenen Mitteilung über Zugriffsprotokollierung klarer.

8. Das an die AdministratorInnen gerichtete absolute Verbot, im Rahmen richterlicher, rechtspflegerischer oder staatsanwaltschaftlicher Tätigkeit erstellte Dokumente selbst einzusehen oder an Dritte weiterzugeben, ist nicht auf Dritte innerhalb der Justizverwaltung und/oder Zwecke der Dienstaufsicht beschränkt. Der Datenzugriff durch die Berechtigten (inkl. VertreterInnen und Geschäftsstellen/Serviceeinheiten) selbst zum Zwecke der rechtsprechenden, rechtspflegerischen oder staatsanwaltschaftlichen Tätigkeit scheint mit umfasst. Dies ist offenkundig nicht gewollt (und auch nicht sinnvoll). Zu bedenken ist aber auch die Weitergabe an Dritte, z.B. im Rahmen der elektronischen Akteneinsicht.

9. Das Verbot der Weitergabe von Meta- oder Protokolldaten (§ 2 Abs. 2 Satz 2 Nr. 3 E-ITJG) ist zu erweitern um das Verbot, solche Daten in einer Weise zusammenfassend aufzubereiten, die für Zwecke der Verhaltens- oder Leistungskontrolle geeignet (nicht: bestimmt) sind. Die in Nr. 3 zuzulassenden Ausnahmen zu Gunsten der Dienstaufsicht sind auf solche Meta- oder Protokolldaten zu beschränken, die im gerichtlichen Verfahren auch der Akteneinsicht durch die Prozess-/Verfahrensbeteiligten unterliegen.

10. Bei elektronischer Aktenführung, die in absehbarer Zeit angestrebt wird, sind die in Nr. 4 vorgesehenen Ausnahmen vom Verbot der Weitergabe an (auch justizinterne) Dritte dem Grunde nach unverzichtbar. Richterliche Unabhängigkeit wird auch in der elektronischen Justiz durch eine gesetzlich zugelassene Dienstaufsicht begrenzt. Bei der elektronischen Aktenführung ist das Problem u.a., dass - entsprechende Zugriffsrechte vorausgesetzt – der dienstaufsichtliche Zugriff von dem Einzelnen unbemerkt und gleichzeitig auf eine Vielzahl von Akten/Dokumenten erfolgen kann. Nr. 4 enthält keine Regelungen, die auf diese spezifischen Risiken reagieren.

Normiert werden sollten nicht „Ausnahmen" von den Nrn. 2 und 3, sondern Befugnisse zur Weitergabe von Dateien und Informationen. Dies schließt es auch aus, dass durch die datenhaltende Stelle im Auftrag der zur Dienstaufsicht befugten Stellen Auswertungs- und Analysetools eingesetzt und lediglich die so gewonnenen Erkenntnisse weitergegeben werden. Zeitpunkt, Art und Umfang einer Weitergabe zu Zwecken der Dienstaufsicht sind auch den von dienstaufsichtlichen Maßnahmen Betroffenen umgehend durch die datenhaltende Stelle auf direktem Wege bekanntzugeben (Transparenz). Die Weitergabe ist grundsätzlich auf die Dokumente zu einzelnen Verfahren und auch ausdrücklich auf bereits (rechtskräftig oder lediglich in der jeweiligen Instanz?) abgeschlossene Verfahren zu begrenzen.

Als verfahrensrechtliche Sicherung mag erwogen werden, für das Verfahren der Daten-/Informationsweitergabe zu Zwecken/auf Veranlassung der jeweiligen Dienstaufsicht als weitere Voraussetzung eine entsprechende Dienstvereinbarung vorzusehen, die von der datenhaltenden Stelle als weitere Übermittlungsvoraussetzung zu beachten ist. In dieser Dienstvereinbarung könnten dann auch die Ausnahmen von der Begrenzung der Datenweitergabe auf die Dokumente zu einzelnen Verfahren (etwa zum Zwecke umfassender Geschäftsprüfungen) oder – soweit dies für erforderlich gehalten wird - Sonder-/Eilübermittlungsbefugnisse vorgesehen werden. Die in § 8 E-ITJG (justizinterne Zugriffs-

rechte) vorgesehene Regelung, dass das für sie zuständige Ministerium „im Benehmen“ mit der IT-Kontrollkommission die entsprechenden Regelungen erlässt, schafft eine richter-/personalvertretungsrechtlich nicht vorgesehene Form der Beteiligung und vermischt begleitende Kontrolle mit prospektiven Gestaltungsbefugnissen.

11. Bei den weiteren Datenverwendungen nach § 2 Abs. 2 Satz 2 Nr. 5 E-ITJG ist die Verwendung, wenn es für die Gewährleistung der Ordnungsmäßigkeit eines automatisierten Verfahrens oder sonst für den Betrieb der IT-Struktur unerlässlich ist, aus meiner Sicht im Ansatz unproblematisch. Eine personenbezogene Verwendung der so möglicherweise gewonnenen Erkenntnisse, die zu Kontroll- oder Überwachungszwecken bestimmt oder geeignet wäre, ist damit regelmäßig nicht verbunden. Wegen der Unbestimmtheit der Ausnahmen zu Betriebszwecken mag das Verwendungs- und Weitergabeverbot zu Kontrollzwecken hier nochmals ausdrücklich normiert werden.

12. Nach § 2 Abs. 2 Satz 2 Nr. 6 E-ITJG ist jeglicher Datenzugriff zu protokollieren und dem Ministerium mitzuteilen. Zumindest die Einschränkung in der Begründung, dass sich dies nur auf Zugriffe durch AdministratorInnen erstrecke, ist in den Gesetzestext aufzunehmen; dem Wortlaut nach scheinen derzeit auch die Zugriffe durch berechtigte Nutzer erfasst.

13. Zu erwägen ist, bei schwerwiegenden Verstößen gegen Kenntnisnahme-, Weitergabe- oder Verwertungsverbote im Rahmen der Strafgewalt des Landes eine strafrechtliche Sanktion anzudrohen.

III. Datenschutz, Mitbestimmung (§ 3)

Die Regelungen zur Geltung des Landesdatenschutzgesetzes, spezialgesetzlicher Datenschutzregelungen sowie des Mitbestimmungsrechts sind ausweislich der Begründung lediglich deklaratorisch und unproblematisch. Vertan wird damit allerdings die Chance, die Mitbestimmungsrechte im IT-Bereich auszubauen und vor allem den spezifischen Anforderungen von IT-Innovationsprozessen anzupassen, indem sie flexibler und prozesshafter gestaltet werden. Dies gilt auch für das Problem der Mitbestimmung/Mitgestaltung der Vertretungsgremien in Bezug auf Entwicklungen in länderübergreifenden Entwicklungsvorhaben, wie sie in der Justiz nicht untypisch sind.[4]

Die Subsidiaritätsklausel des allgemeinen Datenschutzrechts (Vorrang spezialgesetzlicher Regelungen) stellt sicher, dass etwa abweichende Regelungen/Bestimmungen des E-ITJG Vorrang haben. Dies kommt etwa in Betracht im Hinblick auf die allgemeinen datenschutzrechtlichen Regelungen zur Datenverarbeitung im Auftrag.

IV. IT-Stellen (§ 4)

1. Der Gesetzentwurf entscheidet sich gegen ein Modell einer partiell verselbstständigten Datenhaltung von Justizdaten in der und durch die Gerichtsverwaltungen selbst. Dies ist eine verfassungsrechtlich mögliche und bei gesicherter Wahrung der Schutzziele auch vorzugswürdige Gestaltung. Angesichts von Größe und Gewicht der IT der Justiz innerhalb der „IT-Landschaft“ einer Landesverwaltung sprechen gute Gründe dafür, Organisation und Verantwortung für den Einsatz von IT in den Gerichten und Staatsanwaltschaften in der hierarchi-

[4] S.o. A. IV; s.a. Deutscher Richterbund, Positionspapier zum Elektronischen Rechtsverkehr und zu E-Akten, September 2015, Abschnitt V. (Mitbestimmung).

schen Ministerialverwaltung zu bündeln, um die spezifischen Belange von Justiz in der ressortübergreifenden Zusammenarbeit wirksam zur Geltung zu bringen.

2. Rechtsnatur und genaue Stellung der „justizeigenen" Gemeinsamen IT-Stelle (GemIT) innerhalb des für Justiz zuständigen Ministeriums bleibt allerdings unklar. Es handelt sich um eine Organisationseinheit des Ministeriums, die nicht kraft Gesetzes geschaffen werden muss, sondern der Organisationsgewalt des/der für das Ressort zuständigen MinisterIn. Das Ministerium für Justiz, Kultur und Europa des Landes Schleswig-Holstein scheint auch ein Rechtspflegeministerium zu sein, in dem die ministeriale Ressortzuständigkeiten für alle Fachgerichtsbarkeiten gebündelt sind; die GemIT ist also auch nicht erforderlich, um für den Bereich der in der Rechtspflege eingesetzten IT Ressortgrenzen zu überwinden. Nicht abschließend beurteilt werden kann, ob die Bildung einer derartigen Stelle nach der allgemeinen Organisation der ressortübergreifenden IT in Schleswig-Holstein erforderlich ist.

Eine auch durch Gesetz hervorgehobene Gemeinsame IT-Stelle unterstreicht zumindest symbolisch die gewachsene Bedeutung, die der Einsatz von IT für die justizielle Aufgabenerledigung hat. Die Bündelung der IT-Verantwortung für die Justiz auf der Ministerialebene reduziert indes die zumindest aus Akzeptanzgründen angezeigte Beteiligung der Gerichtsverwaltungen auf die ministerialintern regelmäßig unproblematisch möglichen Beteiligungsformen. Wenn schon für die konzeptionelle und operative Bearbeitung des zentralen justiziellen IT-Managements eine durch Gesetz hervorgehobene Stelle geschaffen wird, mag erwogen werden, dieser Stelle für grundlegende konzeptionelle Entscheidungen (z.B. Gestaltung des Auftrags-/Vertragsverhältnisses zu den externen IT-Dienstleister) einen Beirat zur Seite zu stellen, der aus den jeweiligen PräsidentInnen der Obergerichte sowie der/dem Generalstaatsanwalt/wältin besteht, dem (zumindest) das Recht zur Anhörung und – dann auch zu veröffentlichenden – Stellungnahme eingeräumt wird. Während die IT-Kontrollkommission (§ 5 E-ITJG) die Belange der richterlichen Unabhängigkeit repräsentiert, läge die Aufgabe dieses Beirates in der hiervon zu trennenden Betonung der institutionellen Eigenständigkeit der Justiz als dritter Staatsgewalt.

3. § 4 Abs. 2 E-ITJG sichert mit dezentralen IT-Stellen in den Gerichten und Staatsanwaltschaften einen mehrstufigen Aufbau der justizeigenen IT-Stellen gesetzlich ab und stellt so sicher, dass IT-Know how auch „vor Ort" in den Gerichten erhalten bleibt. Dies ist ein sinnvolles und richtiges Signal; es ist zumindest partiell auch der institutionellen Sonderung der Justiz geschuldet. Denn als die Repräsentanten der eigenständigen Staatsgewalt müssen die Gerichtsverwaltungen die personellen, technischen und organisatorischen Voraussetzungen für eine funktionsfähige justizielle Aufgabenerledigung sichern (können). Eine aufgabenadäquate und funktionsgerechte IT-Unterstützung kann auf Dauer nur gelingen, wenn Justiz über qualifiziertes IT-Personal mit Kenntnissen justizieller Abläufe verfügt, die eine fachgerechte Umsetzung der rechtlichen und funktionalen Anforderungen durch (interne oder externe) Programmierer gewährleisten können. Dies setzt einer beliebigen Dienstekonsolidierung oder dem Einsatz von allgemeinen Basis-Querschnittsdiensten ebenso Grenzen wie einer zu starken Zentralisierung innerhalb der (ministerialen) Justizverwaltung. Die vorgesehene Aufgabenabgrenzung im Detail durch Rechtsverordnung erscheint sinnvoll.

Wird dem Vorschlag gefolgt, der GemIT einen Beirat zur Seite zu stellen (s.o. Nr. 2), sollte diesem das Recht zur Anhörung/Stellungnahme zugewiesen werden; die Zuständigkeitsabgrenzung betrifft der Sache nach weniger eine Frage der Sicherung richterlicher Unabhängigkeit durch Organisationen denn einer für die justiziellen Aufgabenerledigung sachgerechten Mittel- und Kompetenzausstattung.

4. Sinnvoll sind die Kontroll- und Zutrittsrechte der GemIT bei den externen IT-Dienstleistern (§ 4 Abs. 3 E-ITJG). Die in Satz 2 bezeichneten Gegenstände der Kontrolle gehen über der Zweckbestimmung der Kontrolle „Schutz vor unbefugten Zugriffen" (Satz 1) hinaus; dieser Zweck ist entweder zu erweitern oder zu streichen.

Die uneingeschränkte Zutrittsrechtgewährung sowie die entsprechenden Auskunfts- und Einsichtsrechte der GemIT (Satz 3) können als gesetzesunmittelbare Rechte nur im Rahmen der Gesetzgebungskompetenz des Landes geregelt werden. Gegenüber privaten Dritten bedarf es wohl entsprechender vertraglicher Vereinbarungen allzumal dann, wenn die GemIT vertragschließende Partei ist. Nicht abschließend geprüft werden konnte, inwieweit es auch gegenüber Dataport der vertraglichen Absicherung entsprechender Rechte bedarf. Entsprechendes gilt für die der IT-Kontrollkommission eingeräumten Zutritts-, Auskunfts- und Einsichtsrechte (§ 5 Abs. 6 Satz E-ITJG).

In der Konsequenz einer umfassenden Kontrolle liegt die Kenntnisnahme von personenbezogenen Daten (Satz 4) und die Einsichtnahme in Dateien und Daten nach § 2 Abs. 2 Satz 2 Nrn. 2 und 3 E-ITJG (Satz 5). Die Datenverwendung zur „Aufgabenerfüllung" sollte dahin spezifiziert werden, dass die Verwendung nur zur Erfüllung der in Satz 2 genannten Zwecke statthaft ist; aus Akzeptanzgründen mag eine weitergehende Verwendung, insbesondere zu Zwecken der Dienstaufsicht, ausdrücklich ausgeschlossen werden.

5. Die Koordination bei der Ausübung der verschiedenen Kontroll- und Aufsichtsrechte (Abs. 4) und die Meldepflicht bei sicherheitsrelevanten Vorfällen sind sinnvoll und sachgerecht.

V. IT-Kontrollkommission

1. Die unabhängige IT-Kontrollkommission ist ein Herzstück des Gesetzentwurfes. Sie dient im Anschluss an die richterdienstgerichtliche Rechtsprechung der Kontrolle der zur Sicherung der richterlichen Unabhängigkeit getroffenen Vorkehrungen und reagiert auf das Problem, dass – allzumal ausgelagerte und/oder zentralisierte – Datenverarbeitung durch die/den einzelne/n Richter/in nicht mehr überblickt und wirksam kontrolliert werden kann. Diese Abhängigkeit von sinnlich nicht mehr wahr- und damit kontrollierbaren technischen Vorgängen ist zwar in der Informationsgesellschaft allgegenwärtig und prägt auch schon die heutige Datennutzung (in) der Justiz. Damit verbundene Probleme und Risiken werden sich aber mit einer führenden Gerichtsakte und durchgängig digitalisierten Bearbeitungsvorgängen potenzieren.

Die Mitglieder der IT-Kontrollkommission nehmen die Kontrollaufgaben quasi „treuhänderisch" für ihre KollegInnen wahr. Dass die richterliche Unabhängigkeit jedem/r einzelnen Richter/in zusteht und diese vor datenverarbeitungsbedingten Einwirkungen und Beeinträchtigungen schützen soll, hindert verfassungsrechtlich nicht eine gewisse „Kollektivierung" ergänzender Kontrollbefugnisse und bedeutet keinen unzulässigen Verweis auf ein vages Kontrollversprechen.[5] Die IT-Kontrollkommission löst auch das Problem, dass in professionell geführten Datenverarbeitungszentren aus Sicherheitsgründen die Sicherheitsvorkehrungen nicht allgemein und/oder gegenüber allen Nutzern offen gelegt werden können.

2. § 5 Abs. 1 E-ITJG sieht eine „unabhängige" IT-Kontrollkommission vor. Die Mitglieder der Kontrollkommission nehmen diese Funktion zwar zur Wahrung der richterlichen Unabhängigkeit, aber nicht in richterlicher Unabhängigkeit war. Es sollte daher ausdrücklich festgelegt werden, dass die Mitglieder der Kontrollkommission bei der Wahrnehmung ihrer Kontrollaufgaben von fachlichen Weisungen aller Art – sowohl solchen des Ministeriums als auch solchen des entsendenden Mitbestimmungsgremiums - freigestellt sind.

3. Die personelle Zusammensetzung der IT-Kontrollkommission lehnt sich an § 3 Gesetz zur Errichtung der Informationstechnik-Stelle der hessischen Justiz (IT-Stelle) und zur Regelung

[5] A.A. Heldt, „Vernunft" und „Besonnenheit" am vernetzten Richterarbeitsplatz, BJ 2015, 27; Boysen, So einfach ist das nicht, verdikt 2.15, 17.

justizorganisatorischer Angelegenheiten an. Verzichtet wird aber auf ein Mitglied der GemIT (oder der datenverarbeitenden Stelle). Dies entspricht einer auf die Kernaufgabe „Schutz der richterlichen Unabhängigkeit“ konzentrierten personellen Zusammensetzung. Sachgerecht erscheinen auch die nicht nach der Größe der Gerichtsbarkeiten gestaffelten Entsendungsrechte, die eine Repräsentation aller Gerichtsbarkeiten/Funktionsbereiche sicherstellt. Die Größe mit insgesamt sieben Personen erscheint für die Aufgabenerledigung hinreichend.

4. Das Entsenderecht der Mitbestimmungsgremien, dem kein Auswahl- oder Bestätigungsrecht des Ministeriums entspricht, ist sachgerecht und auch unter demokratietheoretischen Gesichtspunkten nicht zu beanstanden. Die Mitglieder der IT-Kontrollkommission üben keine hoheitliche Gewalt aus, die eines besonderen, über die aus dem Richteramt vermittelten personellen Legitimation hinausgehenden Bestellungs- oder Bestätigungsaktes bedürfte. Die Wahrnehmung der Aufgaben als Mitglied der Kontrollkommission ist letztlich nicht richter-/personalvertretungsrechtliche Interessenvertretung; es ist die Wahrnehmung einer besonderen Dienstaufgabe.

Angeregt wird, in § 5 Abs. 2 E-ITJG nicht nur die Entsendung der Mitglieder zu regeln, sondern auch die Beendigung der Mitgliedschaft. Eine (freie) Abberufung durch das entsendende Mitbestimmungsgremium sollte ausdrücklich geschlossen werden (der Zusatz „für die Dauer ihrer eigenen Amtsperiode“ reicht nicht). Die Amtszeit ist mit der Maßgabe an die Amtszeit des jeweiligen Mitbestimmungsgremiums zu binden, dass sie erst mit der Bestimmung eines anderen Mitglieds (oder der Bestätigung der Mitgliedschaft) endet. Eine Wiederbenennung ist ausdrücklich zuzulassen. Klarzustellen ist, dass die Mitgliedschaft mit dem Ausscheiden aus dem Landesdienst endet und eine Amtsniederlegung statthaft ist.

5. Die Freistellung zu Schulungs- und Bildungsveranstaltungen nach § 5 Abs. 3 E-ITJG ist dem Wortlaut nach auf die Mitglieder der IT-Kontrollkommission beschränkt. VertreterInnen sind nicht erfasst. Dies erscheint nicht sachgerecht; der Verweis auf § 37 MBG SH (§ 5 Abs. 3 Satz 2 E-ITJG) ist auf § 37 Abs. 1 Satz 2 MBG SH zu erstrecken.

6. Für die Freistellung zur ordnungsgemäßen Durchführung der Aufgaben der IT- Kontrollkommission sollte bei dem Gebot der teilweisen Freistellung ein Korridor (z.B. zwischen 25 und 50 v.H.) festgelegt werden, auch um den Präsidien im Rahmen der Geschäftsverteilung einen entsprechenden Belastungsausgleich zu ermöglichen.

7. Die umfassenden Zutritts-, Auskunfts- und Einsichtsrechte (§ 5 Abs. 6 E-ITJG) entsprechen jenen der GemIT und sind sachgerecht. Soweit dabei personenbezogene Daten zur Kenntnis gelangen, sind die Mitglieder der IT-Kontrollkommission auf Stillschweigen zu verpflichten, soweit die Offenlegung nicht zur Feststellung von Mängeln erforderlich ist. Klarzustellen ist, ob diese Rechte nur der IT-Kontrollkommission als Kollektivgremium, einer von diesem entsandten/beauftragten Delegation oder auch jedem einzelnen Mitglied der Kontrollkommission zustehen. Eine Beschränkung allein auf die IT-Kontrollkommission als Kollektivgremium erscheint nicht sachgerecht.

8. Die Möglichkeiten der IT-Kontrollkommission bei festgestellten Verstößen sollten dahin erweitert werden, dass bei schwerwiegenden Verstößen auch eine umgehende Untersagung der (weiteren) Datenverarbeitung verlangt werden kann; in diesen Fällen ist ihr weiterhin eine Unterrichtung der Öffentlichkeit zu gestatten. Die IT-Kontrollkommission ist zu verpflichten, jährlich einen Tätigkeitsbericht zu erstellen, der (zumindest) allen Justizbediensteten zugänglich zu machen ist.

VI. Standard-IT und Zentrale Dienste

1. Es ist sachgerecht, dass die Justiz des Landes nach Maßgabe des eigenen Ratschlusses über den Einsatz der Standard-IT des Landes sowie die Nutzung der Basisdienste entscheiden kann. Bei einer systematischen Auslegung bleiben dabei die Anforderungen, die sich aus § 2 Abs. 2 E-ITJG ergeben, unberührt. Soweit zu § 4 E-ITJG dem Vorschlag gefolgt wird, der GemIT einen Beirat zur Seite zu stellen, sollte diesem das Anhörungsrecht übertragen werden.

2. Bei der Option (§ 6 Abs. 2 Satz 2 E-ITJG), im Einvernehmen mit dem IT-Management der Landesverwaltung die Einrichtung justizeigener Standards vorzusehen, sollte der – im Vergleich zur allgemeinen Verwaltung deutlich engeren – länderübergreifenden Zusammenarbeit im Bereich der Justiz Rechnung getragen werden. Das IT-Management der Landesverwaltung ist darauf zu verpflichten, bei der Herstellung des Einvernehmens der Justiz des Landes die Übernahme/Verwendung von Standards der Bund-Länder-Kommission zur Datenverarbeitung in der Justiz (BLK) regelmäßig zu ermöglichen und das Einvernehmen nur zu verweigern, wenn dem zwingende Gründe entgegenstehen.

3. Die in § 6 Abs. 3 E-ITJG vorgesehene „frühzeitige“ Unterrichtung sollte dahin spezifiziert werden, dass die Unterrichtung so frühzeitig erfolgt, dass eine wirksame Beteiligung über Grundlagen und Reichweite der Änderungen und Weiterentwicklungen sichergestellt ist.

VII. Fachverfahren

Bei den Belangen, die vertraglich bei den Fachverfahren sicherzustellen sind (§ 7 Abs. 1 E-ITJG), ist die Ergonomie hervorzuheben (inkl. Zeit-/Antwortverhalten).

VIII. Justizinterne Zugriffsrechte

Jedenfalls bei einer Datenhaltung bei einem justizexternen Dritten (inkl. Dataport) ist die Paragraphenüberschrift irreführend, weil auch die zur Dienstaufsicht berufenen Stellen insoweit zwar der Justizverwaltung zuzurechnen sind, aber in Bezug auf die Schutzziele des Gesetzes „Dritte“ sind.

Bei einer Umstrukturierung des § 2 E-ITJG ist systematisch sinnvoller, diese Regelung in § 2 zu verlagern und statt einer einseitigen Festlegung durch das für Justiz zuständige Ministerium für den Regelfall eine Dienstvereinbarung vorzusehen.

IX. Inkrafttreten

Anzuregen ist für die Bildung der IT-Kontrollkommission eine Übergangsregelung.