**BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG**

Drucksache 21/17640

21. Wahlperiode

25.06.19

Mitteilung des Senats an die Bürgerschaft

Stellungnahme des Senats zu dem Ersuchen der Bürgerschaft vom 16. Januar 2019 „Digitalisierung der Hamburger Justiz“ Drucksache 21/15594

I.

Anlass

Bürgerschaftliches Ersuchen vom 16. Januar 2019: „Digitalisierung der Hamburger Justiz“. Die Bürgerschaft hat am 16. Januar 2019 folgendes Ersuchen an den Senat beschlossen (Drucksache 21/15594):

„Der Senat wird gebeten, bis zum 30. Juni 2019 über die laufenden und geplanten Maßnahmen der Digitalisierung der Hamburger Justiz zu berichten.“

II.

Stellungnahme des Senats

1. **Bericht über die Digitalisierung in der Hamburger Justiz**

Die Justiz befindet sich derzeit bundesweit inmitten eines großen Veränderungs- und Modernisierungsprozesses. Noch vor einigen Jahren stand die Entwicklung und Einführung von weitestgehend autonomen und monolithischen IT-Systemen zur unterstützenden Verwaltung von gerichtlichen und staatsanwaltschaftlichen Verfahren (wie zum Beispiel die IT-Fachverfahren forumSTAR, EUREKA-Fach und MESTA) im Vordergrund. Durch die geplante und bundesweit auch gesetzlich vorgeschriebene digitale Transformation kommt es nun zu einer weitestgehend ausschließlich elektronischen Bearbeitung von justiziellen Verfahren. Neben umfangreichen digitalen Angeboten für die Rechtssuchenden und ihre Vertreterinnen und Vertreter werden dabei auch den Beschäftigten der Justiz selbst weitere moderne, ergonomische und die digitale Arbeit unterstützende Arbeitsmittel bereitgestellt. Die sich daraus insgesamt ergebenen Änderungen liegen nicht mehr nur allein in der Technik, sondern sind als großflächiger Kulturwandel auf der Schnittstelle zwischen Recht, Technik, Organisation und Personal zu verstehen. Die Hamburger Justiz bringt sich diesbezüglich aktiv in zahlreiche länderübergreifende und landesinterne Strategien, Handlungsfelder und Maßnahmen ein. Diese werden im Folgenden vorgestellt.

1.1 Länderübergreifende Strukturen, Strategien und Maßnahmen

Stärker noch als in der Verwaltung wird die Digitalisierung in der Justiz maßgeblich von bundesweiten bzw. länderübergreifenden Entwicklungen geprägt. Gesteuert wird diese Zusammenarbeit durch den bereits in 2012 als Ergänzung zum IT-Planungsrat etablierten „E-Justice-Rat“ auf der Ebene der Amtschefinnen und Amtschefs der Landesjustizverwaltungen sowie auf operativer

Ebene durch die „Bund-Länder-Kommission für Informationstechnik in der Justiz“ (BLK). Die vorgenannten Strukturen spiegeln dabei die besondere Rolle der Justiz als rechtsprechende Gewalt wieder, deren Unabhängigkeit so auch im Bereich der justiziellen Informations- und Kommunikationstechnik angemessenen Ausdruck finden kann.

Die Hamburger Justiz nimmt auf oberster Ebene aktiv an der Mitgestaltung der länderübergreifenden Rahmenbedingungen für die Digitalisierung teil. Länderübergreifend werden strategische Vorhaben identifiziert, die hierfür notwendigen IT-Infrastrukturen bundesweit oder länderübergreifend entwickelt und bereitgestellt sowie die erforderlichen bundesgesetzlichen Anpassungen initiiert.

1.1.1 Rahmenbedingungen

Wesentliche Rahmenbedingungen aus übergeordneten Strategieentscheidungen sind

– der bundesweit durch gesetzliche Rahmenbedingungen geleitete Digitalisierungsprozess mit dem Ziel einer verbindlichen elektronischen Außenkommunikation mit professionellen Verfahrensbeteiligten einschließlich einer ausschließlich elektronischen Aktenführung und
– die Entwicklung einer länderübergreifenden IT-Grundarchitektur und IT-Governance in der Justiz mit dem Ziel, zwecks Beherrschbarkeit von IT-Infrastrukturen und finanziellen Aufwänden redundante Entwicklungen zu vermeiden und eine bessere Abstimmung bei fachlich überschneidenden Themen zu erreichen.

Auf Anwendungsebene bieten die Landesjustizverwaltungen bereits heute neben der Möglichkeit zur Online-Antragstellung im Mahnverfahren, dem gemeinsamen Vollstreckungsportal und der Veröffentlichung von Insolvenzbekanntmachungen über das Internet (www.justiz.de) auch für den Bereich der Grundbuch- und Registerführung Auskunftsverfahren an. Darüber hinaus werden Informationsangebote des Bundesministeriums der Justiz und für Verbraucherschutz und der Landesjustizverwaltungen zu Bundes- und Landesrecht sowie zur Rechtsprechung bereitgestellt. Im Rahmen der Umsetzung des E-Justice-Gesetzes ist ein zentrales elektronisches Schutzschriftenregister entstanden.

Auf Grund der umfangreichen rechtsetzenden Aktivitäten der EU-Gremien ist es für die Mitgliedsstaaten wichtig, neben den gesetzlichen Initiativen auch die Entwicklung von IT-Infrastrukturen auf EU-Ebene mit zu beeinflussen und rechtzeitig erforderliche Anpassungen vorzunehmen. Hier sind insbesondere e-CODEX (e-Justice Communication via Online Data Exchange, www.e-codex.eu) und die diversen Folgeprojekte (www.e-codex.eu/projects) wie z.B. e-CODEX PLUS (www.e-codex.eu/e-codex_plus), Me-CODEX (Maintenance of e-CODEX), IRI (Interconnection of Insolvency Registers) und e-SENS (Electronic Simple European Networked Services, www.esens.eu) hervorzuheben.

1.1.2 Bundesweite Vorhaben

Derzeit werden aus der länderübergreifenden Steuerung im Wesentlichen die folgenden weiteren bundesweiten Vorhaben abgeleitet:

– Einführung des elektronischen Rechtsverkehrs und der elektronischen Aktenführung: Durch das „Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten“ vom 10. Oktober 2013 (BGBl. I S. 3786) sowie das „Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs“ vom 5. Juli 2017 (BGBl. I S. 2208) ist der elektronische Zugang zu den Gerichten seit dem 1. Januar 2018 für den Bereich der ZPO, StPO, FamFG, ArbGG, VwGO, SGG und FGO eröffnet. Zudem sind sog. professionelle Einreicher (insb. Rechtsanwältinnen und Rechtsanwälte, Behörden und juristische Personen des öffentlichen Rechts) spätestens ab dem 1. Januar 2022 verpflichtet, bei den Gerichten und Staatsanwaltschaften Schriftsätze elektronisch einzureichen. Die Zahl der elektronischen Eingänge bei den Gerichten wird deshalb spätestens ab dem Jahr 2022 erheblich ansteigen. Um in Zukunft Medienbrüche zwischen elektronischer Repräsentation und Papier möglichst zu vermeiden, ist auch der Postausgang weitestgehend elektronisch abzuwickeln und auf die elektronische Aktenführung umzustellen. Das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs sieht daher vor, dass spätestens ab 1. Januar 2026 die justiziellen Verfahrensakten in allen Bereichen elektronisch geführt werden müssen. In Bund und Ländern sind umfangreiche Vorhaben zur Umsetzung der gesetzlichen Rahmenbedingungen angelaufen. Für die elektronische Akteneinsicht wird ein länderübergreifendes Akteneinsichtsportal bereitgestellt werden.
– Gemeinsame Fachverfahrensentwicklung: Im Rahmen der weitgehenden Standardisierung und Vereinheitlichung von Fachverfahren in

der Justiz wurde beschlossen, neue oder zu ersetzende Fachverfahren zukünftig mit allen 16 Ländern zu entwickeln und zu nutzen. Die hierbei anzuwendende länderübergreifende IT-Grundarchitektur der Justiz baut dazu auf gemeinsam genutzten Standards, Systemkomponenten und deren Kopplung über Web-Services nach einem modularen, serverbasierten und serviceorientierten Architekturansatz auf. Der Weg zu einer einheitlicheren IT-Landschaft wird durch eine Kontroll- und Steuerungsstruktur zur Abstimmung der fachlichen und technischen Architekturen in der Justiz unterstützt und abgesichert. Der IT-Governance unterliegen Neuentwicklungen, Neubeschaffungen und wesentliche Fortentwicklungen von IT-Anwendungen der Gerichte und Staatsanwaltschaften, die Auswirkungen auf das Zusammenwirken von Systemen und ihrer Schnittstellen haben. Ziel ist es, ein einheitliches Zusammenwirken der Komponenten sowie eine wirtschaftliche Programmpflege und einen wirtschaftlichen Betrieb zu gewährleisten.

– Pakt für den Rechtsstaat: Die Bundeskanzlerin und die Regierungschefinnen und Regierungschefs der Länder haben am 31. Januar 2019 den „Pakt für den Rechtsstaat“ vereinbart. Eine zentrale Säule ist die Digitalisierung, die einen wichtigen Beitrag zur Verfahrensbeschleunigung leistet. Im Pakt für den Rechtsstaat wird anerkannt, dass die Länder bereits verschiedene Maßnahmen zur Digitalisierung von Justiz und Polizei ergriffen haben, die es auszubauen und weiter zügig voranzubringen gilt. Um den medienbruchfreien Austausch zwischen Polizei und Staatsanwaltschaft von Bund und Ländern sowie die Interoperabilität mit den Gerichten zu ermöglichen, soll insbesondere die Schaffung einer Kommunikationsschnittstelle zwischen Justiz und Polizei vorangetrieben werden, sodass die gesetzlichen Anforderungen, bis 2026 eine medienbruchfreie Kommunikation zu schaffen, gemeinsam erfüllt werden können. Der Bund hat sich bereit erklärt, in Abstimmung mit den Ländern eine Konzeption dieser Schnittstelle zu beauftragen und dafür die Kosten zu übernehmen.

– Prüfung der Potentiale von künstlicher Intelligenz in der Justiz (Legal Tech) u.a. im Rahmen von BLK-Arbeitsgruppen: Den Bediensteten sollen Werkzeuge an die Hand gegeben werden, welche bei der Bewältigung der täglich anstehenden Aufgaben im Rahmen der Entscheidungsprozesse in der Justiz assistieren. Dabei wird nicht das – hinsichtlich richterlicher Entscheidungen ohnehin verfassungsrechtlich unzulässige – Ziel verfolgt, Entscheidungen auf Computerprogramme zu verlagern und damit zu automatisieren. Es wird stets oberstes Ziel sein, die Aufgaben der dritten Staatsgewalt auch in einer zunehmend digitalen Welt mit höchstem Anspruch erfüllen zu können. Die Nutzer sollen jedoch von Online-Services der Justiz mit intelligenten Assistenten profitieren. Beispielhafte Einsatzgebiete sind maschinelle Übersetzung, Extraktion von Metadateninformationen, intelligente Nutzerunterstützung (z.B. Chatbots) und Strukturierung von Umfangsverfahren.

Über den IT-Planungsrat nimmt die Justiz als Teil des gesamtstaatlichen Handelns auch an den länderübergreifenden Digitalisierungsbestrebungen der Verwaltung teil. Bundesweit ist hier derzeit die Bereitstellung von Online-Diensten nach dem Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) vom 14. August 2017 (BGBl. I S. 3122, 3138) zu prüfen bzw. umzusetzen. Dabei verpflichtet das OZG Bund, Länder und Kommunen bis 2022 ihre Verwaltungsleistungen digital über einen interoperablen Portalverbund anzubieten. Die Freie und Hansestadt Hamburg nimmt hieran mit dem „Hamburg Serviceportal“ teil. In länderübergreifenden Gremien der Justiz werden zu diesem Zweck gemeinsam verpflichtende Verwaltungsleistungen identifiziert. Dies sind neben den bereits im „Hamburg Serviceportal“ angebotenen Diensten wie dem Stiftungsverzeichnis voraussichtlich folgende, wesentliche Leistungen:

– Zulassung zum Rechtsreferendariat,
– Anträge, Zulassungen und Ausstellungen durch die Justizprüfungsämter,
– Einsicht und Eintragung in das Rechtsdienstleistungsregister,
– Einbettung der Einsicht und von Eintragungen in das Dolmetscherverzeichnis,
– Anerkennung ausländischer Berufsqualifikationen, Bildungsabschlüssen und Eheschließungen,
– Hinterlegungssachen beim Amtsgericht,
– Registrierung, Antrag und Nachweise für den Sammelfonds für Bußgelder (zusätzliche Hamburger Leistung),
– Einbettung der Einsicht in das Patentanwaltsverzeichnis (Patentanwaltskammer),
– Einbettung der Einsicht und von Eintragungen in das Vorsorgeregister (Bundesnotarkammer),

– Einbettung der Beantragung von Führungszeugnissen (Bundesamt der Justiz),
– Einsicht in das Gewerbezentralregister (Bundesamt der Justiz).

Die Kerntätigkeit der Rechtspflege ist nicht vom OZG betroffen. Für die Bürgerinnen und Bürger wäre es jedoch nur schwer nachvollziehbar, über den Portalverbund zwar mit der Verwaltung, nicht hingegen mit der Justiz kommunizieren zu können. Die Justiz hat daher ein nachhaltiges Interesse, auch über die gesetzlichen Verpflichtungen hinaus geeignete Online-Dienste im Portalverbund bereitzustellen. Deshalb werden in der Justiz zusätzliche Leistungen der Rechtspflege identifiziert, die über die jeweiligen Bürgerportale der Länder, des Bundes und der Kommunen angeboten werden sollen. Dies sind neben den bereits heute in den Portalen der Länder vorhandenen Leistungen wie dem Grundbuchabrufverfahren voraussichtlich zunächst:

– Einbettung der bereits bestehenden Online-Dienste der Justiz (wie zum Beispiel des Handels-, Partnerschafts- und Genossenschaftsregisters, des Vereinsregisters oder der Insolvenzbekanntmachung),
– Antrag auf Prozesskosten- und Verfahrenskostenhilfe,
– Antrag auf Ausstellung eines Erbscheins,
– Einsicht und Anträge an das Schiffsregister.

Die Verantwortlichkeiten in Hinblick auf die Umsetzung potentieller Online-Dienste werden derzeit unter den Ländern abgestimmt. Für das Thema Schiffsregister ist Hamburg federführend.

1.2 Landesinterne Strukturen, Strategien und Maßnahmen

Im verbleibenden Handlungsspielraum partizipiert die Hamburger Justiz aktiv an den Strategien, Gremien und zentral bereitgestellten IT-Infrastrukturen der Freien und Hansestadt Hamburg. Über das Programm „DigitalFirst“ sind die nachfolgenden Handlungsbereiche vorgegeben:

– Organisatorische Optimierung der Geschäftsprozesse und Verfahrensabläufe,
– Perspektive der Bürgerinnen und Bürger und der Unternehmen als Gestaltungsmaßstab,
– Einsatz und Ausbau benutzungsfreundlicher Technik,
– Weiterentwicklung rechtlicher Rahmenbedingungen,
– Unterstützung und Qualifizierung der Bediensteten.

1.2.1 Umsetzung von Maßnahmen

Die Hamburger Justiz bringt sich mit der konkreten Umsetzung von länderübergreifenden und individuellen Maßnahmen bzw. der Prüfung weiterer Digitalisierungspotentiale in diese Handlungsfelder ein, z.B.:

– Der elektronische Rechtsverkehr ist in allen gesetzlich vorgegebenen Verfahren eröffnet und wird auch in jenen Bereichen, in denen keine gesetzliche Verpflichtung besteht, zugelassen (z.B. seit 2018 im Schiffsregister).
– Im Rahmen der Einführung der elektronischen Akte bei den Gerichten und Staatsanwaltschaften erfolgt zukünftig eine medienbruchfreie elektronische Verfahrensbearbeitung. Diese umfasst auch eine weitergehende Modernisierung der Arbeitsplatzausstattung für die Beschäftigten in der Justiz, z.B. durch eine Ausweitung der Bereitstellung mobiler Endgeräte, und eine Erweiterung der Saalausstattung, sodass die Verwendung digitaler Medien in Gerichtsverhandlungen weiter erleichtert wird. Für die Verfahrensbeteiligten ist die Möglichkeit einer elektronischen Akteneinsicht vorgesehen. Der elektronische Zugang wird barrierefrei ausgestaltet sein.
– Im Kontext der Modernisierung erfolgen ein anforderungsgemäßer Ausbau der Netzwerkanbindung aller Standorte der Hamburger Justiz und eine weitestgehend flächendeckende Ausstattung der Hamburger Justiz mit WLAN. Dieses soll bei Terminen in den Gebäuden der Hamburger Justiz auch den Verfahrensbeteiligten zur Verfügung stehen. Die Maßnahmen sollen noch in der aktuellen Legislaturperiode weitgehend abgeschlossen werden. Zudem erfolgt noch in 2019 die Einführung eines neuen Webbrowser-Produktes für Arbeitsplätze mit hohem Schutzbedarf (insb. für Vollzug, Staatsanwaltschaften und Gerichte), das bei Beibehaltung eines weiterhin hohen Sicherheitsniveaus einen schnelleren Internetzugriff ermöglicht.
– Für die Qualifizierung der Mitarbeiterinnen und Mitarbeiter der Justiz sollen im Bereich „E-Justice-Kompetenz“ ab 2020 weitere Angebote entstehen.
– Unter Einbeziehung der Universität Hamburg und der Bucerius Law School wird ein Konzept erstellt, unter dem ein digitales Ablegen der schriftlichen Prüfungsleistungen im Rahmen der staatlichen juristischen Prüfungen ermöglicht werden kann. Dazu werden die technischen, rechtlichen und finanziellen Rahmenbedingungen für eine Digitalisierung bestimmt

und bewertet. Der Bürgerschaft soll bis zum 30. November 2019 im Rahmen des Ersuchens 21/14523 über die Entwicklung berichtet werden.

– Die Geschäfts- und Buchungsprozesse des Sammelfonds für Bußgelder werden schrittweise digitalisiert, um die manuelle Erfassung bei der Bußgeldverarbeitung wesentlich zu reduzieren. Dies umfasst die Schaffung eines digitalen Zugangswegs, über den gemeinnützige Institutionen Zuweisung von Bußgeldern beantragen und die zweckgemäße Verwendung nachweisen können. Eine Bereitstellung ist für Anfang 2020 vorgesehen.
– In Verbindung mit der Digitalisierung von Geschäftsprozessen im Vollzug kann mit Hilfe von Videodolmetschen ein viel breiteres Spektrum an Übersetzungsleistungen als je zuvor gewährleistet werden. Dolmetscherinnen und Dolmetscher vor Ort werden zudem sukzessive ersetzt. Die flexible Zuschaltung von Dolmetscherinnen und Dolmetschern per Video in mehreren Sprachen sorgt für eine effektivere Arbeitsweise durch weniger Verwaltungsaufwand und geringere Kosten.
– Durch den Aufbau und Einsatz der im länderübergreifenden Entwicklungsverbund entwickelten Software für ein Datawarehouse im Vollzug soll die Daten-Analyse datenschutzkonform professionalisiert und optimiert werden. Damit einhergehen die Vermeidung aufwendiger Einzeldatensatz-Auswertungen, eine Reduzierung von Auswertungsfehlern, die Stärkung der Vertretungsfähigkeit in Statistik-Aufgaben, die Vermeidung von Doppelerfassungen und Parallelsystemen sowie eine Verringerung der Medienbrüche. Darüber hinaus erfolgt eine Stärkung der Zielsetzung „Kriminologische Forschung“.
– Mit der Optimierung der Geschäftsprozesse und einem digitalen Zugang zu den Unterlagen für den Richterwahlausschuss (RWA) sollen Ressourcen eingespart werden. Den berufenen Mitgliedern des RWA ist zur Erfüllung ihrer verfassungsgemäßen Aufgabe Einsicht in die Personalakten und in die Bewerbungsunterlagen der Bewerberinnen und Bewerber zu gewähren. Mit der datenschutzkonformen Digitalisierung entfallen Kopier-, Sortier- und Versandaufwand, kurzfristige Änderungen und Ergänzungen können schneller und einfacher bereitgestellt werden. Die Mitglieder des RWA können die Unterlagen vor der jeweiligen Sitzung online einsehen und auch während der Sitzung digital aufrufen. Die Umstellung auf den „digitalen“ RWA soll noch in 2019 erfolgen. Eine Weiterentwicklung ist bei Umstellung auf die E-Personalakte denkbar.

Im Kontext des Online-Zugangsgesetzes bzw. des Programms „DigitalFirst“ sollen dabei nutzerorientierte Online-Schnittstellen zu den wesentlichen Leistungen der Justiz entstehen. Strategisch strebt der Senat dadurch einen nachhaltigen und gemeinsamen Zugang zu der Verwaltung und der Justiz über das „Hamburg Serviceportal“ an.

Eine besondere Herausforderung besteht vor diesem Hintergrund in der Zusammenführung der Digitalisierungsvorhaben unter Berücksichtigung der bundesweiten und der landesinternen Rahmenbedingungen, die auf Grund der weiter zunehmenden Bedeutung der Digitalisierung einer hohen Dynamik unterliegen. Neben den oben genannten zeigen insbesondere die folgenden Vorhaben diesen Anspruch im besonderen Maße auf:

1.2.2 Umsetzung von Maßnahmen im Kontext DigitalFirst und OZG

– Maschinelles Schiffsregister: Um den Anforderungen eines modernen Schiffsmanagements zu genügen, wird das Schiffsregister im Rahmen eines behördenübergreifenden Projekts mit der Behörde für Wirtschaft, Verkehr und Innovation (BWVI) digitalisiert. Auf Initiative Hamburgs hat der Bundesrat zunächst eine gesetzliche Änderung beschlossen, damit der Schriftverkehr mit dem Schiffsregister auch elektronisch abgewickelt werden kann. Neben der daraus resultierenden Möglichkeit, seit Sommer 2018 Anträge elektronisch einreichen zu können, werden nun auch die Prozesse im Schiffsregisterverfahren digitalisiert und optimiert. Berechtigte Benutzerinnen und Benutzer sollen die Möglichkeit haben, jederzeit den aktuellen Inhalt des Schiffsregisters online über das „Hamburg Serviceportal“ abzurufen. Die Entwicklung des Schiffsregisters orientiert sich dabei an den Standards und der länderübergreifenden IT-Grundarchitektur der Justiz. Die erste Hauptversion soll Anfang 2020 fertiggestellt sein. Eine Nachnutzung der Software in anderen Ländern ist gegen Kostenbeteiligung vorgesehen. Das maschinelle Schiffsregister trägt dazu bei die Attraktivität des Schifffahrtsstandorts Hamburg zu sichern.
– Aufbau einer Schnittstelle zum elektronischen Rechtsverkehr im „Hamburg Serviceportal“: Durch eine länderübergreifende Arbeitsgruppe werden derzeit Vorschläge für gesetzliche Anpassungen erarbeitet, durch welche die Bürgerportale als sicherer Übermittlungsweg im Sinne des § 130a Absatz 4 Nr. 4 ZPO zugelas-

sen werden können, sodass elektronische Einreichungen zu allen oder ausgewählten Verfahren über die Bürgerportale ermöglicht werden können. Der Hamburger Senat erarbeitet die hierzu erforderlichen technischen Vorkehrungen für das „Hamburg Serviceportal“.

– Beschleunigtes Online-Verfahren (BOV): Im Rahmen der länderübergreifenden Arbeitsgruppe „Legal Tech“ wurde von Hamburg federführend das Modell eines „Beschleunigten Online-Verfahrens“ entwickelt. Grundidee des Modells ist es, dass Bürgerinnen und Bürger eine zivilprozessuale Klage mit geringfügigen Streitwerten schnell und unkompliziert „online“ erheben können sollen, wobei sie durch „Chatbots“ oder weitere digitale Anwendungen unterstützt werden. Die Justizbehörde Hamburg prüft derzeit, inwieweit Einzelkomponenten dieses Modells bereits zeitnah ohne bundesgesetzliche Änderungen umgesetzt werden können.

Mit der Durchführung bzw. dem erfolgreichen Abschluss der oben genannten Vorhaben und Maßnahmen werden weitreichende Schritte in Richtung einer umfassenden Digitalisierung in der Hamburger Justiz und damit wichtige Beiträge zu ihrer Modernisierung, dem Erhalt ihrer Funktionsfähigkeit, ihrer Attraktivität als Arbeitgeberin und damit insgesamt zur Sicherstellung ihrer Zukunftsfähigkeit vollzogen sein. Neben diesen qualitativen Aspekten ist die zunehmende Digitalisierung geeignet, insbesondere durch die Vermeidung von zeitlich, finanziell und ökologisch nachteiligen Transporten von Papierdokumenten und deren aufwendiger jahrelanger Archivierung sowohl auf Seiten der berufsmäßigen Kommunikationspartner als auch auf Seiten der Justiz zu monetären Entlastungen beizutragen.

1.3 IT-Infrastrukturen

Neben digitalen Angeboten für die Rechtssuchenden und ihre Vertreter (Außenwirkung) werden den Beschäftigten moderne, ergonomische und die digitale Arbeit unterstützende Arbeitsmittel bereitgestellt (Innenwirkung). Durch die digitale Transformation zu einer weitestgehend ausschließlich elektronischen Bearbeitung von justiziellen Verfahren werden jedoch die zugrundeliegenden IT-Infrastrukturen für die Justiz in Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit zunehmend geschäftskritisch.

1.3.1 Länderübergreifend bereitgestellten Infrastrukturen

Gemeinsame Grundlage hierfür sind die länderübergreifend bereitgestellten Infrastrukturen des elektronischen Rechtsverkehrs, wie insbesondere

– die auf dem sicheren Verwaltungsprotokoll OSCI basierende Infrastruktur für das „Elektronische Gerichts- und Verwaltungspostfach“ (EGVP), das eine Ende-zu-Ende-verschlüsselte Kommunikation ermöglicht,

– die einheitliche Identifizierung über das vom IT-Planungsrat verwaltete eID-System „Secure Access to Federated eJustice/eGovernment“ (SAFE),

– ein länderübergreifend verbindlicher Standard für die strukturierten Daten der Justiz (xjustiz.justiz.de/).

Ein Großteil der länderübergreifend entwickelten IT-Infrastrukturen (insb. die Kommunikationsendpunkte und die Fachverfahren) müssen jedoch durch die Länder selbst betrieben werden. Für den Betrieb derart schützenswerter bzw. im weiteren Verlauf der Digitalisierung zunehmend weiter zu schützender IT-Infrastrukturen wird nach dem vom Bundesamt für Sicherheit in der Informationstechnik entwickelten IT-Grundschutz ein nach ISO 27001 zertifizierter Betrieb empfohlen. Für die Freie und Hansestadt Hamburg stellt der IT-Dienstleister Dataport A.ö.R. ein Twin-Rechenzentrum mit der höchstmöglichen Schutzstufe „TÜV IT Trusted Site Level 4“ bereit.

1.3.2 Data-Center-Justiz (DCJ)

Vor dem Hintergrund des hohen Schutzbedarfs der Daten und Prozesse in der Justiz beabsichtigen die Trägerländer Bremen, Hamburg, Sachsen-Anhalt und Schleswig-Holstein den Betrieb geschäftskritischer IT-Infrastrukturen bei Dataport auf- bzw. auszubauen. Die IT-Verfahren der Dataport-Trägerländer mit einem hohen Schutzbedarf sind bereits heute im Dataport-Rechenzentrum mit einer Zusatzmaßnahme („erweiterte Sicherheit“) von den anderen Strukturen abgetrennt. In Bezug auf die Qualität der IT-Sicherheit, die Einbettung in die IT-Strategie der Justiz sowie die Ausnutzung von Kosten- und Effizienzsynergien kann eine weitergehenden Kooperation der Landesjustizverwaltungen im Sinne eines gemeinsamen „Data Center Justiz“ (DCJ) jedoch von Vorteil sein. Eine länderübergreifende Arbeitsgruppe in Zusammenarbeit mit Dataport prüft daher schrittweise die Machbarkeit.

1.4 Programmsteuerung

Die wachsende Zahl der voranzutreibenden Digitalisierungsvorhaben macht auf Grund der komplexen Anforderungen und Rahmenbedingungen von Seiten der länderübergreifenden und der lan-

desinternen Ebene eine übergreifende Koordination (Programmsteuerung) notwendig. Diese ist in organisatorischer, technischer, finanzieller und personeller Hinsicht anspruchsvoll und kann nur mit qualifiziertem Fachpersonal erfolgreich bewältigt werden. Die Hamburger Justiz verfügt über eine solche übergreifende Stelle mit qualifiziertem Personal bisher nicht; die Teilnahme an regionalen und länderübergreifenden Initiativen zur weiteren Digitalisierung ist mit dem aktuellen Personalbestand nicht möglich. Für die Steuerung wird für die zielgerichtete Weiterentwicklung und den sicheren Aufbau der IT-Infrastrukturen im Spannungsfeld zwischen den bundesweiten und den landesinternen Digitalisierungsstrategien in Verbindung mit einer sicheren Umsetzung ein Projekt eingesetzt. Die Einsetzungsverfügung soll bis Anfang 2020 erstellt werden.

2. **Anlass und Inhalt des IT-Justizgesetzes**

Bereits jetzt ist bei der Organisation und dem Betrieb von IT in der Hamburger Justiz ein hohes Sicherheitsniveau gewährleistet. Dieser Zustand soll durch die Schaffung eines Gesetzes über den Einsatz der Informations- und Kommunikationstechnik bei Gerichten und Staatsanwaltschaften der Freien und Hansestadt Hamburg (IT-Justizgesetz – HmbITJG) langfristig gesichert werden. Zugleich soll der Einsatz und der Betrieb der IT einer effektiven Kontrolle (auch) durch die betroffenen Amtsträgerinnen und Amtsträger, insbesondere der Richterinnen und Richter unterworfen werden

Im Zuge der unter Ziffer 1. dargestellten digitalen Transformation und der damit verbundenen vollständigen Umstellung auf die elektronische Aktenführung und -bearbeitung entstehen beim Schutz der in der Justiz tätigen Personen neue Herausforderungen. Zugriffe auf elektronische Dokumente sind bei unsachgemäßen Schutzmaßnahmen um ein Vielfaches leichter durchzuführen als Zugriffe auf Papiervorgänge. Es besteht in diesem Zusammenhang die Gefahr, dass damit Potentiale für Beeinflussungen und unzulässige Kontrollen der Arbeit, Arbeitsweise und Leistung eröffnet werden. Dies gilt im Grundsatz unabhängig davon, wo die Daten verarbeitet werden. Insbesondere die Richterinnen und Richter sind zur Gewährleistung der verfassungsrechtlich verankerten richterlichen Unabhängigkeit (Artikel 97 Grundgesetz) vor unzulässigen Eingriffen zu schützen.

Die sich aus der Digitalisierung der Arbeit der Justiz potentiell ergebenden Gefahren wirksam einzuhegen, ist Ziel des HmbITJG. Zur Gewährleistung dieses Ziels werden in dem Gesetz Schutzanforderungen definiert und Eingriffe in Daten und Prozesse in mehrfacher Hinsicht beschränkt. Zur Kontrolle sieht der Entwurf die Schaffung einer unabhängigen, primär mit Vertreterinnen und Vertretern der Richterschaft besetzten IT-Kontrollkommission vor, die die Einhaltung der Schutzvorschriften kontrolliert und zu diesem Zwecke mit umfassenden Aufklärungsbefugnissen ausgestattet ist. Das HmbITJG setzt damit die Anforderungen der Rechtsprechung im Zusammenhang mit der sog. hessischen Netzklage (Dienstgerichthof Frankfurt BeckRS 2010, 14555; BGH NJOZ 2012, 787; BVerfG NJW 2013, 2102) um und überträgt die in den Entscheidungen enthaltenen Vorgaben auf die in der Hamburgischen Landesverwaltung bestehenden IT-Organisationsstrukturen.

Die sich aus den vorgenannten Entscheidungen zum Schutz der richterlichen Unabhängigkeit ergebenden Anforderungen werden dabei – ebenso wie in Hessen und anderen Ländern (z.B. Schleswig-Holstein und Baden-Württemberg) – auf den Schutz der sachlichen Unabhängigkeit der Rechtspflegerinnen und Rechtspfleger (§ 9 Rechtspflegergesetz) und auf die Tätigkeiten der Staatsanwaltschaften erstreckt. Die Staatsanwaltschaft wird zwar gemeinhin der Exekutive zugeordnet. Es handelt sich aber auch bei ihr um ein Organ der Rechtspflege. Hier gilt es, die vom Legalitätsprinzip (§§ 152 Absatz 2, 160 StPO) getragene Ermittlungs- und Anklagetätigkeit zu schützen und damit zugleich das Vertrauen der Öffentlichkeit in eine von außen unbeeinflusste, objektive Tätigkeit der Staatsanwaltschaft zu stärken.

Die Mitglieder der IT-Kontrollkommission werden teilweise vom Dienst freigestellt und im Übrigen für ihren Aufwand entschädigt. Die Arbeit der Kommission wird durch eine Koordinierungsstelle unterstützt. Für den Ausgleich der Freistellungen sind 1,5 Stellen in der Wertigkeit R1 Richterinnen bzw. Richter einzurichten, damit die Arbeit der Kommission nicht die Leistungsfähigkeit der Gerichte beeinträchtigt. Für die Koordinierungsstelle ist eine Stelle der Wertigkeit Regierungsrätin bzw. Regierungsrat A13 zusätzlich erforderlich. Zudem erhält die Kommission das Recht, in Ausnahmefällen auch externe Gutachten einzuholen.

Im Ergebnis soll ein Zustand geschaffen werden, der hinsichtlich des Schutzes der in Rede stehenden Rechtsgüter dauerhaft ein auch für das digitale Zeitalter angemessenes Sicherheitsniveau gewährleistet.

3. **Kosten**

Für die Ausgleichsstellen sowie die Koordinierungsstelle für die Umsetzung des IT-Justizgesetzes werden ab 2020 Personalkosten in Höhe von rd. 275 Tsd. Euro jährlich anfallen.

Die nicht freigestellten Mitglieder der IT-Kontrollkommission sollen in Form einer Pauschale in Höhe von jeweils 100 Euro pro Monat entschädigt werden. Ausgehend von zwei nicht freigestellten Mitgliedern entstehen für die Aufwandsentschädigung jährliche Kosten in Höhe von 2.400 Euro.

Für die in Ausnahmefällen mögliche Beauftragung externer Gutachter sind jährlich 50.000 Euro einzuplanen.

Die Finanzierung der zusätzlichen Kosten erfolgt im Rahmen der vorhandenen Ermächtigung aus dem Einzelplan 2 und im Bedarfsfall – in Abstimmung mit der Finanzbehörde – ergänzend aus Mitteln des Paktes für den Rechtsstaat.

III.

Petitum

Der Senat bittet, die Bürgerschaft möge

1. von den Ausführungen dieser Drucksache Kenntnis nehmen,
2. das nachstehende Gesetz beschließen und
3. die aus der Anlage ersichtliche Änderung des Stellenplans zum Haushaltsplan 2020 beschließen.

Gesetz über den Einsatz der Informations- und Kommunikationstechnik bei Gerichten und Staatsanwaltschaften der Freien und Hansestadt Hamburg (IT-Justizgesetz – HmbITJG)

Vom . . . . . .

§ 1

Regelungszweck und Geltungsbereich

(1) Bei Organisation und Betrieb von Informations- und Kommunikationstechnik (IT) für die Gerichte und Staatsanwaltschaften sind die richterliche Unabhängigkeit, die sachliche Unabhängigkeit der Rechtspflegerinnen und Rechtspfleger sowie das Legalitätsprinzip in der Strafverfolgung zu beachten und besonders zu schützen. Insbesondere sollen die Integrität und die Vertraulichkeit der Entscheidungsprozesse geschützt werden. Zudem ist die Funktionsfähigkeit der Justiz zu sichern.

(2) Der Einsatz von IT darf nicht zur Ausweitung von Verhaltens- und Leistungskontrollen im richterlichen Bereich führen.

(3) Das Gesetz regelt zur Gewährleistung dieser Ziele organisatorische und rechtliche Rahmenbedingungen des IT-Betriebes für die Gerichte und Staatsanwaltschaften einschließlich des Hamburgischen Verfassungsgerichtes.

(4) Die jeweils anwendbaren datenschutzrechtlichen Regelungen bleiben von diesem Gesetz unberührt. Sie finden auf die Verarbeitung personenbezogener Daten vorrangig Anwendung.

§ 2

Verantwortlichkeit

(1) Die zuständige Behörde stellt durch geeignete Maßnahmen die Einhaltung der Ziele und Vorschriften dieses Gesetzes sicher.

(2) Die Aktenhoheit liegt bei dem jeweils zuständigen Gericht beziehungsweise der jeweils zuständigen Staatsanwaltschaft.

(3) Die Einhaltung der Ziele und Vorschriften dieses Gesetzes wird durch ein unabhängiges Kontrollgremium (IT-Kontrollkommission) überwacht.

§ 3

Zu schützende Daten, Prozesse und Personen; unmittelbar Berechtigte

(1) Zu schützen sind die gesamten Prozesse der richterlichen, rechtspflegerischen oder staatsanwaltschaftlichen Entscheidungsfindung und die Entscheidungen selbst.

(2) Zu den zu schützenden Daten zählen im Rahmen der geschützten Prozesse insbesondere:

1. sämtliche erstellten, erhaltenen oder weiterverarbeiteten elektronischen Dokumente oder sonstigen Daten einschließlich aller Metadaten (Inhaltsdaten),
2. verfahrensbezogene Daten, die in Fachverfahren, in der elektronischen Akte oder in sonstigen Programmen oder Datenspeichern – auch nur zeitlich befristet – erfasst werden (Verfahrensdaten),
3. systemintern automatisch erstellte Daten über die Benutzung der zur Verfügung stehenden IT (Logdaten).

(3) Inhaltsdaten, welche die richterliche, rechtspflegerische oder staatsanwaltschaftliche Entscheidungsfindung ganz oder teilweise dokumentieren, sowie Verfahrensdaten, die Rückschlüsse auf den Prozess der Entscheidungsfindung ermöglichen, sind besonders geschützt. Umfassend geschützt sind Entwürfe zu Urteilen, Beschlüssen und Verfügungen, die Arbeiten zu ihrer Vorbereitung, Annotationen zu Dokumenten und die Dokumente, die Beratungen und Abstimmungen betreffen, sowie die auf die IT-Nutzung durch geschützte Amtsträger bezogenen Log- und Metadaten.

(4) Besonders geschützt sind Richterinnen und Richter, Rechtspflegerinnen und Rechtspfleger, Staatsanwältinnen und Staatsanwälte sowie Amtsanwältinnen und Amtsanwälte (geschützte Amtsträgerinnen und Amtsträger).

(5) Unmittelbar berechtigt für jede Art des Umganges mit den jeweiligen Daten sind die mit der Verfahrensbearbeitung betrauten Amtsträgerinnen und Amtsträger der Gerichte und Staatsanwaltschaften im Rahmen ihrer jeweiligen Zuständigkeit (unmittelbar Berechtigte). Zuständigkeiten können sich auf Grund gesetzlicher Vorschriften, aus den Geschäftsverteilungsplänen der Gerichte und aus Regelungen im Rahmen der Organisationshoheit der Leitungen der Gerichte und Staatsanwaltschaften sowie im nichtrichterlichen Bereich der Landesjustizverwaltung ergeben.

§4
Technische, betriebliche und organisatorische Maßnahmen

(1) Im Anwendungsbereich des §3 sind bei der Ausgestaltung der zur Verarbeitung von Daten eingesetzten Anwendungssoftware und dem Betrieb der IT die Grundsätze der Datensparsamkeit und Datenvermeidung zu beachten.

(2) Die in der Datenverarbeitung tätigen Auftragsverarbeiter sowie in der Datenverarbeitung tätige Dienststellen (datenverarbeitende Stellen) haben eine sichere Verarbeitung der zu schützenden Daten unter Beachtung des Standes der Technik zu gewährleisten.

(3) Bei dem Betrieb der IT und der Datenverarbeitung haben sie unter Beachtung des Standes der Technik insbesondere sicherzustellen, dass

1. keine unbefugten Einsichtnahmen und Eingriffe in die richterliche, rechtspflegerische und staatsanwaltschaftliche Tätigkeit erfolgen,
2. unbefugte Übermittlungen und sonstige Verarbeitungen nach §3 geschützter Daten unterbleiben,
3. keine unbefugten Veränderungen der technischen Zugriffsberechtigungen erfolgen und
4. die Funktionsfähigkeit der IT nicht eingeschränkt wird.

(4) Die datenverarbeitenden Stellen erstellen Sicherheitskonzepte, die eine effektive Kontrolle durch die IT-Kontrollkommission und die zuständige Behörde gewährleisten. Dazu gehört die Etablierung geeigneter Mechanismen zur internen Kontrolle, mittels derer sicherheitsrelevante Betriebsabläufe und Zustände regelmäßig nachvollziehbar daraufhin überprüft werden, ob unbefugte Zugriffe, Unregelmäßigkeiten oder Probleme des ordnungsgemäßen Betriebs aufgetreten sind. Zugriffe durch Administratorinnen und Administratoren sind revisionssicher zu protokollieren, es sei denn, der Zugriff erfolgt mit ausdrücklicher Einwilligung der oder des unmittelbar Berechtigten. Die Einwilligung soll protokolliert werden. Die Konzepte und Protokolle sind der zuständigen Behörde, den Leitungen der Gerichte und Staatsanwaltschaften für ihren jeweiligen Geschäftsbereich sowie der IT-Kontrollkommission auf Verlangen zugänglich zu machen.

(5) Die Inhaberinnen und Inhaber administrativer Zugänge sind der IT-Kontrollkommission sowie für ihren jeweiligen Geschäftsbereich den Leitungen der Gerichte und Staatsanwaltschaften bekanntzugeben.

(6) Sicherheitsrelevante Ereignisse sind der IT-Kontrollkommission, der zuständigen Behörde und den Leitungen der Gerichte und Staatsanwaltschaften innerhalb angemessener Frist zu melden.

(7) Der Senat wird ermächtigt, Einzelheiten zu den technischen Anforderungen, zu internen Kontrollmechanismen, zur Protokollierung und den Aufbewahrungsfristen, zu Meldepflichten im Sinne des Absatzes 6 und zu den Sicherheitskonzepten durch Rechtsverordnung zu regeln. Der Senat kann die Ermächtigung durch Rechtsverordnung auf die zuständige Behörde weiter übertragen. Bei Erlass oder Änderungen der Verordnung nach Satz 1 sind die Leitungen der Gerichte und Staatsanwaltschaften sowie die IT-Kontrollkommission zu beteiligen.

§ 5

Behandlung der Daten und Prozesse

(1) Einsichtnahmen und Eingriffe in die geschützten Daten und Prozesse sind grundsätzlich nur Berechtigten gestattet, soweit es zur Erfüllung ihrer Aufgabe erforderlich ist. Einsichtnahmen und Eingriffe in die in § 3 Absatz 3 Satz 2 genannten Daten sind im richterlichen Bereich nur zulässig mit Einwilligung der unmittelbar berechtigten Richterinnen und Richter oder auf Grund zwingender technischer Erfordernisse. Die betroffenen Richterinnen und Richter sind über technisch bedingte Eingriffe nach Möglichkeit angemessen zu informieren.

(2) Neben den unmittelbar Berechtigten sind weitere Amtsträgerinnen und Amtsträger der Gerichte und Staatsanwaltschaften sowie die in den datenverarbeitenden Stellen tätigen Beschäftigten nur berechtigt, soweit sich das aus

1. der Einwilligung der unmittelbar Berechtigten,
2. gesetzlichen Vorschriften, insbesondere auch zur Dienstaufsicht, unter Beachtung des Absatzes 3,
3. Erfordernissen des technischen IT-Betriebes oder
4. dem zwingenden Erfordernis, eine unmittelbar bevorstehende Gefahr für die Schutzgüter des § 1 Absatz 1 und des § 3 abzuwehren,

ergibt. Im Einzelfall sowie für regelmäßig wiederkehrende Fälle kann die IT-Kontrollkommission außerhalb des Bereiches des § 3 Absatz 3 Satz 2, höchstens für die Dauer ihrer jeweiligen Amtszeit, aus wichtigen dienstlichen Gründen Eingriffe zulassen, etwa wenn eine Einwilligung wegen der großen Zahl der Betroffenen nicht von allen zuständigen Amtsträgerinnen und Amtsträgern eingeholt werden kann oder wenn unklar ist, welche Personen betroffen sind oder dies nur mit einem unverhältnismäßig hohen Aufwand ermittelt werden kann; die Betroffenen sind hierüber nach Möglichkeit zu informieren.

(3) Statistik im richterlichen Bereich der Justiz darf ausschließlich aus hinreichend aggregierten und anonymisierten Daten im Sinne des § 3 Absatz 2 Nummer 2, soweit sie in Fachverfahren erfasst werden, erstellt werden. Die erforderlichen Daten werden von den jeweiligen Leitungen der Gerichte an das Statistische Amt für Hamburg und Schleswig-Holstein – Anstalt des öffentlichen Rechts – oder an eine andere hierfür unter Beachtung der Grundsätze des § 5 Absatz 2 des Hamburgischen Statistikgesetzes vom 19. März 1991 (HmbGVBl. S. 79, 474), zuletzt geändert am 17. Februar 2009 (HmbGVBl. S. 29, 34), in der jeweils geltenden Fassung bestimmte Stelle übermittelt. An eine andere entsprechende Stelle können die Daten auch vom Statistischen Amt für Hamburg und Schleswig-Holstein – Anstalt des öffentlichen Rechts – weiterübermittelt werden. Eine Weitergabe der übermittelten nicht aggregierten Daten an weitere Stellen oder ein Zugriff auf die übermittelten nicht aggregierten Daten durch sonstige Dritte ist unzulässig. Zu anderen, auch statistischen Zwecken können anonymisierte Daten im Sinne des § 3 Absatz 2 Nummern 1 und 2 von den Leitungen der Gerichte bei hinreichender Beachtung der zu schützenden Interessen übermittelt oder freigegeben werden, wenn diese Daten – soweit möglich – aggregiert sind und sichergestellt ist, dass aus diesen kein Rückschluss auf einzelne Richterinnen und Richter gezogen wird und sie nicht für eine Beobachtung, Analyse und Kontrolle von Verhalten und Leistung der Richterinnen und Richter beziehungsweise Kollegialspruchkörper verwendet werden. Die für die Geschäftsverteilung und die Dienstaufsicht unter Berücksichtigung des § 1 Absätze 1 und 2 erforderlichen Daten gemäß § 3 Absatz 2 Nummer 2 stehen der jeweiligen Leitung des Gerichtes und dem Präsidium im Rahmen ihrer Zuständigkeit zur Verfügung. Entsprechendes gilt für den Kollegialspruchkörper. Über weitergehende interne Auswertungen können die Leitungen der Gerichte mit den Richterräten Dienstvereinbarungen schließen.

(4) Die datenverarbeitenden Stellen erstellen nach Maßgabe der vorstehenden Bestimmungen Konzepte für die Zuordnung von technischen Berechtigungen und den Zugriff auf Daten und Prozesse nach § 3 durch Administratorinnen und Administratoren. Einzelne geschützte Amtsträgerinnen und Amtsträger, die Leitungen der Gerichte und Staatsanwaltschaften sowie Richter- und Personalräte haben im Einzelfall das Recht, die Konzepte und deren Umsetzung einzusehen, soweit Daten und Prozesse nach § 3 betroffen sind.

(5) Soweit für die Einrichtung und den Betrieb der IT Auftragsverarbeiter, einzelne Dienststellen der Justiz oder Dritte eingeschaltet werden, ist die Einhaltung der Vorschriften dieses Gesetzes, gegebenenfalls vertraglich, sicherzustellen. Bei wesentlichen Veränderungen oder dem Neuabschluss von Verträgen ist die IT-Kontrollkommission zu beteiligen.

(6) Der Senat wird ermächtigt, Einzelheiten der Ausgestaltung der Konzepte gemäß Absatz 4 durch Rechtsverordnung zu regeln. Der Senat kann die Ermächtigung durch Rechtsverordnung auf die zuständige Behörde weiter übertragen. Bei Erlass oder Änderungen der Verordnung nach Satz 1 sind die Leitungen der Gerichte und die Staatsanwaltschaften sowie die IT-Kontrollkommission zu beteiligen.

§ 6

IT-Kontrollkommission

(1) Die IT-Kontrollkommission wird bei der zuständigen Behörde eingerichtet. Diese hält für sie eine Koordinierungsstelle vor, stellt ihr die für die Wahr-

nehmung ihrer Aufgaben erforderlichen Mittel zur Verfügung und trägt die durch ihre Tätigkeit entstehenden Kosten.

(2) Die IT-Kontrollkommission besteht aus

1. vier Vertreterinnen beziehungsweise Vertretern der Richterschaft,
2. einer Staatsanwältin beziehungsweise einem Staatsanwalt oder einer Amtsanwältin beziehungsweise einem Amtsanwalt sowie
3. einer Rechtspflegerin beziehungsweise einem Rechtspfleger

mit gleichem Stimmrecht. Der Kommission gehören ferner als beratende Mitglieder zwei Vertreterinnen beziehungsweise Vertreter der Gerichtsleitungen sowie zwei Angehörige der zuständigen Behörde (behördliche Mitglieder) an. Zwei der Mitglieder nach Satz 1 Nummer 1 werden gemeinsam von den Richterräten gemäß § 29 Absatz 1 Nummern 1 bis 3 des Hamburgischen Richtergesetzes (HmbRiG) vom 2. Mai 1991 (HmbGVBl. S. 169), zuletzt geändert am 4. April 2017 (HmbGVBl. S. 96, 97), in der jeweils geltenden Fassung, die zwei weiteren gemeinsam von den Richterräten gemäß § 29 Absatz 1 Nummern 4 bis 8 HmbRiG, das Mitglied nach Satz 1 Nummer 2 vom Personalrat der Staatsanwaltschaften, das Mitglied nach Satz 1 Nummer 3 gemeinsam von den Personalräten der Gerichte und Staatsanwaltschaften gewählt. Die Amtszeit der Mitglieder beträgt drei Jahre. Für ausgeschiedene Mitglieder werden entsprechend Satz 3 neue Mitglieder für die restliche Amtszeit nachgewählt. Der Präses der zuständigen Behörde benennt die behördlichen Mitglieder, die Gerichtsleitungen benennen ihre Vertreterinnen beziehungsweise Vertreter.

(3) Für die Beratung konkreter Vorgänge ist auf Antrag mindestens zweier – auch nicht stimmberechtigter – Mitglieder eine Vertreterin beziehungsweise ein Vertreter der Leitung des betroffenen Gerichtes oder der betroffenen Staatsanwaltschaft hinzuzuziehen.

(4) Die IT-Kontrollkommission trifft ihre Entscheidungen mit der Mehrheit der stimmberechtigten Mitglieder. Die IT-Kontrollkommission gibt sich eine Geschäftsordnung. Sie kann durch Beschluss Befugnisse auf einzelne Mitglieder übertragen.

(5) Die Beratungen der IT-Kontrollkommission sind grundsätzlich vertraulich, Einzelheiten regelt die Geschäftsordnung. Die Mitglieder der IT-Kontrollkommission sind zur Verschwiegenheit verpflichtet, soweit das zum Schutz der Rechte Einzelner, zum Schutz von Betriebs- und Geschäftsgeheimnissen oder zur Gewährleistung der IT-Sicherheit erforderlich ist. Absatz 3 sowie § 7 Absätze 3 und 4 sowie § 8 bleiben unberührt.

(6) Die Mitglieder der IT-Kontrollkommission mit Ausnahme der Vertreterinnen beziehungsweise Vertreter der Gerichtsleitungen sind von ihrer dienstlichen Tätigkeit teilweise freizustellen, wenn und soweit es zur ordnungsgemäßen Durchführung ihrer Aufgaben erforderlich ist; für nicht freigestellte Mitglieder ist eine angemessene Aufwandsentschädigung nach § 3 Nummer 12 des Einkommensteuergesetzes in der Fassung vom 8. Oktober 2009 (BGBl. I S. 3369, 3862), zuletzt geändert am 25. März 2019 (BGBl. I S. 357), in der jeweils geltenden Fassung vorzusehen.

(7) Der Senat wird ermächtigt, weitere Einzelheiten der Wahl und der Amtszeit der Mitglieder nach Absatz 2 Satz 1 Nummern 1 bis 3, der Bestimmung und der Amtszeit der beratenden Mitglieder, der Beschlussfassung in der IT-Kontrollkommission sowie der Freistellung und der Aufwandsentschädigung der Mitglieder der Kommission durch Rechtsverordnung zu regeln. Der Senat kann die Ermächtigung durch Rechtsverordnung auf die zuständige Behörde weiter übertragen. Bei Erlass oder Änderungen der Verordnung nach Satz 1 sind die Leitungen der Gerichte und die Staatsanwaltschaften sowie die IT-Kontrollkommission zu beteiligen.

§ 7
Kontrollrechte der IT-Kontrollkommission

(1) Die IT-Kontrollkommission kann sowohl anlassbezogen als auch verdachtsunabhängig, zur Aufdeckung von Verstößen und Missbrauch oder vorbeugend, Einsicht in alle Datenverarbeitungsvorgänge gemäß §§ 4 und 5 nehmen und alle dabei anfallenden Daten zur Erfüllung ihrer Aufgaben nach diesem Gesetz verarbeiten. Sie kann ferner Einsicht in alle die IT betreffenden Verträge und Konzepte nehmen sowie auch Inaugenscheinnahmen der IT-Einrichtungen vornehmen. Soweit erforderlich kann sie auch Auskünfte von den datenverarbeitenden Stellen einholen. Einsichtnahmen in geschützte Daten und Prozesse im Sinne des § 3 Absatz 2 Nummer 1 und Absatz 3 Satz 2 sind unbeschadet des § 5 Absatz 1 nur gestattet, soweit sie zur Aufgabenerfüllung geboten sind. Die Rechte nach den Sätzen 1 bis 3 stehen auch einer Minderheit von mindestens zwei stimmberechtigten Mitgliedern zu.

(2) Die Ergebnisse der Überprüfungen nach § 4 Absatz 4 Satz 2 sind der IT-Kontrollkommission auf Verlangen zugänglich zu machen.

(3) Soweit dies zur ordnungsgemäßen Erfüllung ihrer Aufgaben erforderlich ist, kann die IT-Kontrollkommission sachkundige Dritte, auch aus den Gerichtsverwaltungen oder der zuständigen Behörde, hinzuziehen. Soweit die Hinzuziehung externer Sachverständiger im Einzelfall erforderlich ist, vergibt die zuständige Behörde unter Beteiligung der IT-Kontroll-

kommission die Aufträge und trägt die Kosten; Rückgriffsforderungen nach sonstigen Vorschriften bleiben unbenommen.

(4) Stellt die IT-Kontrollkommission Verstöße gegen die Bestimmungen dieses Gesetzes fest, so unterrichtet sie die zuständige Behörde, die betroffene Dienststelle sowie gegebenenfalls den jeweiligen IT-Dienstleister und, sofern sie das für geboten erachtet, die Betroffenen. Ferner fordert sie die verantwortlichen Stellen unter Setzung einer angemessenen Frist zur Beseitigung auf. Handelt es sich um einen erheblichen Verstoß oder erfolgt keine fristgerechte Beseitigung, so spricht die IT-Kontrollkommission eine Beanstandung aus. Die zuständige Behörde ist verpflichtet, auf Beanstandungen im Rahmen ihrer Zuständigkeit angemessen zu reagieren und die IT-Kontrollkommission sowie die Leitungen der Gerichte und Staatsanwaltschaften über ergriffene Maßnahmen zu unterrichten.

(5) Einzelne geschützte Amtsträgerinnen und Amtsträger, die Leitungen der Gerichte und Staatsanwaltschaften sowie Richter- und Personalräte haben das Recht, sich in Verdachtsfällen oder mit konkreten Beschwerden an die IT-Kontrollkommission zu wenden.

(6) Außerhalb der bei den Gerichten im Rahmen ihrer justitiellen Tätigkeit vorgenommenen Datenverarbeitung wird die IT-Kontrollkommission zum Schutz personenbezogener Daten nicht tätig.

§8
Berichte

(1) Die IT-Kontrollkommission erstellt jährlich zum 31. Oktober einen Bericht über die Organisation und den Einsatz der IT in den Gerichten und Staatsanwaltschaften. Der Bericht enthält auch eine Darstellung zur Gewährleistung der Ziele dieses Gesetzes. Die IT-Sicherheit und die Rechte Einzelner sind bei der Erstellung des Berichtes zu beachten.

(2) Der Bericht ist den Richter- und Personalvertretungen, den Leitungen der Gerichte und Staatsanwaltschaften sowie der zuständigen Behörde unverzüglich zuzuleiten.

(3) Besteht nach Auffassung der zuständigen Behörde, der Leitung eines Gerichts, der Leitung einer Staatsanwaltschaft oder eines zuständigen Richter- oder Personalrates die Besorgnis einer über einen Einzelfall hinausgehenden Verletzung der in §1 Absatz 1 genannten Schutzgüter, so ist auch außerhalb der Frist nach Absatz 1 zu berichten.

§9
Verhältnis zu anderen Regelungen, Übergangsregelungen, Evaluation

(1) Die Vorschriften des Hamburgischen Richtergesetzes und des Hamburgischen Personalvertretungsgesetzes zur Mitbestimmung, diejenigen des Hamburgischen Beamtengesetzes zur Verbändebeteiligung sowie der Dataport-Staatsvertrag vom 27. August 2003 (HmbGVBl. S. 590), zuletzt geändert vom 6. August 2013 bis 27. September 2013 (HmbGVBl. 2014 S. 52), bleiben unberührt.

(2) Spätestens vier Jahre nach seinem Inkrafttreten überprüft der Senat dieses Gesetz im Hinblick auf seine Anwendung und Auswirkungen, berücksichtigt dabei die Berichte der IT-Kontrollkommission und berichtet der Bürgerschaft über das Ergebnis.

(3) Ist zum Zeitpunkt des Erlasses oder der Änderung einer Verordnung nach §4 Absatz 7 Satz 1, §5 Absatz 6 Satz 1 und §6 Absatz 7 Satz 1 eine IT-Kontrollkommission noch nicht gebildet, so treten an ihre Stelle die Richter- und Personalräte der Gerichte sowie der Personalrat der Staatsanwaltschaften. Gleiches gilt für die Zulassung von Eingriffen nach §5 Absatz 2 Satz 2.

(4) Soweit zum Zeitpunkt des Inkrafttretens dieses Gesetzes Vorgaben wegen bestehender technischer Gegebenheiten noch nicht vollständig verwirklicht werden können, wirken die jeweiligen datenverarbeitenden Stellen auf die möglichst baldige Umsetzung hin.

Begründung

Allgemeiner Teil

1. Im Zuge der fortschreitenden Digitalisierung und der absehbar vollständigen Umstellung auf elektronische Aktenführung und -bearbeitung ergeben sich neue Herausforderungen für die Justiz: Die richterliche Unabhängigkeit (Artikel 97 GG), die sachliche Unabhängigkeit der Rechtspflegerschaft und das Legalitätsprinzip bei der Staatsanwaltschaft müssen weiterhin gewährleistet sein. Zudem sind die in der Justiz tätigen Personen auch generell vor unzulässigen Eingriffen zu schützen, die durch neue Techniken möglich werden können. Zugriffe auf elektronische Dokumente sind bei unsachgemäßen und unzureichenden Schutzmaßnahmen um ein Vielfaches leichter durchzuführen als Zugriffe auf Papiervorgänge. Es besteht in diesem Zusammenhang die Gefahr, dass damit Potentiale für Beeinflussungen und unzulässige Kontrollen der Arbeit, Arbeitsweise und Leistung eröffnet werden. Überdies kann subjektiv bei denjenigen, die mit neuer Technik arbeiten, schnell ein Gefühl des „Beobachtet-Werdens“ entstehen. Dies gilt im Grundsatz unabhängig davon, wo die Daten verarbeitet werden. Die sich aus der Digitalisierung der Arbeit der Justiz potentiell ergebenden Gefahren wirksam einzuhegen, ist Ziel des Gesetzes. Neue Arbeitsbedingungen werden demgegenüber durch das Gesetz nicht konstituiert.

   Bereits jetzt ist bei der Organisation und dem Betrieb von Informations- und Kommunikationstechnik (IT) in der Hamburger Justiz ein hohes Sicherheitsniveau gewährleistet. Dieser Zustand soll langfristig gesichert und effektiver Kontrolle (auch) durch die betroffenen Amtsträgerinnen und Amtsträger unterworfen werden. Im Ergebnis soll ein Zustand geschaffen werden, der hinsichtlich des Schutzes der in Rede stehenden Rechtsgüter dauerhaft mindestens dasselbe Niveau gewährleistet, wie es zu Zeiten vollständig in Papier geführter Akten bestand. Zur Gewährleistung definiert das Gesetz Schutzanforderungen und beschränkt Eingriffe in Daten und Prozesse in mehrfacher Hinsicht. Zur Kontrolle sieht das Gesetz die Schaffung einer unabhängigen, primär mit Vertreterinnen und Vertretern der Richterschaft besetzten IT-Kontrollkommission vor, die die Einhaltung der Schutzvorschriften kontrolliert und zu diesem Zwecke mit umfassenden Aufklärungsbefugnissen ausgestattet ist.

2. Das Gesetz zieht damit gleichzeitig die Konsequenzen aus der dienstgerichtlichen Entscheidung über die von Richterinnen und Richtern des Landes Hessen erhobene sog. hessische Netzklage. Gegenstand dieser rechtlichen Auseinandersetzung war – bis hin zum Bundesverfassungsgericht – die Frage, ob die verfassungsrechtlich gewährte und gebotene richterliche Unabhängigkeit dadurch verletzt wird, dass der Betrieb und die Administration des EDV-Netzes für den Rechtsprechungsbereich bei der Hessischen Zentrale für Datenverarbeitung (HZD), einer Oberbehörde der Landesfinanzverwaltung, und nicht bei den Gerichten angesiedelt ist.

   Nähere Maßstäbe für eine gesetzliche Regelung in diesem Zusammenhang können dem in dieser Sache ergangenen Urteil des Dienstgerichtshofes Frankfurt vom 20. April 2010 (DGH 4/08) entnommen werden: Danach ist es insbesondere erforderlich, verbindliche Regeln über den Umgang mit richterlichen Dokumenten festzulegen, die sicherstellen, dass diese grundsätzlich nicht an Dritte weitergegeben werden. Die Einhaltung dieser Regeln soll durch die zuständige Behörde „unter gleichberechtigter Mitwirkung von gewählten Vertretern der Richterschaft“ im Rahmen einer Kommission mit „uneingeschränkten Auskunfts- und Einsichtsrechten“ überwacht werden (DGH Frankfurt, Urteil vom 20. April 2010, BeckRS 2010, 14555, S. 18). Im zugehörigen Revisionsverfahren hat der Bundesgerichtshof klargestellt, dass hinsichtlich einer Beeinträchtigung der richterlichen Unabhängigkeit allein relevant sei, ob Grund zu der Annahme bestehe, dass das EDV-Netz zur inhaltlichen Kontrolle richterlicher Dokumente im Kernbereich der Rechtsprechung genutzt werde; die bloße Eignung technischer Einrichtungen zu einer solchen Kontrolle genüge insoweit nicht [BGH, Urteil vom 6. Oktober 2011, NJOZ 2012, 787 (788f.)]. Das Bundesverfassungsgericht hat diese Auffassung des Bundesgerichtshofes mit der Erwägung bestätigt, dass jedenfalls unter den vom Dienstgerichtshof Frankfurt formulierten Bedingungen kein Anlass bestehe, eine inhaltliche Kontrolle richterlicher Dateien oder eine Manipulation von Dokumenten zu befürchten; es spreche nichts dafür, dass die Kontrolle unter Beteiligung von Vertretern der Richterschaft nicht hinreichend sein könnte [BVerfG, Beschluss vom 17. Januar 2013, NJW 2013, 2102 (2103)].

   Die IT der Justiz wird auch für Hamburg zum Teil von externen Dienstleistern, derzeit namentlich der Anstalt des öffentlichen Rechts „Dataport“, wahrgenommen: Die Freie und Hansestadt Hamburg ist neben den Ländern Schleswig-Holstein, Bremen und Sachsen-Anhalt Trägerland der An-

stalt des öffentlichen Rechts Dataport, welche IT-Dienstleistungen für öffentlichen Einrichtungen ihrer Trägerländer erbringt und über nach ISO-27001-zertifizierte Rechenzentren für den hochsicheren Betrieb von deren Fachanwendungen und sonstigen IT-Infrastrukturen verfügt. Eine Fachaufsicht besteht für die Freie und Hansestadt Hamburg zwar – anders als für das Land Hessen gegenüber der dortigen Zentrale für Datenverarbeitung – gegenüber Dataport nicht. Dataport wurde auf der Grundlage des Staatsvertrages vom 27. August 2003 zwischen den Ländern Schleswig-Holstein und Freie und Hansestadt Hamburg errichtet und unterliegt gemäß § 10 des Staatsvertrages nur der Rechtsaufsicht der Trägerländer, wobei Aufsichtsbehörde das für ressortübergreifende IT-Angelegenheiten zuständige Ministerium des Landes Schleswig-Holstein ist.

Zur Sicherung der richterlichen Unabhängigkeit ist eine Fachaufsicht aber auch nicht erforderlich; vielmehr kommt es auf eine hinreichende inhaltliche Regelungsdichte der Bestimmungen an, die den Zugriff auf richterliche Dokumente begrenzen und eine Kontrolle der Datenverarbeitung ermöglichen (vgl. DGH Frankfurt, Urteil vom 20. April 2010, BeckRS 2010, 14555, S. 12). Die Fachaufsicht ist – über die Rechtsaufsicht hinausgehend – nicht auf die Kontrolle der Rechtsmäßigkeit beschränkt, sondern umfasst auch Weisungen zur Umsetzung von Zweckmäßigkeitserwägungen. Zum Schutz der richterlichen Unabhängigkeit muss aber gerade nicht auf Zweckmäßigkeitserwägungen eingewirkt werden, sondern es sind „verbindliche konkrete Regeln über den Umgang mit richterlichen Dokumenten“ sowie die Überwachung durch das zuständige Ministerium im „gleichberechtigten Zusammenwirken mit Richtern“ geboten (DGH Frankfurt, Urteil vom 20. April 2010, BeckRS 2010, 14555, S. 14f.). Eine Kontrolle der Einhaltung der konkreten gesetzlichen Vorgaben für den Umgang mit richterlichen Dokumenten und Daten ist Teil der Rechtsaufsicht (diese erstreckt sich stets auf die Beachtung von Gesetz und Satzung).

Die zum Schutz der richterlichen Unabhängigkeit gebotene Effektivität der Kontrolle der Datenverarbeitung wird durch die IT-Kontrollkommission in ihrer in diesem Gesetz vorgesehenen Ausgestaltung und mit den für sie dort vorgesehenen Rechten gewährleistet. Insoweit ist entscheidend, dass die IT-Kontrollkommission die Einhaltung der insbesondere in §§ 4, 5 vorgesehenen Regelungen zu Datenverarbeitung, Sicherheitskonzepten, Protokollierung, internem Kontrollsystem und Zugriffsrechten durch uneingeschränkte Einsichts- sowie ergänzende Auskunftsrechte kontrollieren kann. Diese sind in § 7 vorgesehen, um den skizzierten Ansprüchen zu genügen.

3. Die sich aus der Rechtsprechung im Zusammenhang mit der sog. hessischen Netzklage (Dienstgerichthof Frankfurt BeckRS 2010, 14555; BGH NJOZ 2012, 787; BVerfG NJW 2013, 2102) ergebenden Anforderungen zum Schutz der richterlichen Unabhängigkeit werden durch das Gesetz auf den Schutz der sachlichen Unabhängigkeit der Rechtspfleger (§ 9 RPflG) und auf die Tätigkeiten der Staatsanwaltschaften erstreckt, wobei der Schutzumfang teilweise unterschiedlich ausfällt. Die Staatsanwaltschaft wird zwar gemeinhin der Exekutive zugeordnet. Es handelt sich aber auch bei ihr um ein Organ der Rechtspflege. Hier gilt es, die vom Legalitätsprinzip getragene Ermittlungs- und Anklagetätigkeit (§§ 151 ff. 160 StPO) zu schützen und das Vertrauen in eine von außen unbeeinflusste, objektive Tätigkeit der Staatsanwaltschaft zu erhalten bzw. zu stärken.

Besonderer Teil

Zu § 1:

Die Vorschrift beschreibt die Ziele und den Regelungsbereich des Gesetzes und regelt zudem das Verhältnis zum Datenschutzrecht.

Zu Absatz 1:

Es wird zunächst geregelt, dass der Anwendungsbereich des Gesetzes sich nur so weit erstreckt, wie tatsächlich Informations- und Kommunikationstechnik zur Anwendung kommt. Auf Papierakten, ausgedruckte oder handschriftliche Voten und sämtliche nicht elektronischen Dokumente findet das Gesetz keine Anwendung. Soweit hingegen IT zum Einsatz gelangt, findet das Gesetz umfassend auf alle Systeme, mit denen Daten und Dokumente nach § 3 verarbeitet werden, Anwendung; sowohl die technische Ausgestaltung (Hardware und Software) als auch die organisatorische Ausgestaltung des Betriebes (z.B. Räume, Personal, Prozesse) sind erfasst. Ferner regelt das Gesetz sowohl die Datenverarbeitung durch externe IT-Dienstleister als auch die durch die IT-Stellen der Gerichte und Staatsanwaltschaften selbst, denn auch im letzteren Bereich ist das gesetzlich vorgesehene Schutzniveau zu gewährleisten.

Des Weiteren werden die Regelungsziele des Gesetzes beschrieben. Sowohl die Arbeit der Richterinnen und Richter als auch die der Rechtspflegerinnen und Rechtspfleger, Staatsanwältinnen und Staatsanwälte, Amtsanwältinnen und Amtsanwälte ist geschützt. Das unterschiedliche Niveau der Schutzgebote kommt dadurch zum Ausdruck, dass der Schutz der richterlichen Unabhängigkeit umfassend zu gewährleisten ist (Artikel 92, 97 GG), während im Be-

reich der Rechtspflegerschaft (sachliche Unabhängigkeit, § 9 RPflG) und der Staatsanwaltschaften (Legalitätsprinzip und allgemeine Rechtmäßigkeit) eingeschränktere Schutzbereiche benannt sind. Primär ist dabei der Bereich der Entscheidungsvorbereitung und -findung geschützt, denn dort findet die Unabhängigkeit ihre stärkste Ausprägung; im Bereich der weisungsgebundenen Staatsanwaltschaft kann das indes nur stark eingeschränkt gelten.

Zu gewährleisten ist ferner die Funktionsfähigkeit der Justiz in dem Sinne, dass die verantwortliche Behörde, soweit IT eingesetzt wird, zu gewährleisten hat, dass die benötigten Funktionen und Daten im erforderlichen und vertraglich zugesicherten Umfang zur Verfügung stehen (Ausfallsicherheit) und ein zielgerichtetes, effizientes und geschütztes Arbeiten (Benutzungsfähigkeit) ermöglicht wird.

Zu Absatz 2:

Ausdrücklich wird festgehalten, dass die richterliche Unabhängigkeit jeder Art von ausgeweiteten Leistungs- und Verhaltenskontrollen entgegensteht. Die von der Rechtsprechung ausgeformten Kompetenzen der Gerichtsleitungen im Rahmen der Dienstaufsicht dürfen nicht durch technisch mögliche Kontroll- und Auswertungsinstrumente erweitert werden. Die Niederlegung in einem gesonderten Absatz hebt die besondere Bedeutung hervor.

Für den nichtrichterlichen Bereich der Justiz trifft das Gesetz insoweit keine Anordnungen. Allerdings ergeben sich entsprechende Schutzrechte aus Vereinbarungen des Senates mit den Spitzenorganisationen der Gewerkschaften nach § 93 HmbPersVG [bzw. § 94 HmbPersVG (a. F.)].

Zu Absatz 3:

Es handelt sich um eine Ergänzung der Bestimmungen des Absatzes 1 Satz 1 und des Absatzes 2. Die Vorschrift stellt klar, dass das Gesetz sowohl technisch-organisatorische Maßnahmen regelt als auch rechtliche Rahmenbedingungen für die Nutzung der IT durch die Leitungen der Dienststellen, die Justizbehörde und auch die datenverarbeitenden Stellen setzt.

Zu Absatz 4:

§ 1 Absatz 4 stellt klar, dass es sich bei Vorschriften dieses Gesetzes nicht um datenschutzrechtliche Vorschriften handelt. Vielmehr werden durch dieses Gesetz ausschließlich technische, betriebliche und organisatorische Maßnahmen und damit technische Sicherheitsstandards zum Schutz der Tätigkeit von Richterinnen und Richtern, Staatsanwältinnen und Staatsanwälten, Amtsanwältinnen und Amtsanwälten, Rechtspflegerinnen und Rechtspflegern und der in Absatz 1 genannten Schutzbereiche festgeschrieben. Soweit hiermit Regelungen zur Verarbeitung bestimmter von den vorgenannten Personen verarbeiteter Daten getroffen werden, ist es unausweichlich, dass hiervon auch personenbezogene Daten mitumfasst sind. Deshalb wird der Anwendungsbereich dieses Gesetzes durch § 1 Absatz 4 dahingehend beschränkt, dass für die Verarbeitung von personenbezogenen Daten die allgemeinen datenschutzrechtlichen Vorschriften [VO (EU) 2016/679, BDSG für den justitiellen Bereich, HmbDSG für den nichtjustitiellen Bereich] vorrangig anzuwenden sind. Satz 2 dient insbesondere der Klarstellung, dass auch das HmbDSG im nichtjustitiellen Bereich sämtlichen Datenverarbeitungsvorschriften dieses Gesetzes in Bezug auf die Verarbeitung personenbezogener Daten vorgeht, sodass Vorschriften dieses Gesetzes nicht als datenschutzrechtliche Regelungen verstanden werden können.

Die Regelung dient zudem der Klarstellung, dass dieses Gesetz die Gesetzgebungskompetenz des Bundes bezüglich des gerichtlichen Verfahrens gem. Artikel 70, 74 Absatz 1 Nr. 1 GG und die damit verbundene Annexkompetenz zur Regelung des Datenschutzes nicht berührt.

Zu § 2:

Die Vorschrift hält die unterschiedlichen Zuständigkeiten bei Organisation und Einsatz der IT fest. Sie nimmt keine Änderungen am Ist-Zustand vor, steht aber auch organisatorischen Veränderungen in der Zukunft nicht im Wege; insbesondere können die momentan von den Gerichten oder den Staatsanwaltschaften wahrgenommenen Aufgaben des IT-Betriebes und der IT-Organisation ausgeweitet oder verringert werden, ohne dass hiervon der Regelungsgehalt des Gesetzes berührt wäre.

Zu Absatz 1:

Geregelt wird die grundsätzliche rechtliche und politische Verantwortung der zuständigen Behörde für den Betrieb und die Organisation der IT. Letztlich hat die Behörde – im Rahmen der Vorgaben des § 1 und unter Beachtung des Absatzes 2 – zu entscheiden und zu verantworten, wie die IT beschafft wird, wie sie zum Einsatz kommt und wer sie verwaltet. Dass dabei die Gerichte und Staatsanwaltschaften intensiv eingebunden werden, entspricht der Bedeutung der Sache und guter hamburgischer Tradition.

Ferner wird die zuständige Behörde darauf verpflichtet, die Einhaltung der Vorschriften dieses Gesetzes und seiner Ziele zu gewährleisten. Hieraus erwächst eine generelle Verpflichtung, bei Organisation und Betrieb der IT die Schutzgüter und Vorgaben des § 1 Absatz 1 und 2 stets zu beachten.

Zu Absatz 2:

Der Begriff der Aktenhoheit stellt klar, dass sich hinsichtlich der souveränen Verfügung der Gerichte über die Akten durch die fortschreitende Einführung der bzw. die zunehmende Umstellung auf IT nichts am bisherigen Zustand ändern darf. Der Grundsatz der Aktenhoheit ist ein Strukturelement der gerichtlichen Rechtsschutzgewährung; dementsprechend ist er ein zentraler Maßstab für die Ausgestaltung der gerichtlichen IT. Den Rechtsprechungsorganen muss die souveräne Verfügung über die Akten erhalten bleiben.

Das Bundesverfassungsgericht hat mit seinem Beschluss vom 22. März 2018 (BVerfG, 2 BvR 780/16, juris, Rn 50 f.) verdeutlicht, dass den Gerichten im Gewaltengefüge notwendig eine Sonderstellung zukommt, die eine institutionelle Unabhängigkeit erfordert:

„... Dabei verlangt die funktionsbedingt erforderliche Unabhängigkeit und Unparteilichkeit der rechtsprechenden Gewalt eine striktere Trennung der Rechtsprechung von den übrigen Gewalten, als sie durch das in Artikel 20 Absatz 2 Satz 2 GG normierte, Gewaltenverschränkungen erlaubende allgemeine Organisations- und Funktionsprinzip der Gewaltenteilung gefordert wird. Ausnahmen hiervon sind lediglich in geringem Umfang zulässig, wenn – wie etwa bei der Betrauung von Richtern mit Geschäften der Justizverwaltung – der Charakter der Gerichte als besondere Organe der Staatsgewalt nicht beeinträchtigt wird [vgl. BVerfGE 4, 331 (346 f.)].

a) Von besonderer Bedeutung für die vorliegend aufgeworfenen Fragen ist das Gebot der organisatorischen Trennung von Rechtsprechung und Verwaltung [vgl. BVerfGE 18, 241 (254); 27, 312 (321) – zu Artikel 20 Absatz 2 Satz 2 GG)], zunächst im Sinne institutioneller Unabhängigkeit (vgl. Tschentscher, Demokratische Legitimation der dritten Gewalt, 2006, S. 162). Nur wenn die Gerichte als besondere, von der Exekutive getrennte Institutionen ausgestaltet sind, kann eine Rechtsprechung gegenüber dem Staat oder seinen Behörden im Sinne des Artikel 19 Absatz 4 GG wie durch einen unbeteiligten Dritten verwirklicht werden [BVerfGE 4, 331 (346)].“

Bislang werden die Verfahren in Papierakten geführt, die vom Gericht bzw. der Staatsanwaltschaft verwaltet werden und über deren Inhalt die jeweils zuständigen Bearbeiter bestimmen. Die IT kann und darf weder durch ihre Organisation noch durch ihren Betrieb vorgeben, was Inhalt der Akte wird. Zwar können und dürfen elektronische Akten (technisch) auch bei externen Dienstleistern geführt und dort alle für den IT-Betrieb erforderlichen technischen Voraussetzungen geschaffen und Maßnahmen durchgeführt werden (wie etwa Speicherung, Backups, Virenprüfung, Sperrung befallener Dateien etc.). Für den Inhalt der Akten und deren Herausgabe, für Fragen der Einsichtnahme etc. bleiben aber allein die zuständigen Bearbeiterinnen und Bearbeiter (Inhalt der Akte) bzw. die Dienststelle (Verwaltung der „Akte an sich“) zuständig. Jeder Eingriff in die Akte von außerhalb berührt damit auch die Aktenhoheit und bedarf der Rechtfertigung.

Soweit die Vorschrift von dem „jeweils zuständigen Gericht beziehungsweise der jeweils zuständigen Staatsanwaltschaft“ spricht, sind damit die – ja primär verantwortlichen – Amtsträgerinnen und Amtsträger als Teile dieser Stellen mit umfasst. Die Aktenhoheit, soweit sie den Gerichtsleitungen zusteht, berechtigt – selbstverständlich – diese nicht zu Eingriffen in die richterliche Unabhängigkeit.

Zu Absatz 3:

Zentrale Instanz zur Kontrolle der Gewährleistung der Ziele des Gesetzes ist eine IT-Kontrollkommission (ITKK), deren Struktur, Aufgaben und Rechte insbesondere in §§ 6, 7 näher beschrieben werden. Die Einrichtung der Kommission setzt die Vorgaben der Rechtsprechung um und dient dem umfassenden Schutz der in § 1 genannten Schutzgüter. Kontrollaufgaben bestehen dabei sowohl gegenüber der Exekutive als auch gegenüber den Gerichtsleitungen, sowie selbstverständlich gegenüber allen datenverarbeitenden Stellen inner- und außerhalb der Justiz.

Die Vorschrift stellt zudem klar, dass die ITKK in ihrem Wirken Unabhängigkeit genießt; diese Unabhängigkeit erstreckt sich auch auf die jeweiligen Mitglieder der Kommission, soweit sie ihre Aufgaben nach diesem Gesetz wahrnehmen. Sie sind aber an die Vorgaben dieses Gesetzes gebunden, etwa was Vertraulichkeit und Verschwiegenheit betrifft.

Zu § 3:

Die Norm konkretisiert, welche Daten und Abläufe auf welchem Niveau zu schützen sind und welche Personen den Schutz des Gesetzes genießen. Sie ist eine der zentralen Vorschriften des Gesetzes.

Zu Absatz 1:

Die Vorschrift definiert den sachlichen Schutzbereich des Gesetzes und greift dabei die Bestimmungen des § 1 auf. Geschützt sind im richterlichen, staatsanwaltlichen und rechtspflegerischen Bereich grundsätzlich alle Entscheidungen sowie insbesondere deren Vorbereitung. Der Begriff der Vorbereitung ist dabei im weitesten Sinne zu verstehen. Alle vorbereitenden Arbeiten, seien es durch die geschützten Amtsträgerinnen und Amtsträger (Legaldefinition in

Absatz 4) angefertigte Auswertungen von Literatur und Rechtsprechung, Notizen zu Dokumenten, Entscheidungs- oder Verfügungsentwürfe, Verfügungen, Voten – für den Bearbeiter und/oder Dritte – oder sonstige der Vorbereitung dienende Dokumente und Prozesse, zählen dabei zum Bereich der Entscheidungsfindung. Entscheidungen im Sinne der Vorschrift sind auch Zwischenentscheidungen. Zum staatsanwaltlichen Bereich gehört auch die Tätigkeit der Amtsanwältinnen und Amtsanwälte.

Zu Absatz 2:

Die Vorschrift konkretisiert, welche Daten im Rahmen der in Absatz 1 beschriebenen Entscheidungsprozesse regelmäßig anfallen, da sie entweder der Entscheidungsfindung der geschützten Amtsträgerinnen und Amtsträger zugrunde liegen bzw. für die Entscheidungsfindung oder Verfahrensbearbeitung aus den zugrundeliegenden Daten weiterverarbeitet (z.B. verdichtet oder extrahiert) oder im Verlauf der gerichtlichen oder staatsanwaltschaftlichen Verfahrensbearbeitung durch Beschäftigte oder (automatisiert) durch IT-Systeme der Justiz erzeugt werden. Dabei wird unterschieden zwischen

– Inhaltsdaten: Inhaltsdaten werden in der Regel zur Durchdringung des juristischen Sachverhalts benötigt. Hierbei handelt es sich in erster Linie um Dokumente (Schriftsätze aller Art) der Verfahrensbeteiligten oder Dritter (z.B. Ermittlungsakten, Beiakten), die über elektronische Eingangskanäle bei Gericht oder bei der Staatsanwaltschaft eingereicht oder über Briefpost, Telefax oder persönliches Erscheinen eingereicht und für die elektronische Bearbeitung bei Gericht oder bei der Staatsanwaltschaft digitalisiert (gescannt) werden, oder um Dokumente, die im Rahmen der Verfahrensbearbeitung durch die zuständigen Amtsträgerinnen und Amtsträger erzeugt werden und zur Verfahrensakte gelangen (z.B. Verfügungen, Urteile, Beschlüsse). Zu den Inhaltsdaten gehören auch die mit den o.g. Dokumenten verbundenen Daten der qualifizierten elektronischen Signaturen, da diese die handschriftliche Unterschrift der die jeweiligen Inhalte verantwortenden Personen abbilden, sowie die bei der maschinellen Verarbeitung erzeugten Prüfprotokolle und Transfervermerke, welche inhaltliche Aussagen über den frist- und formgerechten Zugang der o.g. Dokumente bzw. über deren gesetzeskonforme Umwandlung enthalten. Auch auf den o.g. Dokumenten angebrachte Annotationen (d.h. z.B. elektronische Kommentare oder Unterstreichungen) werden zu Inhaltsdaten, sofern diese nicht nur temporär zum Zwecke der persönlichen Durchdringung des Sachverhaltes angebracht werden, sondern mit dem jeweiligen Dokument revisionssicher zur Akte gelangen sollen. In zweiter Linie können den o.g. Dokumenten durch die einreichende Person selbst oder bei der weiteren Verarbeitung bei Gericht oder Staatsanwaltschaft sog. Metadaten beigefügt werden. Metadaten sind strukturierte maschinenlesbare Datensätze, welche Informationen über Merkmale der o. g. Dokumente enthalten, wie z.B. zu deren Inhalt [z.B. Aktenzeichen, Kläger- und Beklagtenname; vgl. z.B. §2 Absatz 3 der Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung – ERVV)] oder zu der Struktur (z.B. Reihenfolge, Inhaltsverzeichnis, Anlagen) von mehreren Dokumenten eines Schriftsatzes oder einer Akte.
– Verfahrensbezogene Daten: Hierbei handelt es sich um manuell oder automatisiert erfasste oder weiterverarbeitete fachliche Daten, die zur Verwaltung der gerichtlichen oder staatsanwaltschaftlichen Verfahren oder der Akten benötigt werden, z.B. Anschriften der Verfahrensbeteiligten, den Verfahrensstand, die Benennung des Verfahrensgegenstandes, um Fristen und Termine (z.B. Gerichtsverhandlungen), Verweise auf Akten, Schriftsätze oder Beweismittel, Eingangs- und Erledigungsdaten, die Art der Erledigung, das Aktenzeichen, das Erstellungsdatum oder die Aufbewahrungsdauer einer Akte etc.
– Logdaten: Hierbei handelt es sich um das automatisch geführte Protokoll bestimmter technischer Aktionen auf einem IT-System. Protokolldaten werden in der Regel erhoben, um Fehler oder Missbrauch erkennen, vermeiden oder aufklären zu können (z.B. unerlaubtes Eindringen in ein IT-System) oder um im Fall eines Fehlers oder eines unerwünschten Ergebnisses die Rücksetzung auf einen früheren Stand zu erlauben (z.B. „Rückgängig“-Aktion bei einem Schreibprogramm).

Zu Absatz 3:

Für bestimmte Daten besteht die Notwendigkeit eines gesteigerten Schutzes. Das Schutzniveau für diese Daten wird zweistufig festgelegt. Gewährleistet wird es dadurch, dass weitere Vorschriften des Gesetzes auf diese Schutzbestimmungen Bezug nehmen.

Grundsätzlich besonders zu schützen sind alle Daten, die den Prozess der Entscheidungsfindung in irgendeiner Weise dokumentieren; dieser Bereich stellt – insbesondere bei der richterlichen Tätigkeit – den Kern der zu schützenden Güter dar. Einflüsse auf die Entscheidungsfindung müssen vermieden werden, was auch durch den Schutz „vorbereitender“ Dokumente erfolgt. Dabei gilt wiederum für den Bereich der weisungsgebundenen Staatsanwaltschaften

anderes als für die Tätigkeit der Richterinnen und Richter sowie der in sachlicher Unabhängigkeit tätigen Rechtspflegerinnen und Rechtspfleger.

Ein nochmals gesteigertes Schutzniveau ergibt sich – aus den genannten Gründen wiederum primär für den richterlichen und rechtspflegerischen Bereich – für die in Satz 2 genannten Daten, soweit sie in irgendeiner Weise Rückschlüsse auf den Prozess der Entscheidungsfindung zulassen. Hier wird zunächst der Kern der zur Entscheidungsfindung dienenden Dokumente und Daten definiert. Dabei geht es um Entscheidungsentwürfe, auch für Zwischenentscheidungen, Entwürfe zu Verfügungen, Voten, alle der Vorbereitung dienenden Arbeiten (etwa die durch den geschützten Amtsträger aufgezeichneten Ergebnisse von Strukturierungsvorgängen, Datenbankrecherchen o. ä.), als persönlich gekennzeichnete Annotationen, das heißt nur zur persönlichen Kenntnisnahme angebrachte Anmerkungen der Amtsträgerin oder des Amtsträgers an anderen Dokumenten, sowie Beratungs- und Abstimmungsdokumente. Schließlich genießen auch Log- und Metadaten, die sich auf die IT-Nutzung der geschützten Amtsträgerinnen und Amtsträger beziehen, wie z.B. etwaige technische Zusatzinformationen über Verfasser von Dokumenten oder Bearbeitungsdauer, umfassenden Schutz. Letzteres dient der Gewährleistung der Regelung des §1 Absatz 2.

Die jeweiligen Autoren der geschützten Daten und Dokumente sind befugt, diese wieder zu löschen, sofern sie nicht Aktenbestandteil geworden sind.

Zu Absatz 4:

Die Vorschrift enthält eine Legaldefinition der „geschützten Amtsträgerinnen und Amtsträger“. Dieser Begriff wird im Gesetz anders gebraucht als der des „Amtsträgers“ bzw. der „Amtsträgerin“ im allgemeinen Sinne, zu dem alle Mitarbeiterinnen und Mitarbeiter der Gerichte und Staatsanwaltschaften, etwa auch Urkundsbeamten der Geschäftsstelle und Justizfachangestellte, zählen. Geschützte Amtsträgerinnen und Amtsträger sind dagegen nur die in dieser Norm genannten Personengruppen.

Zu Absatz 5:

Hier ist inhaltlich geregelt und legaldefiniert, wer unmittelbar – also primär – „berechtigt“ für die Handhabung der genannten Daten und Prozesse ist. Dies sind die Amtsträgerinnen und Amtsträger (nur) der Gerichte und Staatsanwaltschaften, die das jeweilige Verfahren bearbeiten, im Rahmen ihrer Zuständigkeit. Zuständigkeiten können sich dabei ergeben:

- Auf Grund gesetzlicher Vorschriften: Dies ist weit zu verstehen. Insoweit wird auf die Erläuterung zu §5 Absatz 3 verwiesen. Unmittelbar berechtigt können in diesem Zusammenhang aber immer nur Personen sein, die in gesetzlich zulässiger Weise zum Inhalt einer Akte beitragen.
- Aus den Geschäftsverteilungsplänen: Hier sind die jeweiligen Zuständigkeiten, im Bereich der Gerichte durch Präsidiumsbeschluss, geregelt.
- Aus Regelungen im Rahmen der Organisationshoheit der Leitungen der Gerichte und Staatsanwaltschaften sowie – im nichtrichterlichen Bereich – der Landesjustizverwaltung: Insbesondere im nichtrichterlichen Bereich werden die Aufgaben in weitem Umfang durch die Leitungen der Gerichte und Staatsanwaltschaften bzw. die Landesjustizverwaltung verteilt. Die Organisationsgewalt erstreckt sich zum Beispiel auf die Zuteilung der Urkundsbeamtinnen und -beamten der Geschäftsstelle, die Landesjustizverwaltung hat beispielsweise Kompetenzen im Bereich der Bezirksrevisorinnen und -revisoren sowie der Gerichtsvollzieherinnen und Gerichtsvollzieher.

Zu §4:

Die Vorschrift trifft Regelungen technisch-organisatorischer Art, die sich überwiegend an die datenverarbeitenden Stellen richten und in erster Linie sicherstellen sollen, dass die Schutzgüter des §3 in technischer Hinsicht nicht mehr als unbedingt nötig beeinträchtigt werden. Hierzu wird eine Vielzahl von Vorgaben gemacht.

Zu Absatz 1:

Adressat dieser Vorschrift sind sowohl die datenverarbeitenden Stellen (Legaldefinition in Absatz 2) als auch, soweit sie die Ausgestaltung der eingesetzten IT verantworten, die zuständige Behörde und die Leitungen der Gerichte und Staatsanwaltschaften. Inhaltlich wird geregelt, dass die allgemeinen Grundsätze der Datensparsamkeit und Datenvermeidung auch im Regelungsbereich des Gesetzes zu beachten sind. Es ist nur das an Daten zu erfassen, was zur Erledigung einer Fachaufgabe und zum sicheren, effizienten, barrierefreien und ergonomischen Betrieb der IT erforderlich ist. Das gilt aber nicht für die durch die Tätigkeit im justitiellen Bereich durch geschützte Amtsträgerinnen und Amtsträger erstellte Daten.

Der Begriff der Verarbeitung bezeichnet im Sinne des gemäß der auch hier gültigen Definition Artikels 4 Nr. 2 der Datenschutzgrundverordnung [VO (EU) 2016/679] „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Über-

mittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.

Zu Absatz 2:

Die Vorschrift enthält zunächst eine Legaldefinition des Begriffes „datenverarbeitende Stelle“. Datenverarbeitende Stelle sind neben externen, in der Datenverarbeitung für die Justiz tätigen Dienstleistern, wie etwa Dataport, alle IT-Stellen der Gerichte und Staatsanwaltschaften sowie andere Stellen inner- und außerhalb der hamburgischen Verwaltung, die Justizdaten verarbeiten.

Diese Stellen haben, so der weitere Regelungsgehalt der Vorschrift, immer eine möglichst sichere Verarbeitung anhand des Standes der Technik zu gewährleisten. Zu diesem Zweck müssen gegebenenfalls, wenn sich sicherheitsrelevante technische Neuerungen oder Probleme ergeben, Soft- und gegebenenfalls auch Hardware sowie betriebliche Prozesse entsprechend angepasst werden.

Zu Absatz 3:

Auch dieser Absatz richtet sich an die datenverarbeitenden Stellen. Er enthält konkrete Befehle, die dem Schutz der Rechtsgüter des §3 dienen. Er führt ferner Begrifflichkeiten ein:

Eingriff im Sinne des Gesetzes ist dabei im weitesten Sinne zu verstehen. Der Begriff beschreibt in technischer Hinsicht jede denkbare, über bloße Einsichtnahme hinausgehende Art, mit einem Datum umzugehen, einschließlich seiner Veränderung, unabhängig davon, wer ihn vornimmt. Daneben bezeichnet er Eingriffe im allgemeinen Sprachgebrauch, also Einwirkungen auf Prozesse, etwa der Entscheidungsfindung.

Übermittlung bezeichnet als Unterfall des Eingriffes jede Weiterleitung eines Datums an einen anderen Ort zu jedwedem Zweck.

Zu Absatz 4:

Auch diese Vorschrift richtet sich an die datenverarbeitenden Stellen. Sie gibt ihnen auf, präzise Sicherheitskonzepte zu erstellen, anhand derer es der zuständigen Behörde und vor allem der ITKK (vgl. §2 Absatz 3) möglich ist, die Sicherheitsarchitektur nachzuvollziehen und auf ihre Wirksamkeit zu kontrollieren. Wesentliche Anforderungen hierfür definiert die Informationssicherheitsleitlinie (IS-LL) der Freien und Hansestadt Hamburg; dort wird auf BSI-Standards Bezug genommen. Die Konzepte müssen auch interne Kontrollmechanismen sowie Vorgaben zur revisionssicheren Protokollierung administrativer Zugänge enthalten. Die Vorschrift führt ferner weitere Begrifflichkeiten ein:

Zugriff im Sinne der Vorschrift ist der „technisch erfolgende Eingriff“, mithin ein Unterfall des Eingriffes.

Administratorinnen und Administratoren im Sinne des Gesetzes sind primär Beschäftigte der datenverarbeitenden Stellen, die zwecks der Organisation oder des Betriebes der zur Verarbeitung von Daten und Dokumenten nach §3 genutzten IT-Systeme über technische Berechtigungen verfügen. Hierzu zählen ferner auch justizinterne Personen, die etwa nur für eine kleine Gruppe von Bediensteten die Zugriffsrechte verwalten. Administratorinnen und Administratoren verfügen also über technische Eingriffsmöglichkeiten; die technische Berechtigung, also die Möglichkeit des Eingriffes im Sinne des „Könnens“, ist zu unterscheiden von der „rechtlichen Berechtigung“ im Sinne der §3 Absatz 5, §5, die das „Dürfen“ regelt.

Eine revisionssichere Protokollierung eines administrativen Zugriffs liegt dann vor, wenn in nicht veränderbarer Weise protokolliert ist, mit welcher administrativen Kennung auf welches IT-System (z.B. eine Serveranwendung, eine Datenbank oder ein Endgerät wie ein PC oder ein Notebook) zu welchem Zeitpunkt zugegriffen wird. Die Protokollierung kann dabei (abhängig vom Einsatz der Administratorin beziehungsweise des Administrators und dem zugegriffenen IT-System) auf unterschiedliche Weise erfolgen, etwa als Aufzeichnung der Aktivitäten der Administratorin oder des Administrators (z.B. durch Videoprotokollierung), als Papierdokument mit Abzeichnung durch Zugreifenden und unmittelbar Berechtigten i.S.v. §3 Absatz 5 oder durch IT-interne (organisatorische) Kontrollmechanismen wie etwa ein 4-Augen-Prinzip (Unterschriften von zwei Administratoren). Nähere Vorgaben für die Protokollierung in Abhängigkeit vom zugegriffenen IT-System können mittels Rechtsverordnung erlassen werden.

Soweit die oder der unmittelbar Berechtigte einwilligt, ist eine Protokollierung nicht zwingend erforderlich. Dies deckt in erster Linie die Hilfestellung einer Administratorin oder eines Administrators beim Benutzersupport ab. Soweit mit vertretbarem Aufwand möglich, soll die Zustimmung der oder des unmittelbar Berechtigten protokolliert werden.

Zu Absatz 5:

Zu Kontrollzwecken müssen die ITKK sowie die jeweiligen Leitungen der Gerichte und Staatsanwaltschaften über eine Liste der als Administratorinnen und Administratoren tätigen Personen verfügen.

Zu Absatz 6:

Die Vorschrift richtet sich in erster Linie an die datenverarbeitenden Stellen, kann aber gegebenenfalls auch die zuständige Behörde oder die Leitungen der

Gerichte und Staatsanwaltschaften erfassen. Wer Kenntnis von einem sicherheitsrelevanten Ereignis erlangt, hat dieses binnen angemessener Frist den genannten Stellen mitzuteilen. Die Beurteilung der Frage, ob es sich um ein sicherheitsrelevantes Ereignis handelt, sowie die Angemessenheit der Meldefrist haben sich in erster Linie am Gewicht des Vorfalles und der daraus resultierenden Konsequenzen (z.B. Schadenseintritt, Anzahl der Betroffenen, Schwere der Folgen) zu orientieren. Es bietet sich an, die Art der möglichen Ereignisse (z.B. unbefugte Zugriffe im Einzelfall, generelle Sicherheitslücken oder andere Gefährdungen, siehe auch Absatz 3 Nummern 1 bis 4) und die Zuordnung der auszuführenden Handlungen in einer ergänzenden Rechtsverordnung zu regeln, um einer Überflutung mit irrelevanten Meldungen geeignet vorzubeugen bzw. die Meldungen in Bezug auf gegebenenfalls erst zukünftig entstehende Risikobereiche in geeigneter Weise anpassen zu können.

Zu Absatz 7:

Der Absatz enthält eine Verordnungsermächtigung für den Senat, die auf die zuständige Behörde subdelegiert werden kann. In der Verordnung können geregelt werden:

- Einzelheiten zu den technischen Anforderungen: Das dient dazu, in flexibler Weise die Anforderungen an einen veränderten Stand der Technik oder an neue Bedrohungslagen anpassen zu können.
- Einzelheiten der Protokollierung und der Aufbewahrung der Protokollierung: Hier können Vorgaben zur Art der Protokollierung gemacht sowie vor allem die Aufbewahrungsfristen geregelt werden. Bei der Bemessung der Fristen muss neben dem Kostenaspekt in Ansatz gebracht werden, dass einerseits längere Fristen potentiell bessere Kontrolle durch die ITKK ermöglichen, andererseits aber unter anderem die in Absatz 1 genannten Gesichtspunkte für eine Löschung in eher kurzer Frist sprechen.
- Einzelheiten zu den Meldepflichten: Hier können Vorgaben gemacht werden, welche Gruppen von Vorfällen binnen welcher Frist zu melden sind. Sinnvoll erscheint etwa eine Staffelung: Schwerwiegende Fälle sind sofort zu melden, „normale“ zeitnah, eher untergeordnete auch zusammengefasst zu einem späteren Zeitpunkt. Die Regelung per Verordnung ermöglicht eine flexible Handhabung.
- Einzelheiten zu den Sicherheitskonzepten: Den datenverarbeitenden Stellen können Vorgaben zu der Ausgestaltung ihrer Sicherheitskonzepte gemacht werden. Dabei kann z.B. im Kontext der IS-LL der Freien und Hansestadt Hamburg auf Einhaltung aktueller Standards nach BSI-Grundschutz verwiesen werden.

Die hier und in weiteren Verordnungsermächtigungen vorgesehene Beteiligung der ITKK sowie der Leitungen der Gerichte und Staatsanwaltschaften soll formlos erfolgen; angemessene Stellungnahmefristen sind zu gewährleisten. Soweit die ITKK noch nicht gebildet ist, gilt für Verordnungsermächtigungen der §9 Absatz 3.

Zu §5:

Die Vorschrift regelt in Ergänzung zu §3 Absatz 5 umfassend die „rechtliche Berechtigung“ im Hinblick auf die Schutzgüter des §3 und stellt damit eine weitere zentrale Norm des Gesetzes dar. Sie regelt alle weiteren Fälle der Berechtigung außerhalb des Bereiches der unmittelbaren Berechtigung. Ferner enthält sie Sondervorschriften zu Datenerhebungen im richterlichen Bereich und erlegt schließlich den datenverarbeitenden Stellen und der zuständigen Behörde Pflichten auf.

Zu Absatz 1:

Die Vorschrift stellt klar, dass nur (rechtlich) Berechtigte Daten im Sinne des §3 einsehen und in diese Daten oder in §3 geschützte Prozesse eingreifen dürfen, und das auch nur, soweit es zur Erfüllung ihrer jeweiligen Aufgabe erforderlich ist. Ferner wird hier das umfassende Schutzniveau der Daten des §3 Absatz 3 Satz 2 für den richterlichen Bereich durch die Anordnung gewährleistet, dass Einsichtnahmen und Eingriffe nur mit Zustimmung der unmittelbar berechtigten (§3 Absatz 5) Richterin bzw. des unmittelbar berechtigten Richters oder auf Grund zwingender technischer Erfordernisse gestattet sind. Eine Zustimmung kann auch impliziert werden, wenn eine berechtigte Person Daten und Dokumente (z.B. zwecks Zusammenarbeit) an andere Personen versendet oder diese in einem öffentlichen oder einem mit anderen ausgewählten Personen geteilten Zugriffsbereich bereitstellt. Zwingende technische Erfordernisse sind insbesondere dann gegeben, wenn ein Eingriff zur Aufrechterhaltung der Funktionsfähigkeit (hierzu gehören auch notwendige Maßnahmen im Bereich der IT-Sicherheit, wie z.B. die Prüfung auf Schadsoftware oder die Herstellung von Datensicherungen) unerlässlich ist. Dieser Kernbereich der richterlichen Unabhängigkeit ist damit jedem unbefugten Eingriff entzogen.

Zu Zwecken der Transparenz ist den betroffenen Richterinnen und Richtern die Möglichkeit zur Erlangung von Informationen über den Umgang mit ihren Daten und Dokumenten durch die von der Justizverwaltung für den jeweiligen Einsatzzweck bereitgestell-

ten IT-Systeme zu gewähren. Dabei ist zu berücksichtigen, dass die Anwendung technischer Maßnahmen von den im jeweiligen Fachbereich oder gegebenenfalls auch individuell eingesetzten IT-Systemen und der Art und Weise ihrer Nutzung durch den Betroffenen selbst abhängig sein kann. Vor diesem Hintergrund kann eine für den Betroffenen angemessene Information über den Umgang mit den Daten zum Beispiel im Rahmen der Anwenderschulung zu neu einzuführenden IT-Systemen oder über ähnliche gezielte Informationsangebote (z.B. zum Themenbereich IT-Sicherheit) erfolgen. Auf besondere technische Maßnahmen, die eine Vielzahl von Benutzern betreffen (wie zum Beispiel eine Datenmigration), kann zum Beispiel auch durch ein Rundschreiben o.ä. hingewiesen werden (entsprechend der bisherigen Praxis bei größeren Updates des Programmcodes gegebenenfalls auch im Vorwege der Maßnahme).

Bedingt durch das Gebot zur Datensparsamkeit und durch die Maßnahmen dieses Gesetzes wird es hingegen in der Regel weder in Einzelfällen noch in regelmäßig automatisiert ablaufenden Prozessen (z.B. Virenscans oder automatische Datensicherung) möglich sein, die einzelnen Daten und Dokumenten, auf die dabei immer auch zugegriffen wird, bestimmten Personen (z.B. deren Autorin oder Autor) zuzuordnen. Sollte die Zuordnung eines Dokuments zu einem bestimmten Betroffenen im Einzelfall zurückverfolgt werden müssen, so wäre diese höchstens durch eine (gegebenenfalls manuelle) Überprüfung des Dokumenteninhaltes oder ergänzender Metadaten möglich, was in Hinblick auf die Schutzziele dieses Gesetzes aber regelmäßig nicht vertretbar erscheint. Eine individuelle Information der oder des Betroffenen über in kurzen Zeitabständen kontinuierlich und hochgradig automatisiert ablaufende Prozesse, z.B. zur Virenprüfung oder zur Datensicherung, erscheint zudem aus Gründen der Häufigkeit und der Menge solcher (Standard-)Ereignisse unangebracht. Über besondere Einzelfälle technisch bedingter Eingriffe mit direkter Zuordnungsfähigkeit zu bestimmten Personen (wie etwa die Bitte an Administratorinnen und Administratoren, ein versehentlich gelöschtes Dokument wiederherzustellen oder die Sperrung einer lokalen Datei wegen Virenbefalls) ist die oder der Betroffene entweder bereits informiert, da sie oder er die Erlaubnis zum Eingriff selbst gegeben hat, oder es ist im Rahmen der durchzuführenden administrativen Tätigkeit zu informieren, sofern dies im Einzelfall mit vertretbarem Aufwand möglich ist.

Zu Absatz 2:

Hier werden – neben den unmittelbaren Berechtigungen (§ 3 Absatz 5) – weitere Berechtigungen geregelt.

Zu Satz 1 Nr. 1:

Die Einwilligung einer oder eines unmittelbar Berechtigten kann selbstverständlich nicht nach anderen Gesetzen (etwa den Datenschutzgesetzen oder strafrechtlichen Geheimhaltungsnormen) bestehende Beschränkungen aufzuheben. Dementsprechend kann die oder der unmittelbar Berechtigte nicht nach Gutdünken Dritten Zugriff auf Daten gewähren. Es sind indes durchaus zahlreiche Fälle denkbar, in welchen lediglich der Schutzbereich des HmbITJG betroffen und daher eine Einwilligung ausreichend ist. Beispielhaft genannt seien etwa die Weitergabe entscheidungsvorbereitender Literatur-/Rechtsprechungsrecherchen an Kolleginnen und Kollegen, die Weitergabe anonymisierter Voten, die Einwilligung in die statistische Auswertung anonymisierter Verfahrensdaten, die Einwilligung gegenüber einer Administratorin/einem Administrator zwecks Reparatur defekter Dateien oder die Einwilligung zur Einsichtnahme in Logdaten.

Zu Satz 1 Nr. 2:

Unter „gesetzliche Vorschriften fallen auch das Grundgesetz und die Verfassung der Freien und Hansestadt Hamburg (HVerf), aus denen sich Eingriffsbefugnisse und Zuständigkeiten ergeben können. Es existiert eine ganze Reihe gesetzlicher Vorschriften, die Zuständigkeiten begründen. Exemplarisch zu nennen sind etwa die zur Aufgabenerfüllung der Präsidien nach § 21e GVG notwendige Maßnahmen, aus dem GG abgeleitete allgemeine Veröffentlichungspflichten der Gerichtsverwaltungen, Maßnahmen zur Erfüllung der anerkannten, nicht kodifizierten Auskunftsansprüche der Presse [für Urteile etwa BGH, Beschluss vom 20. Juni 2018, NJW 2018, 3123 (3124 Rn 15)] oder dritter Personen, die Erfüllung des laut BGH (Beschluss vom 5. April 2017, NJW 2017, 1819 Rn 16) unmittelbar aus dem GG folgenden Anspruches auf Erteilung einer anonymisierten Urteilsabschrift, die Gewährung von Akteneinsicht nach §§ 299 Absatz 2 ZPO, 475 StPO oder die Erfordernisse der Dienstaufsicht (Beurteilungswesen, Verstöße gegen Dienstpflichten). Die besondere Hervorhebung der Dienstaufsicht dient lediglich der Klarstellung. Ebenfalls unter diese Vorschrift fällt die Auskunft im Zusammenhang mit dem sich unmittelbar aus Artikel 25 HVerf ergebenden parlamentarischen Fragerecht. Den Senat trifft insoweit eine dem Fragerecht korrespondierende Antwortpflicht, als andere Rechte und Verfassungsprinzipien einer Antwort nicht entgegenstehen. Auskunftspflichtig im Rahmen parlamentarischer Anfragen ist zwar allein der Senat und nicht die Gerichtsleitung oder der einzelne Spruchkörper. Die Gerichtsleitungen liefern jedoch im Zusammenhang mit der Beantwortung parlamentarischer Anfragen (also sowohl schriftliche kleine Anfragen als auch große An-

fragen) Informationen an die sie beteiligende Justizbehörde zu, die wiederum dem Senat zuliefert. Die Suche nach und/oder die Weitergabe von zu schützenden Daten und Prozessen i.S.v. §3 durch die Gerichtsleitungen steht daher in einem Spannungsverhältnis zur richterlichen Unabhängigkeit gem. Artikel 92 GG. Das landesverfassungsrechtlich verbriefte parlamentarische Fragerecht ordnet sich normhierarchisch der richterlichen Unabhängigkeit aus Artikel 92 GG unter, Artikel 31 GG. Eine Interessen- und Güterabwägung von Fragerecht und richterlicher Unabhängigkeit im Einzelfall ist daher ausgeschlossen. Die Zuständigkeit der Amtsträgerinnen und Amtsträger erstreckt sich insoweit nicht auf die Suche oder gar Herausgabe zu schützender Daten und Prozesse i.S.v. §3 Absatz 1 und 2, da lediglich Informationen zuzuliefern sind, die nicht geeignet sind, die Sphäre der richterlichen Unabhängigkeit zu verletzen.

Die für die Datenerhebung im richterlichen Bereich aus Absatz 3 sich ergebenden Beschränkungen sind zu beachten.

Ferner können Erfordernisse des technischen IT-Betriebes eine Berechtigung begründen (Nr. 3) – insoweit wird die technische Berechtigung der Administratoren durch die „rechtliche Berechtigung“ des §5 unterlegt.

Nr. 4, der eine Berechtigung im Rahmen des zwingenden Erfordernisses, eine unmittelbar bevorstehende Gefahr für die Schutzgüter des §1 Absatz 1 und des §3 abzuwehren, vorsieht, stellt eine eng auszulegende Ausnahmevorschrift dar; gedacht ist hier an nicht vorhersehbare Einzelfälle, in denen entweder technisch bedingt (wird in der Regel bereits durch Nr. 3 erfasst sein) oder vor allem durch unerlaubte Zugriffe eine Gefahrensituation bevorsteht.

Satz 2 regelt die Zulassung von Eingriffen durch die ITKK. Diese Kompetenz soll Fälle abdecken, in denen ein Eingriff, beispielsweise eine – auch wiederkehrende – Datenerhebung, aus wichtigen dienstlichen Gründen sinnvoll und zweckmäßig ist, aber keine Eingriffsgrundlage existiert. Im Sinne von Regelbeispielen werden Gründe für das Gebrauchmachen von der Vorschrift genannt. Da es aber auch der ITKK nicht grundsätzlich möglich sein darf, nach Belieben neue Eingriffsbefugnisse zu schaffen, ist diese Kompetenz in mehrfacher Hinsicht zu begrenzen: Zunächst sind Ermächtigungen durch die ITKK innerhalb des umfassend geschützten Bereiches des §3 Absatz 2 Satz 2 nicht gestattet. Ferner kann eine Bewilligung durch die ITKK höchstens für die Dauer ihrer Amtszeit – diese entspricht der regelmäßigen Amtszeit ihrer Mitglieder – gelten. Satz 3 bestimmt zudem, dass die Betroffenen hierüber nach Möglichkeit zu informieren sind – Ausnahmen gelten insbesondere dann, wenn die Zulassung erfolgt ist, weil unklar ist, welche Personen betroffen sind oder dies nur mit unverhältnismäßig großem Aufwand ermittelt werden kann.

Zu Absatz 3:

Absatz 3 regelt Besonderheiten der Datenerhebung im richterlichen Bereich. Es handelt sich um eine Sondervorschrift, die ihre Begründung in der umfassenden verfassungsrechtlichen Gewährleistung der richterlichen Unabhängigkeit hat. Für die Bereiche der Staatsanwaltschaft und der Rechtspfleger gewährleisten die Absätze 1 und 2 im Zusammenhang mit §3 Absatz 5 bereits einen weitreichenden Schutz.

Grundsätzlich ist mit Einwilligung der betroffenen Richterinnen und Richter jegliche Datenerhebung möglich. Die Vorschrift regelt Fälle, in denen eine ausdrückliche oder konkludente Einwilligung der Betroffenen nicht vorliegt.

Sie untersagt in Satz 1, dass für Statistik auf nicht aggregierte und/oder nicht anonymisierte Daten zurückgegriffen wird und beschränkt die insoweit zur Verfügung stehenden Daten ferner auf in Fachverfahren erstellte Verfahrensdaten. Fachverfahren sind dabei IT-Systeme, in welchen fachliche Daten zur Verwaltung des gerichtlichen oder staatsanwaltschaftlichen Verfahrens verarbeitet werden. Diese Einschränkung dient unmittelbar dem Schutz der richterlichen Unabhängigkeit vor unzulässiger Kontrolle. Satz 2 und 3 stellen sicher, dass die erste Übermittlung der Daten von den Gerichtsleitungen vorgenommen wird und kein direkter Zugriff aus der zuständigen Behörde erfolgt. Ein Großteil der Daten wird derzeit beim Statistikamt gesammelt, es existieren indes auch noch weitere damit befasste Stellen. Soweit weitere Stellen einbezogen werden, sind die strengen Vorgaben des §5 Absatz 2 des Hamburgischen Statistikgesetzes zu beachten; eine Weitergabe der von den Gerichtsleitungen an das Statistikamt übermittelten Daten durch das Statistikamt ist unter diesen Voraussetzungen zulässig.

Satz 5 gibt den Gerichtsleitungen als Teil der Justizverwaltung die Kompetenz, zu anderen, auch statistischen Zwecken Daten im Sinne des §3 Absatz 2 Nr. 1, 2 zu übermitteln oder bereits übermittelte Daten freizugeben. Dies ist aber nur unter engen Voraussetzungen möglich. Insbesondere ist aus Gründen des Schutzes der richterlichen Unabhängigkeit zu gewährleisten, dass aus diesen Daten kein Rückschluss auf die Tätigkeit einzelner Richterinnen und Richter gezogen wird und dass sie ferner generell nicht für Beobachtungs- und Kontrollzwecke verwendet werden; hier wird auch das Gebot des §1 Absatz 2 aufgegriffen. Das ist durch geeignete Maßnahmen in transparenter Weise sicherzustellen. Die Beschränkungen dürften sich bereits unmittelbar aus dem Grundsatz

der richterlichen Unabhängigkeit ergeben, sodass es sich insoweit nur noch um eine Konkretisierung bzw. Klarstellung handelt. Die Kompetenz erstreckt sich nur auf anonymisierte Daten, die, soweit das möglich ist, auch aggregiert sein müssen; eine Aggregierung wird lediglich dann im Einzelfall nicht möglich sein, wenn die Daten nur einen bestimmten Aufgabenbereich betreffen, der lediglich von einem bestimmten Spruchkörper/Amtsträger wahrgenommen wird.

Die Sätze 6–8 eröffnen aus Gründen der Praktikabilität weitere Möglichkeiten der Datenerhebung für die Arbeiten der Präsidien und Gerichtsleitungen.

Zu Absatz 4:

Die Vorschrift dient der besseren Kontrolle der datenverarbeitenden Stellen. Die Zugriffsberechtigungen der Administratorinnen und Administratoren sind durch Berechtigungskonzepte transparent zu machen.

Zu Absatz 5:

Die Vorschrift richtet sich an die datenverarbeitenden Stellen und an die zuständige Behörde. Gegenüber IT-Abteilungen der Gerichte und anderen Behörden(teilen) der Freien und Hansestadt Hamburg gilt das Gesetz unmittelbar. Da datenverarbeitende Stellen nicht zwingend ihren Sitz in Hamburg haben und auf sie möglicherweise hamburgisches Landesrecht nicht direkt anwendbar ist, muss die Einhaltung der Vorschriften des Gesetzes mitunter gesondert sichergestellt werden.

Für Dataport folgt das etwa daraus, dass gemäß §1 Absatz 2 S. 2 des Staatsvertrages für die Errichtung und den Betrieb von Dataport als Anstalt öffentlichen Rechts schleswig-holsteinisches Landesrecht gilt, soweit nichts anderes bestimmt ist.

Es ist indes ohne weiteres unbedenklich möglich und entspricht auch der generellen Handhabung bei Einschaltung von Dataport oder anderer externer Dienstleister, die Geltung der einzelnen spezifischen Anforderungen des Gesetzes für den Umgang mit Justizdaten einschließlich der Kontrolle durch die IT-Kontrollkommission, wie sie in diesem Gesetz vorgegeben sind, mit diesen Dienstleistern vertraglich zu vereinbaren. Dementsprechend wird hier geregelt, dass bei Einschaltung von Dritten, zu denen auch Dataport zu rechnen ist, beim Betrieb der IT die Einhaltung der Vorschriften des Gesetzes gegebenenfalls vertraglich sicherzustellen ist.

Gegebenenfalls – das heißt, soweit dieses Gesetz keine direkte Geltung hat und sich auch keine anderen Möglichkeiten der Sicherstellung ergeben – hat also die Sicherstellung vertraglich zu geschehen. Die zuständige Behörde – oder im Falle der Auftragserteilung direkt durch die Leitung eines Gerichts oder einer Staatsanwaltschaft diese – hat in solchen Fällen zwingend durch Einzel- und oder Rahmenverträge umfassend die Einhaltung der Vorschriften dieses Gesetzes zu gewährleisten bzw. (z.B. im Falle der Einschaltung von Subunternehmern) durch den Auftragnehmer gewährleisten zu lassen. Wie genau eine solche vertragliche Regelung aussehen müsste und ob sie gegebenenfalls als Rahmenvertrag ausgestaltet werden könnte, der auch bereits bestehende Verträge abändert, gibt das Gesetz nicht vor. Entscheidend ist insoweit, dass auf dem Wege der vertraglichen Vereinbarung eine Regelungsdichte und ein Kontrollniveau sichergestellt werden, wie es durch dieses Gesetz vorgesehen ist.

Zu Absatz 6:

Der Absatz enthält eine Verordnungsermächtigung für den Senat, die auf die zuständige Behörde subdelegiert werden kann. In der Verordnung können Einzelheiten der nach Absatz 4 zu erstellenden Konzepte geregelt werden. Eine solche Regelung empfiehlt sich vermutlich erst, nachdem die ITKK eine gewisse Zeit Erfahrungen gesammelt hat und Vorschläge machen kann.

Zu §6:

Die Vorschrift regelt Einrichtung, Zusammensetzung und Arbeitsweise der ITKK.

Zu Absatz 1:

Die Einrichtung der ITKK bei der zuständigen Behörde ist lediglich als organisatorische Anbindung zu verstehen und beschränkt die Unabhängigkeit der ITKK und ihrer Mitglieder nicht. Mit dieser Anbindung im Zusammenhang steht die Verpflichtung der zuständigen Behörde, der ITKK die nötigen Arbeitsmittel – z.B. Raum, IT, allgemeine Arbeitsmittel, finanzielle Ressourcen – zur Verfügung zu stellen und ihr zudem eine Koordinierungsstelle einzurichten. Diese Stelle soll einerseits organisatorische Aufgaben wahrnehmen und insoweit wie eine Geschäftsstelle tätig sein. Die Verwendung des Begriffes „Koordinierungsstelle“ soll aber klarstellen, dass die Arbeit dieser Stelle in Abstimmung mit der ITKK über rein verwaltende Tätigkeiten hinaus sich auch auf inhaltliche Aufgaben, etwa die Beratung in IT-Fachfragen, den Kontakt zu den datenverarbeitenden Stellen sowie die Einholung, Auswertung oder Aufbereitung von Auskünften, Protokoll- oder Ereignisdaten, erstrecken kann. Die Ausgestaltung und Personalausstattung der Stelle im Einzelnen obliegt der zuständigen Behörde.

Zu Absatz 2:

Hier werden die Zusammensetzung der ITKK und die Wahl bzw. Bestimmung der Mitglieder festgelegt.

Da es bei der Einrichtung des Gremiums in erster Linie um die Gewährleistung der richterlichen Unabhängigkeit beim Einsatz elektronischer Arbeitsmittel geht, ist es folgerichtig, dass die Mehrheit der stimmberechtigten Mitglieder aus Richterinnen und Richtern besteht. Ein Verstoß gegen den Grundsatz der Gewaltenteilung ist nicht zu besorgen. Mit der Dreiteilung in Legislative, Exekutive und Judikative ist die Differenziertheit staatlicher Funktionen kaum zu erfassen, die Verfassung kennt insoweit viele Vermischungen. Ein Verstoß gegen den Gewaltenteilungsgrundsatz kann daher nur angenommen werden, wenn der Kernbereich einer Gewalt verletzt wird (Sachs, in: Sachs, GG, 6. Aufl., 2011, Artikel 20 Rn. 83, 85, 93). Dies ist vorliegend nicht der Fall. Weder wird durch die Beteiligung von Richterinnen und Richtern an der nach dem Staatsvertrag grundsätzlich der Exekutive obliegenden Kontrolle der Datenverarbeitung der Kernbereich der Exekutive verletzt, noch wird durch die Einsicht von Exekutivvertreterinnen und -vertretern in richterliche Daten und Dokumente im Rahmen der ITKK der Kernbereich der Judikative verletzt. Vielmehr ist die Konstruktion der ITKK als Mischgremium dem Kontrollgegenstand geschuldet, der funktional die Beteiligung der Exekutive und der Judikative erfordert.

Die Wahl der stimmberechtigten Mitglieder erfolgt durch die in der Vorschrift bezeichneten Räte. Dass zunächst diese Mitglieder durch Wahl bestimmt werden, geschieht mit Blick auf die in der Allgemeinen Begründung bereits dargestellten Gerichtsentscheidungen und auf allgemeine verfassungsrechtliche Erwägungen:

Der Dienstgerichtshof Frankfurt hält es zur Sicherung der richterlichen Unabhängigkeit im vorliegenden Zusammenhang für erforderlich, dass die Einhaltung der von ihm im Einzelnen benannten Regelungen zum Umgang mit richterlichen Dokumenten durch eine Kommission „unter gleichberechtigter Mitwirkung von gewählten Vertretern der Richterschaft“ überwacht wird (DGH Frankfurt, Urteil vom 20. April 2010, BeckRS 2010, 14555, S. 18). Eine inhaltliche Begründung für die Erforderlichkeit einer Wahl der richterlichen Vertreterinnen und Vertreter findet sich in der genannten Entscheidung nicht. Das Bundesverfassungsgericht hat in seinem nachfolgenden Beschluss vom 17. Januar 2013 auch lediglich ausgeführt, dass nichts dafür spreche, das die „unter Beteiligung von Vertretern der Richterschaft ausgeübte Kontrolle“ nicht hinreichend sein könnte, um die Befolgung der Vorschriften zum Umgang mit richterlichen Dokumenten sicherzustellen [BVerfG, NJW 2013, 2102 (2103)].

Auch wenn es danach vertretbar erscheinen mag, verfassungsrechtlich nur die Vertretung der Statusgruppe der Richterinnen und Richter in der ITKK und nicht auch die Wahl der Vertreterinnen und Vertreter für geboten zu halten, erscheint es jedenfalls zur Verfolgung des „sichersten Weges“ vorzugswürdig, gesetzlich sicherzustellen, dass die Vertreterinnen und Vertreter der Justiz in der Kommission auch gewählt sind.

Die Wahl erfolgt aus Gründen der Praktikabilität durch die Richter- und Personalräte. Um den Kreis der kompetenten Kandidatinnen und Kandidaten für eine Mitwirkung in der ITKK zu vergrößern, können auch Justizangehörige, die selbst nicht Mitglied des jeweiligen Richter- bzw. Personalrates sind, zu Mitgliedern der ITKK gewählt werden.

Da die richterlichen Mitglieder der ITKK nach den obigen Ausführungen gewählt sein müssen, wäre für solche „normalen“ Richterinnen und Richter ein eigenes Wahlverfahren zu schaffen. Die in §5 Absatz 2 des IT-Gesetzes für die Justiz des Landes Schleswig-Holstein vorgesehene Benennung der Kommissionsmitglieder aus dem Kreis (aller) Angehörigen der Gerichte und Staatsanwaltschaften durch die Mitbestimmungsgremien dürfte demgegenüber das Kriterium einer „Wahl“ nicht erfüllen.

Eine Urwahl der Mitglieder der ITKK durch alle Richterinnen und Richter der Hamburger Justiz kommt wegen des damit verbundenen erheblichen Aufwandes nicht in Betracht.

Eine Wahl durch den jeweiligen Richter- bzw. Personalrat ist verfassungsrechtlich zulässig. Zwar sind die Richter- und Personalräte grundsätzlich keine Gremien, zu deren Aufgaben die Wahl von Dritten für bestimmte Ämter gehört; insoweit könnte jedenfalls bei der ersten Wahl der IT-Kommissionsmitglieder das Problem bestehen, dass der wählende Richterrat seinerseits nicht von der Gesamtrichterschaft für die Wahl der Kommissionmitglieder legitimiert wurde. Dem Hamburgischen Richtergesetz ist aber die Legitimation Dritter durch den Richterrat nicht gänzlich fremd, wie die Benennung von Mitgliedern der Schlichtungsstelle gemäß §50 Absatz 2 HmbRiG durch den Richterrat zeigt. Auch geht es bei der hier in Rede stehenden Wahl um die Sicherung der Stellung eines von der Exekutive unabhängigen Vertreters einer Statusgruppe und nicht um eine persönliche Legitimation. Der Gesetzgeber ist daher nicht gehindert, dem Richter- bzw. Personalrat als Vertretungsgremium der jeweiligen Statusgruppen als zusätzliche Aufgabe die Wahl der Vertreterinnen und Vertreter in der ITKK zuzuweisen. Hierdurch und nicht durch die eigene Wahl wird der Richter- bzw. Personalrat zur Wahl der Kommissionsmitglieder legitimiert. Aus diesem Grunde kommt es auch nicht darauf an, ob der Richter- bzw. Personalrat zum Zeitpunkt seiner eigenen Wahl schon die Aufgabe der Wahl der Kommissionsmitglieder hatte oder nicht.

Das Wahlverfahren muss in seinen wesentlichen Zügen gesetzlich geregelt werden, um einen zu großen Einfluss des Verordnungsgebers auf die Auswahl der richterlichen Vertreter in der ITKK zu vermeiden. Die formalen Fragen der Beschlussfassung sind bereits in § 46 HmbRiG und § 39 HmbPersVG normiert (z.B. jeweils in Absatz 2 der genannten Normen die Beschlussfassung durch die Mehrheit der Anwesenden). Verbleibende Fragen können auf der Grundlage des Absatzes 7 durch Rechtsverordnung geregelt werden.

Soweit das Gesetz anordnet, dass die Räte die Mitglieder gemeinsam wählen, bezeichnet „gemeinsam“ das Wahlgremium, nicht die zu Wählenden: Die zuständigen Räte wählen zusammen die einzelnen Mitglieder der ITKK.

Die Regelungen zur Amtszeit stellen einerseits durch die Festlegung auf drei Jahre ein Gleichgewicht zwischen Arbeitsfähigkeit und Legitimation des Gremiums her und sichern andererseits durch die Bestimmung, dass Nachwahlen immer nur für den Rest der Amtszeit erfolgen, den Gleichlauf der Amtszeiten.

Zu Absatz 3:

Die Vorschrift dient dazu, dass der Sachverstand der Leitungen der Gerichte und Staatsanwaltschaften bei Bedarf nutzbar gemacht werden kann. Die Vorschrift ist als Minderheitsrecht ausgestaltet.

Vertreterin oder Vertreter der Leitung muss nicht zwingend ein Mitglied der Leitung selbst sein; die Leitungen der Gerichte und Staatsanwaltschaften können im Einzelfall oder generell geeignete Vertreterinnen oder Vertreter für diese Zwecke bestimmen.

Zu Absatz 4:

Die Vorschrift regelt einerseits die Beschlussfassung und vermeidet damit das Auftreten etwaiger Zweifelsfragen im Zusammenhang mit Stimmenthaltungen. Gleichzeitig verpflichtet sie die ITKK, die Einzelheiten ihrer Arbeitsweise durch eine Geschäftsordnung zu regeln; diese Verpflichtung dient der Sicherstellung effizienter Arbeit.

Überdies wird es der ITKK ermöglicht, einzelne Aufgaben oder Befugnisse generell oder im Einzelfall durch – grundsätzlich jederzeit widerrufbaren – Beschluss auf einzelne Mitglieder oder auch mehrere einzelne Mitglieder zu übertragen. Auch dies dient der Verbesserung der Arbeitsfähigkeit. Näheres kann und sollte in der Geschäftsordnung geregelt werden.

Zu Absatz 5:

Da die Arbeit der ITKK hochsensible Bereiche betrifft, sind Regelungen zur Vertraulichkeit ihrer Beratungen und zur Verschwiegenheit der Mitglieder unabdingbar.

Beratungen müssen grundsätzlich vertraulich sein, ihr Inhalt darf nicht nach außen getragen werden. Dies ist ein wesentlicher Baustein der Gewährleistung der Unabhängigkeit der Kommission. Allerdings muss es der ITKK möglich sein, zur Erhaltung der Arbeitsfähigkeit davon punktuell bis zu einem gewissen Grade abweichen zu können. Beratung und Austausch mit Dritten im dienstlichen Kontext kann sinnvoll und unbedenklich sein. Auch die Koordinierungsstelle wird sinnvollerweise in größerem Umfang in die Arbeit der ITKK einbezogen werden müssen. Aus diesem Grunde wird dieser die Möglichkeit eingeräumt, in der Geschäftsordnung Einzelheiten – d.h. Umfang und punktuelle Ausnahmen – zu regeln. Ausnahmen müssen indes auf das zur Gewährleistung der Arbeitsfähigkeit unbedingt Erforderliche beschränkt bleiben – etwa die Mitteilung des Gegenstandes einer Beratung an eine datenverarbeitende Stelle, die Koordinierungsstelle oder eine Gerichtsleitung, soweit dies zur effektiven Sachaufklärung nötig ist.

Außerhalb des Beratungsgeheimnisses sind die Mitglieder – vorbehaltlich ihrer Aufgabenerfüllung nach den in Satz 3 genannten Vorschriften – zur Verschwiegenheit verpflichtet, soweit das zum Schutz der Rechte Einzelner, zum Schutz von Geschäftsgeheimnissen oder zur Gewährleistung der IT-Sicherheit nötig ist. Der Begriff der IT-Sicherheit ist weit zu verstehen; er beinhaltet die Gewährleistung aller in Bezug auf Daten und IT-Systeme zu schützenden Grundwerte (Vertraulichkeit, Integrität, Verfügbarkeit bzw. Funktionsfähigkeit, Authentizität, Revisionsfähigkeit).

Die Verschwiegenheitsverpflichtung umfasst insbesondere auch für die der ITKK überlassenen Verträge und Konzepte (z.B. Sicherheits- oder Berechtigungskonzepte), die Informationen über Inhaberinnen und Inhaber administrativer Zugänge und ähnliche Daten und Dokumente; ebenso ist eine (auch auszugsweise) Weitergabe solcher interner Daten und Dokumente an unbeteiligte Dritte untersagt.

Zu Absatz 6:

Die Mitglieder der ITKK sind grundsätzlich entweder (teilweise) von ihrer dienstlichen Tätigkeit freizustellen oder angemessen – und nach § 3 Nr. 12 EStG steuerbefreit – für ihren Aufwand zu entschädigen. Die Entscheidung darüber, welche Mitglieder in welchem Umfang freigestellt werden, trifft die zuständige Behörde. Sie hat dabei aber die Gewährleistung der Arbeitsfähigkeit der ITKK sicherzustellen. Angesichts der vielfältigen und umfangreichen Aufgaben der Kommission wird eine teilweise Freistellung mehrerer Mitglieder erforderlich sein.

Die Freistellungsmöglichkeit gilt nicht für die Vertreterinnen beziehungsweise Vertreter der Gerichtsleitungen in der ITKK. Auch für sie ist aber eine angemessene Aufwandsentschädigung vorzusehen.

Zu Absatz 7:

Der Absatz enthält eine Verordnungsermächtigung für den Senat, die auf die zuständige Behörde subdelegiert werden kann. Die potentiell zu regelnden Materien sollten mit Blick auf die nötige Flexibilität im Verordnungswege erfolgen. Geregelt werden können Einzelheiten zu folgenden Fragen:

– Wahl und Amtszeit der stimmberechtigten Mitglieder: Hier kann etwa geregelt werden, dass die Mitglieder der ITKK nach Ende ihrer Amtszeit im Amt bleiben, bis neue Mitglieder gewählt sind. Ferner können Regelungen zum Umgang mit fehlerbehafteten Wahlen, zu Elternzeiten, Mutterschutz etc. getroffen werden.
– Bestimmung der beratenden Mitglieder: Während die Vertreterinnen und Vertreter der zuständigen Behörde von deren Präses ernannt werden, sodass insoweit kein Regelungsbedarf besteht, erscheint es sinnvoll, ein Verfahren zur Bestimmung der Vertreterinnen und Vertreter der Gerichtsleitungen zu etablieren, weil insoweit lediglich zwei Personen sämtliche hamburgischen Gerichte repräsentieren.
– Beschlussfassung der ITKK: Geregelt werden könnten etwa Ladungsfristen vor Beschlüssen, die Möglichkeit der Beschlussfassung im Umlaufverfahren o. ä. Rechtlich möglich wäre es aber auch, diese Regelungen der Geschäftsordnung zu überlassen.
– Freistellung und Aufwandsentschädigung: Eine Regelung per Gesetz oder Verordnung ist erforderlich. Aus Gründen der schnelleren Anpassbarkeit ist der Verordnung auch insoweit der Vorzug zu geben.

Zu § 7:

Die Norm regelt im Einzelnen die Rechte und Pflichten der ITKK.

Zu Absatz 1:

Konstituiert wird zunächst ein umfassendes Einsichtsrecht der ITKK hinsichtlich aller Datenverarbeitungsvorgänge (bzw. auch Teile derselben) und der zu erstellenden Konzepte, auch unabhängig von konkreten Anlässen. Dieses Recht ist zur Wahrnehmung ihrer Aufgaben unerlässlich und gilt grundsätzlich unbeschränkt. Inhaltliche Beschränkungen ergeben sich lediglich im Hinblick auf die Inhaltsdaten (§ 3 Absatz 2 Nummer 1) sowie vor allem auf die umfassend geschützten Dokumente nach § 3 Absatz 3 Satz 2, bei denen ein Erforderlichkeitsvorbehalt konstituiert wird. Erforderlich im Sinne der Vorschrift können aber zum Beispiel auch verdachtsunabhängige Routinekontrollen sein. Die Gewährung dieser umfangreichen und generell nicht bzw. wenig beschränkten Einsichtsrechte schließt allerdings nicht aus, dass besonders schutzwürdige Daten (etwa die Identität verdeckter Ermittlerinnen oder Ermittler betreffend, oder, soweit es um Verträge geht, gegebenenfalls Preise) geschwärzt werden können; der Fokus der Arbeit der ITKK liegt in der inhaltlichen Kontrolle, diese wird durch solche Schwärzungen nicht beeinträchtigt. Die Rechte der ITKK richten sich in aller Regel an die jeweils zuständige Stelle; nur in Ausnahmefällen – etwa dann, wenn gerade gegen Mitarbeiterinnen oder Mitarbeiter derselben ein aufzuklärender Verdacht besteht – kann die ITKK ihre Rechte auch auf anderem Wege zu verwirklichen suchen.

Damit Einsichtnahmen sinnvoll vorgenommen werden können, muss es der ITKK auch möglich sein, vorbereitend oder begleitend Auskünfte und Erläuterungen von den datenverarbeitenden Stellen einzuholen. Diese Kompetenz erstreckt sich indes nur auf einfache, schnell zu erteilende Auskünfte. Komplexere Fragestellungen, die die ITKK nicht mit eigenem Sachverstand klären kann, sind nach Absatz 3 zu handhaben.

Geregelt ist ferner in Satz 5 ein Minderheitsrecht, insoweit allerdings nur für die stimmberechtigten Mitglieder.

Zu Absatz 2:

Die Vorschrift erstreckt die Einsichtsrechte der ITKK auch auf die Ergebnisse der von den datenverarbeitenden Stellen nach § 4 Absatz 4 vorzunehmenden Überprüfungen.

Zu Absatz 3:

Die ITKK dürfte, gegebenenfalls nach einer gewissen Einarbeitungszeit, bereits selber oder bei entsprechender personeller Ausgestaltung auch mit Hilfe ihrer Koordinierungsstelle nach § 6 Absatz 1 Satz 2 die nötige Sachkunde entwickeln, eine Vielzahl der zu prüfenden Vorgänge zu beurteilen. Sofern eine Problemstellung im Einzelfall mit der fachlichen Kompetenz der ITKK allein nicht lösbar oder überblickbar ist, ist zunächst der Rat fachkundiger Personen aus den IT-Stellen der Gerichte und Staatsanwaltschaften oder der zuständigen Behörde heranzuziehen; bei entsprechenden Fragestellungen ist auch die Befassung der gerichtlichen oder behördlichen Datenschutzbeauftragten, der oder des Hamburger Beauftragten für Datenschutz und Informationsfreiheit, der oder des Gesamtverantwortlichen für Informationssicherheit (CISO) oder ähnlicher zentraler Institutio-

nen der Freien und Hansestadt Hamburg in Betracht zu ziehen. Nur dann, wenn diese Maßnahmen nicht zum Erfolg führen oder im Einzelfall wegen etwaiger Besonderheiten untunlich sind – etwa dann, wenn unklar ist, ob eine Gefährdung der Schutzgüter möglicherweise auch von Mitarbeitern der Behörde oder der Gerichtsverwaltung ausgeht –, kommt die Einbeziehung einer oder eines externen Sachverständigen zu technischen Fragestellungen in Betracht.

Die Heranziehung hat durch die Behörde unter Beachtung des Vergaberechts zu erfolgen; die Behörde prüft dabei auch die Erforderlichkeit. Die ITKK ist einzubeziehen. Die konkrete Auswahl der oder des Sachverständigen wird – im Rahmen der vergaberechtlichen Vorschriften – in aller Regel den Wünschen der ITKK entsprechend vorgenommen werden müssen.

Entstehende Kosten trägt die zuständige Behörde. Sie kann aber, sofern die Voraussetzungen vorliegen, Regress nehmen. Dies wird in der Regel nur dann möglich sein, wenn der Einholung des Gutachtens Fehlleistungen eines von der Behörde beauftragten externen Datenverarbeiters zugrunde liegen, die Vertragspflichtverletzungen darstellen. In Ausnahmefällen ist bei grober Fahrlässigkeit oder Vorsatz seitens einzelner Mitarbeiterinnen oder Mitarbeiter auch ein Rückgriff nach beamten- oder arbeitsrechtlichen Vorschriften nicht ausgeschlossen. Das wird indes in der Praxis kaum jemals relevant werden. Noch seltener dürfte ein – grundsätzlich ebenfalls eröffneter – Rückgriff wegen grob fahrlässiger oder vorsätzlicher Pflichtverletzungen der ITKK-Mitglieder vorkommen, zumal bei der Entscheidung eines Gremiums der Vorwurf grober Fahrlässigkeit nur äußerst schwer unterlegbar ist.

Zu Absatz 4:

Die Vorschrift regelt Unterrichtungspflichten und -rechte der ITKK bei der Feststellung von Verstößen sowie ferner weitere Rechte.

Betroffene Dienststelle im Sinne des Satzes 1 bezeichnet hier die Dienststelle im herkömmlichen Sinne, also die Leitung des betroffenen Gerichtes oder der betroffenen Staatsanwaltschaft. IT-Dienstleister im Sinne der Vorschrift können auch Stellen der Gerichte sein, die Aufgaben der IT wahrnehmen, sei es datenverarbeitender oder auch nur rein vorbereitender oder begleitender Natur (etwa Auf- und Abbau von Computern).

Die Entscheidung darüber, ob auch etwa betroffene Mitarbeiterinnen und Mitarbeiter unterrichtet werden, trifft die ITKK. Sie wird dabei die Rechte der Einzelnen und etwaige Sicherheitsinteressen abzuwägen haben.

Im Übrigen ist in Satz 2 bis 4 das weitere Verfahren geregelt. Der ITKK werden keine exekutiven Befugnisse verliehen. Die zuständige Behörde ist aber zu einer angemessenen Reaktion auf Beanstandungen verpflichtet. Das Spektrum angemessener Reaktionen umfasst eine Vielzahl denkbarer Maßnahmen, etwa die Geltendmachung vertraglicher Ansprüche gegenüber externen Datenverarbeitern bis hin zur Kündigung, die Einleitung strafrechtlicher oder gegebenenfalls dienstaufsichtsrechtlicher Verfahren, Abmahnungen etc.

Zu Absatz 5:

Die Vorschrift begründet das Recht für Betroffene, Räte und Dienststellenleitungen, sich mit konkreten Anliegen an die ITKK zu wenden. Die Gewährung dieses Rechts dient nicht nur den Interessen der Berechtigten, sondern auch der Effektivität der Arbeit der ITKK: Aufsichts- und Kontrollinstanzen gewinnen in der Regel einen nennenswerten Teil ihrer relevanten Erkenntnisse aus Meldungen Dritter.

Gleichzeitig wird im Umkehrschluss klargestellt, dass die ITKK nicht zum Schutz justizfremder Dritter tätig wird.

Zu Absatz 6:

Durch die Vorschrift wird klargestellt, dass die IT-Kontrollkommission zum Schutz personenbezogener Daten im nicht justitiellen Bereich nicht tätig wird. Die Vorschrift dient der Abgrenzung der Kompetenzen und Befugnisse der IT-Kontrollkommission gegenüber denen der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit gem. Artikel 57, 58 DSGVO [VO (EU) 2016/679] im nicht justitiellen Bereich der Gerichte. Die Kontrolle und Einhaltung aller datenschutzrechtlichen Anforderungen bezüglich der Verarbeitung personenbezogener Daten im Bereich der nicht justitiellen Tätigkeit obliegt allein der oder dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit als zuständiger Aufsichtsbehörde. Da die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit gemäß Artikel 55 Absatz 3 VO (EU) 2016/679 keine Zuständigkeit für die Aufsicht von Gerichten im justitiellen Bereich hat, bestehen diesbezüglich keine möglichen Kompetenzkonflikte. Im justitiellen Bereich übt die ITKK ihre Kontrollrechte gem. §7 ohne Einschränkungen aus.

Zu §8:

Die in §8 geregelte Berichtspflicht verstärkt die Möglichkeiten der ITKK, auf Missstände hinzuweisen und deren Behebung herbeizuführen. Der nach Absatz 2 für zahlreiche Adressaten zugängliche Bericht wird, soweit er berechtigte Bedenken enthält, nicht ignoriert werden können.

Zu § 9:

Die Norm regelt das Verhältnis zu anderen Vorschriften sowie eine Evaluationsverpflichtung. Ferner werden Übergangsregelungen getroffen.

Zu Absatz 1:

Die Vorschrift regelt das Verhältnis zu anderen Vorschriften.

Zu Absatz 2:

Die Evaluationsverpflichtung trifft den Senat. Die Überprüfung hat spätestens vier Jahre nach dem Inkrafttreten zu beginnen, der Senat kann sie aber, wenn ihm das tunlich erscheint, auch früher einleiten.

Zu Absatz 3:

Geregelt wird zunächst das Verfahren bei Erlass oder Änderung von Verordnungen nach den Absätzen 7 der §§ 4, 5 und 6, solange eine ITKK noch nicht gebildet ist. In diesem Fall sind statt der ITKK die Richter- und Personalräte zu beteiligen. Diese Beteiligung beim Erlass einer Verordnung soll formlos erfolgen; angemessene Stellungnahmefristen sind zu gewährleisten.

Ferner wird den Richter- und Personalräten für den Zeitraum vor Bildung einer ITKK für ihren jeweiligen Bereich das Recht zur Zulassung von Eingriffen nach § 5 Absatz 2 Satz 2 eingeräumt.

Zu Absatz 4:

Die Vorschrift trägt dem Umstand Rechnung, dass möglicherweise noch betriebliche Prozesse zur Anwendung kommen oder sonstige technisch-organisatorische Rahmenbedingungen gegeben sind, die es nicht erlauben, alle Vorgaben des Gesetzes sofort umzusetzen.

Anlage

Stellenveränderungen zum Stellenplan 2020

Lfd. Nr.	Aufgaben-bereich	Anzahl	Stellenveränderung	Erläuterung
			Stellenneuschaffungen	
1	233	1,5	R 1 Richterin/ Richter	
2	233	1,0	A 13 Regierungsrätin / Regierungsrat	

Gestaltung und Layout: Lütcke & Wulff, Rondenbarg 8, 22525 Hamburg, Tel. (040) 23 51 29-0