Den Mitgliedern des
AfMJV

Stellungnahme zum ThürIKTGerStG

Sehr geehrte Damen und Herren, liebe Kls.

Wieder einmal möchten wir uns für diese für uns sehr informative und lehrreiche Möglichkeit einer Stellungnahme im Bereich der staatlichen Digitalisierung bedanken. Bislang war uns die Thüringer Judikative nur in Form von ebenfalls sehr lehrreichen und gut geschriebenen Texten zu unseren Widersprüchen zu Allgemeinverordnungen oder Transparenzklagen bekannt. Das wir aber in der 3. Staatlichen Gewalt einen so großen und gut motivierten Mitstreiter für echte Transparenz, IT-Sicherheit und Datenschutz haben, war uns bislang entgangen. **Wir begrüßen dies außerordentlich!**

Wir können die **Bedenken** der 3. Staatlichen Gewalt **absolut nachvollziehen**. Digitalisierung darf nicht zu einer „Hintertür" verkommen mit der Demokratie und Rechtsstaat ausgehebelt werden können. Das sich Demokratie und Rechtsstaat derzeit nicht in der einfachsten (welt-)politischen Lage befindet dürfte niemand ernsthaft bestreiten wollen. Nutzen wir die Digitalisierung also lieber um die Demokratie, den Rechtsstaat und damit auch die absolute Unabhängigkeit der 3. Staatlichen Gewalt sicherzustellen, gleichzeitig aber auch und die Transparenz und rechtsstaatliche Kontrolle der 3. Staatlichen Gewalt sicherstellen zu können.

Wir können die Bedenken der 3. Staatlichen Gewalt auch deshalb so gut nachvollziehen, da wir auch selbst Probleme mit der technischen Qualität und der eigentlich absolut notwendigen und eigentlich gesetzlich geregelten Transparenz des Freistaates Thüringen als IT-Dienstleister haben. In unseren „Ausschreibungen" wäre dieser Dienstleister sicherlich bei jedem Thema, außer vielleicht bei den Gebäuden von Rechenzentren, schon in der Qualifikationsrunde ausgeschieden. Von der ministerialen Ebene bis hin zur *Kommunale Informationsverarbeitung Thüringen GmbH (KIV)* wird unserer Ansicht nach absichtlich gegen das Thüringer Transparenzgesetz (ThürTG) verstoßen in dem schlicht nicht oder ausweichend geantwortet wird; indem veraltete oder für die Fragen komplett irrelevante Informationen rausgegeben werden; indem Dokumente und ganze Veranstaltungen als *„verwaltungsintern"* deklariert werden; indem das ThürTG und seine Anwendbarkeit ganz verleugnet wird. Beispiele hierfür finden sich auf Frag-den-Staat zur Genüge. Leider helfen hier auch Klagen vor den Verwaltungsgerichten nur bedingt, wie unsere Klagen zu verwandten Themen zeigen. **Warum sollte jemand der digitalaffine BürgerInnen dermaßen abschätzig behandelt die 3. Staatliche Gewalt und deren IT-Kontrollkommission besser behandeln?** Zumal das Risiko das hierbei fachfremde Kommissionsmitglieder mit wohlklingenden IT-Buzzwords einfach „an die Wand gequatscht" werden deutlich höher ist?

Auf Grund dieser Weigerung bei vielen transparenzpflichtigen Stellen Auskunft über die KIVs bzw. über ihre Zusammenarbeit mit der KIVs zu geben, empfehlen wir einen Untersuchungsausschuss im Landtag über die Machenschaften und die Rolle des Landes-CIOs, des Landesverwaltungsamtes und der KIVs in dieser Hinsicht. Wir sehen hier einen Anfangsverdacht der Vorteilsnahme und Vorteilsgewährung als erfüllt an.

Bevor sich die 3. Staatliche Gewalt also in weitreichende IT-Abhängigkeiten begeben bei denen die Unabhängigkeit der 3. Gewalt einer konkreten Gefahr ausgesetzt sein wird, empfehlen wir den Bereich „IT-Dienstleistungen" der Freistaates Thüringen grundlegend zu reformieren und überalterte Strukturen abzuschaffen bzw. in Pension zu schicken. Die 3. Staatliche Gewalt braucht einen IT-Dienstleister bei dem **IT-Sicherheit-*by-Default***, **Datenschutz-*by-Default***, **Transparenz-*by-Default***, **Open Source-*by-Default***, **OpenData-*by-Default*** als Grundlage jedes Prozesses gelebt wird. Ansonsten empfehlen wir Brieftauben (vgl. RFC 1149).

Als Alternativvorschlag möchten wir – wie schon häufiger – nochmals für ein eigenes **Ministerium für Transparenz und Digitale Schnittstellen (TMTDS)** werben. Wir sind uns sicher, dass die Verortung der Digitalisierung verteilt auf viele Ministerien und die staatliche Verwaltungsdigitalisierung unterhalb des Finanzministeriums einer der Geburtsfehler der Thüringer Digitalisierung darstellt. Zu groß sind die Interessenkonflikte und zu groß die Sicherheitsrisiken bei der Gewährleistung einer effektiven staatlichen Gewaltenteilung. Dies Ministerium sollte ebenfalls unabhängig von allen anderen staatlichen Institutionen sein und sich bewusst als echter reiner Dienstleister verstehen, der die Zusammenarbeit zwischen allen staatlichen Institutionen aktiv fördert, aber auch ein Vetorecht bei abstrusen Alleingängen einzelner Institutionen hat. Die Stelle des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) wäre innerhalb eines eigenen Ministeriums sicherlich ebenfalls besser aufgehoben und könnte effektivere Arbeit leisten als heutzutage.

So positiv wie wir die grundlegende Intention der 3. Staatlichen Gewalt zu dieser Gesetzesinitiative sehen, so sehr wundert uns doch der Inhalt des Gesetzes. Ein wenig wirkt es so, als ob man in der 3. Gewalt, wenn man nicht mehr weiter weiß einen Arbeitskreis für eine gesetzliche Regelung schafft – ähnlich wie in der IT-Branche gern mal ein „Standard" produziert wird, wenn man Zeit gewinnen will. Ob dies auch zielführend ist, scheint dann niemand mehr in Frage stellen bzw. überprüfen zu wollen. Eher schreibt man bei Bedarf einfach noch einen Standard bzw. einfach noch ein Gesetz. Dabei hat die 3. Staatliche Gewalt doch mit der gesetzlichen Festlegung von DE-Mail als „sichere" Kommunikation zwischen BürgerInnen und u.a. der Judikative bereits vor längerer Zeit bewiesen, dass solche Wege zum Scheitern verurteilt sind.

Unsere Kritik aus dem vorherigen Absatz verstärkt sich durch die vielen offensichtlich absichtlich sehr schwachen Forderungen im Gesetz und der Gesetzesbegründung. Laut Volksmund muss man ja jedes Wort der Judikativen auf die Goldwaage legen, da wundert es dann um so mehr, wenn die Judikative mit einem eigenen Spezialgesetz ihre Unabhängigkeit einfordern will, sich dann aber bei Forderungen die nach Sicherheitsgarantien auf dem Niveau von „Wünschen", vertraglichen Regelungen und „Checklistensicherheit" (Compliance) beschränkt, obwohl an den meisten dieser Stellen auch eine mathematisch und informatisch beweisbare technische und organisatorische Sicherheit hätte gefordert werden können. So ist es beispielsweise vollkommen nebensächlich, ob ein Mitarbeiter des Landes-IT-Dienstleisters auf irgendwelche Daten und Dokumente **"nicht zugreifen darf"**, denn als **interner Angreifer** wird ihn dieses Verbot schlicht nicht interessieren. Eine juristisch, mathematisch und informatisch korrekte Formulierung muss deshalb **„nicht zugreifen kann"** lauten (vgl. § 8 3.). Es wäre interessant zu wissen, ob diese mehrfachen Formulierungsschwächen durch Unwissenheit auf Seiten der Judikativen, oder durch absichtlich falsche Vorberatung durch den Landes-IT-Dienstleister zu Stande gekommen sind.

Der Eindruck einer falschen Vorberatung durch den Landes-IT-Dienstleister verstärkt sich durch Äußerungen wie: *„Eine Trennung auf Hardware-Ebene ist daher nicht zwingend, sofern eine solche auf Software-Ebene oder durch sonstige organisatorische Maßnahmen erfolgt"*. Diesen Satz kann man als InformatikerIn nur als bewusst eingebaute „Hintertür" lesen, denn in einem jeden Rechenzentrum gibt es wirklich sehr sehr viele Computer so, dass die Notwendigkeit Dienste mit hohem Sicherheitsniveau auf der gleichen Hardware mit Diensten eines niedrigen Sicherheitsniveaus laufen zu lassen praktisch bei NULL liegt. Aus der Informatik sind aber etliche Angriffsmuster auf Computer-Hardware bekannt die es sich zu Nutze machen, dass schlecht gesicherte Dienste – weil sie laut Risikoanalyse für sich allein gesehen unkritisch sind – auf der gleichen Hardware laufen wie sicherheitskritische Anwendungen und somit u.a. private kryptographische Schlüssel kopiert werden können... trotz all der „Softwaresicherheit" zwischen den Diensten. Die Sicherheitsprobleme entstehen hier also erst bei der Orchestrierung von Diensten auf einer gemeinsamen Hardware. Der einzige Ausweg ist es diese Probleme durch strikt getrennte Hardware zu lösen und dies ist auch der de-facto Standard in der IT-

Branche. Wie so eine Formulierung im Jahre 2022/23 in eine Gesetzesvorlage kommen kann, ist deshalb vollkommen unverständlich! Mit Blick auf unsere damalige Stellungnahme zum Thüringer E-Government-Gesetz wundert uns dies allerdings wenig. Bereits das ThürEGovG hatte haarsträubende technische Mängel (beispielsweise 2 MBit/s Internetanbindung als „ausreichend" für kommunale Einrichtungen) und wirkte lustlos zusammenkopiert ohne nochmalige Redigatur.

Unseres Wissens nach darf ein Gesetzgeber nur dann ein Gesetz erlassen, wenn auch die Finanzierung der dort definierten Leistungen ausreichend geregelt wurde. Hier verlangt die 3. Staatliche Gewalt einiges an IT-Leistungen, welche weder IT-Standard sind noch von den aktuellen staatlichen IT-Dienstleistern auch nur ansatzweise geleistet werden kann (eine konkrete Anfrage auf *Frag-den-Staat* hierzu läuft gerade). Hier müssen also aus unserer Sicht so oder so neue Stellen geschaffen und Millionen von Euros investiert werden. Es stellt sich also die Frage, ob dies Geld wirklich gut beim aktuellen Landes-IT-Dienstleiser aufgehoben wäre. Da von Doppeltstrukturen wirklich niemand profitiert, würden wir auch hier nochmals für ein gemeinsames Ministerium für Transparenz und Digitale Schnittstellen (TMTDS) werben.

Widersprechen wollen wir der in der Drucksache 7/6771 gemachten abwertenden Äußerungen gegenüber privaten Unternehmen und deren Leistungen. Schaut man sich vorurteilsfrei die IT-Systemlandschaft in Deutschland an, dann gibt es einige vorbildlicher (IT-)Firmen und eine Menge Insolvenzkandidaten. Die staatlichen Verwaltungen befindet sich praktisch ausschließlich im Bereich der Insolvenzkandidaten. Es vergeht fast keine Woche in den letzten Jahren (vgl. 15 bekannte Vorfälle in den ersten 21 Wochen des Jahres 2023) in dem nicht irgendeine Verwaltungs-IT von Angriffen und Ausfällen betroffen war und praktisch immer lag es an veralteter und schlecht gepflegter Informationstechnik und schlecht geschultem Personal. Nun mag es in der freien Wirtschaft nicht allzu häufig wirklich ernsthafte Sicherheitsanforderungen aus reinem Selbstzweck geben, aber solche Anforderungen werden sehr häufig von staatlicher Seite (BSI, PTB, BNetzA, etc.pp) definiert und durch Konformitätsprüfungen eingefordert. All dies tun wir im Bereich der Gesundheit, Automobil, Transport, Flugverkehr, etc.pp und mit den Resultaten scheinen alle recht zufrieden zu sein, oder? Die 3. Staatliche Gewalt setzt bei Ihrer Computer-Hardware ja auch auf die Privatwirtschaft und nicht auf staatliche Prozessoren- und Mainboard-Hersteller. Mit welcher Begründung sollte eine staatliche Verwaltungs-IT hier eine Sonderrolle spielen? Echte Synergie-Effekte wird es für den Staat und die freie Wirtschaft erst dann geben, wenn der Staat seine eigene IT so offen, transparent und fair auch für die freie Wirtschaft öffnet wie andere regulierte Technikbereiche eben auch. Vor diesem hierdurch allgemein erhöhten Sicherheitsniveau würde dann sicherlich auch die übrige Wirtschaft und die Bevölkerung profitieren. Ebenfalls macht es keinen Sinn jeden Verwaltungsprozess als möglicherweise „hochgeheim" zu klassifizieren und damit die Notwendigkeit eigener Rechenzentren zu begründen. Die überwiegende Mehrheit aller Prozesse sind gähnend langweilig und könnten in jeder Public Cloud besser und billiger verarbeitet werden... sofern grundlegende IT-Sicherheitsanforderungen umsetzen würden. Ein deutlich differenzierterer Blick auf die Anforderungen und notwendigen Sicherheitsniveaus der sehr komplexen Prozess- und Dienste-Landschaft der öffentlichen Verwaltung wäre nicht nur wünschenswert, sondern eigentlich Voraussetzung für das Gelingen von Projekten wie „OZG Versuch 2.0" oder eben diese hier skizierte IT für die 3. Staatliche Gewalt.

Die Regeln zur Benennung der Mitglieder der IT-Kontrollkommission scheint bislang aus einer reinen Verwaltungslogik heraus getroffen worden zu sein. Insofern macht sie auch durchaus Sinn für das Verständnis der rechtlichen und fachlichen IT-Anforderungen in der täglichen Praxis. Dennoch fehlen uns hier fachliche VertreterInnen die auch die informationstechnische Seite verstehen und richtig einordnen können. Immerhin steht die Kontrollkommission in ihrer „Wächterfunktion" den IT-Experten des Landes-IT-Dienstleisters gegenüber und müssen fachlich jederzeit in der Lage sein jede Behauptung in ihrem Wesenskern zu verstehen, einzuordnen und im Bedarfsfalls widerlegen zu können. Mit ein

paar Schulungen kann man dies nicht nachholen. Ebenso scheint es an externen ExpertInnen in der Kontrollkommission zu fehlen. Wenn dieses Gesetz so wichtig für den Rechtsstaat und dessen Gewaltenteilung ist, dann müssen hier auch Vertreter der Zivilgesellschaft und kritische InformatikerInnen der freien Wirtschaft in die Kontrollkommission. All dies wird ja in deren Auftrag und zu deren Wohl getan und nicht als reiner Selbstzweck der staatlichen Verwaltung.

Um den allgemeinen Charakter dieser Forderungen zu unterstreichen, würden wir deshalb auch empfehlen die **Informationsrechte aus diesem Spezialgesetz weitgehend zu streichen** und in das **Thüringer Transparenzgesetz (ThürTG)** zu verlagern. Nicht nur ist es unseres Wissens nach keine gute Rechtspraxis in Spezialgesetzen Regelungen zu treffen, die bereits in allgemeineren Gesetzen definiert wurden bzw. hätten definiert werden können, es wirkt auch äußerste befremdlich auf die BürgerInnen, wenn die staatlichen Gewalten mehr Transparenz untereinander einfordern, als sie den BürgerInnen zugestehen. Nach Meinung des Verwaltungsgerichtes Gera ist das ThürTG derzeit nur wenig besser als das alte Thüringer Informationsfreiheitsgsetz (ThürIFG) und bleibt somit weit hinter den Transparenzgesetzen anderer (Bundes-)Länder zurück. Diesen Missstand könnte man hier in einem Zug beheben, indem man eine echte einklagbare Transparenzpflicht für BürgerInnen und damit auch andere Verwaltungsabteilungen und andere staatliche Gewalten einführt. Erst wenn das aktive Verwenden des ThürTGs zum Arbeitsalltag einer jeden Verwaltung gehört, um die für sie notwendigen Informationen für die eigene tägliche Arbeit zu erhalten, wird das ThürTG aus seinem Schattendasein als „verhasster Mehraufwand" heraustreten können. Hierzu gehören dann natürlich auch Sanktionen und Strafen im ThürTG, um notorische Transparenzverweigerer zum Umdenken zu bewegen. Notfalls bis zur Entfernung aus dem öffentlichen Dienst und aus allen öffentlichen Ämtern.

In diesem Zuge sollten dann auch gleich sämtliche Gebühren des ThürTG, welche eindeutig nur auf Grund schlechter IT-Kenntnisse oder einer schlechten IT-Ausstattung gefordert werden abgeschafft werden. Wir stellen ja gerne Transparenzanfragen die absichtlich so gestellt wurden, dass sie sich sehr leicht z.B. mit einem geeigneten Dokumentenmanagementsystem beantworten lassen würden. Man könnte auch sagen, dass wir *eigentlich* Anfragen nach dem Stand der Verwaltungsdigitalisierung stellen. Solche Dokumentenmanagementsysteme existieren auf Nachfrage nach den Gründen für diese Kosten und dem Zustand der eingesetzten IT angeblich immer und würden auch benutzt werden. Es ist deshalb umso erstaunlicher, dass wir so häufig lesen müssen, dass solche Anfragen auf Grund des „Aufwandes" bis zu 500€ kosten sollen. Die Transparenzgebühren sind ja sicherlich vom Gesetzgeber nicht zum Stopfen der Löcher im IT-Budget gedacht, noch als Ausrede um sich bei unangenehmen Fragen besonders gern auf veraltete analoge Bearbeitung im Aktenkeller zurückziehen zu können. Dieser Missbrauch der Gebühren im ThürTG gehört umgehend abgeschafft. Die Verwaltung muss motiviert werden möglichst kostensparen und effizient Transparenzanfragen zu bearbeiten und nicht die BürgerInnen um ihre Informations- und Transparenzrechte zu betrügen.

Wir würden uns auch eine eindeutige „Ermächtigungsregelung" zur unmittelbaren Öffentlichkeit der Ergebnisse der IT-Kontrollkommission wünschen. Wiederum geht es uns hier vor allem um das ThürTG. Jedoch sollte die IT-Kontrollkommission hier proaktiv und zeitnah, nach ein angemessenen Rückhaltezeit, Informationen veröffentlichen müssen, nicht nur auf Nachfrage oder nur einmal im Jahr als Report. Andernfalls wird erfahrungsgemäß kein wirklicher Druck auf die IT-Dienstleister aufgebaut Probleme auch zeitnah und umfassend zu lösen. Es geht hier nicht um *„Transparenz-Nettigkeiten"*, wie die Formulierung der Gesetzesbegründung den Anschein erweckt, sondern um IT-Sicherheit und die rechtsstaatliche Ordnung an sich. Auch die BürgerInnen sind Betroffene von Schwachstellen der staatlichen IT und einer nicht vollständig unabhängigen 3. Gewalt!

Im Folgenden wollen wir kurz auf ein paar konkrete Formulierungen im Gesetzestext eingehen:

§2 Begriffsbestimmungen

[...]
8. Metadaten Informationen über Merkmale oder Eigenschaften von elektronischen Dokumenten,

8. Metadaten Informationen über Merkmale oder Eigenschaften von elektronischen Dokumenten, **(Roh-)Daten, sowie des Datenverkehrs**

[...]

Hier fehlen schlicht einige bekannte Metadaten jenseits von elektronischen Dokumenten, welche ja kurz davor sehr spezifisch definiert wurden.

§3 Ziel

[...]

..., sich aus der richterlichen Unabhängigkeit, der sachlichen Unabhängigkeit der Rechtspflegerinnen und Rechtspfleger und aus dem für die Strafverfolgung geltenden Legalitätsprinzip ergebenen besonderen Belange der Justiz sicherzustellen und zu schützen.

..., sich aus der richterlichen Unabhängigkeit, der sachlichen Unabhängigkeit der Rechtspflegerinnen und Rechtspfleger, aus dem für die Strafverfolgung geltenden Legalitätsprinzip **und dem staatlichen proaktiven Transparenzgebot** ergebenen besonderen Belange der Justiz sicherzustellen und zu schützen.

[...]

Dies dient vor allem dazu dies Spezialgesetz in den Kontext des allgemeinen Transparenzgesetzes zu rücken, um das Prinzip der proaktiven staatlichen Transparenz weiter zu stärken.

§7 Nutzung zentraler Infrastrukturkomponenten und Dienste [...]

(4) Die Gerichte und Staatsanwaltschaften sind an das Landesdatennetz mit dessen entsprechenden Sicherheitsmechanismen angeschlossen.

Man muss davon ausgehen, dass diese Sicherheitsmechanismen auf dem veralteten Grundsatz der Perimeter-Sicherheit - den Errichten einer "virtuellen Mauer" um IT-Systeme – basiert und den von der 3. Staatlichen Gewalt formulierten Schutz gegenüber vor allem internen Angreifern nicht gewährleisten kann. An dieser Stelle müssten zusätzliche Sicherheitsmaßnahmen definiert werden wie "Defence-in-Depth" d.h. mehrstufige Ende-zu-Ende-Sicherheitslösungen, Overlay- bzw. Virtuelle Private Netze, Onion-Routing, Camouflage Traffic, ...

Auch fehlt es hier an der Absicherung der notwendigen Anbindung der 3. Staatlichen Gewalt an das öffentliche Internet und damit die BürgerInnen. Wie kann/soll/muss eine sichere Durchleitung durch das Landesdatennetz aussehen? Welche zusätzlichen Regeln müssen getroffen werden, wenn Daten von externen Dritten entgegen genommen werden?

§8 Administration und Schranken

[...]

3. die im Rahmen richterlicher, rechtspflegerischer oder staatsanwaltschaftlicher Tätigkeit erstellten Daten und elektronische Dokumente von den administrativ berechtigten Personen weder eingesehen noch weitergegeben werden ~~dürfen~~,

3. die im Rahmen richterlicher, rechtspflegerischer oder staatsanwaltschaftlicher Tätigkeit erstellten Daten und elektronische Dokumente von den administrativ berechtigten Personen weder eingesehen noch weitergegeben werden **können**,

[...]

Wie bereits weiter oben erläutert kann es in diesem Gesetz nicht um „Checklisten-Sicherheit" gehen. Auf Grund der Tragweite für die Funktionsfähigkeit der rechtsstaatlichen Ordnung müssen hier geeignete mathematische und informatische Methoden verwendet werden, um unberechtigten Zugriff und Einsichtnahme ausschließen zu können. Es entspricht auch schon lange nicht mehr dem Stand der Technik, dass es überhaupt noch „allmächtige" administrative Zugänge in einem solchen System gibt. Gerade durch den konsequenten Einsatz von Verschlüsselungstechnologien und digitalen Signaturen kann eine strikte Trennung von IT-Infrastruktur und (Meta-)Daten garantiert werden. Offensichtlich kann dies der Landes-IT-Dienstleister jedoch bislang nicht gewährleisten.

Gleichzeitig stellt sich bzgl. 6. die Frage wie „Intrusion Detection"-Mechanismen umgesetzt werden sollen, um verdächtiges Verhalten automatisiert erkennen, bewerten und Gegenmaßnahmen einleiten zu können. Solche Maßnahmen funktionieren meist nur dann zuverlässig, wenn sie auch wissen auf welche Inhalte (zumindest anhand gut gepflegter Metadaten) zugegriffen wird. Es ist nicht zwingend notwendig, dass der IT-Dienstleister über die Inhalte Bescheid weiß, jedoch aber ein automatisches u.U. KI-basiertes „Wächtersystem". Zwar wird ein KI-System nicht von sich aus Daten missbrauchen oder unbefugt ins Internet stellen, dennoch bleibt die Frage wer, wie, wann und wo Zugriff auf die internen Daten(banken) eines solchen Systems erhalten kann, beispielsweise um die Rate von False-Positive-Warnmeldungen zu reduzieren.

Für 7. gibt es nach Stand der Technik der freien Wirtschaft keine Veranlassung. Im veralteten Landesdatennetz mag dies natürlich u.U. anders aussehen.

Auch hier wurden btw. wieder die BürgerInnen vergessen. Wenn ein Administratorin (unberechtigt) auf einen Datensatz zugegriffen hat, so ist natürlich auch der betroffene Bürger bzw. die betroffene Bürgerin zu informieren!

Auch in der restlichen Gesetzesinitiative fällt auf, dass an die BürgerInnen am wenigsten gedacht wurde. Der Bereich der Bürger-IT-Dienste scheint praktisch vollständig zu fehlen, jedoch ist dieser doch einer der Grundpfeiler der rechtsstaatlichen Ordnung.

Wie schaut beispielsweise die Kommunikation mit klagenden BürgerInnen aus? E-Mail mit digitalen Signaturen PGP/GPG, Telekonferenzsystem, revisionssichere Dokumentenaustauschplattform mit Verschlüsselung, digitalen Signaturen und umfangreichem Zugriffsrechtsmanagement sucht man heutzutage vergeblich. Selbst bei Klagen vor Verwaltungsgerichten wird man auf Papier und Bleistift verwiesen, oder aber auf gescheiterte IT-Projekte wie „DE-Mail". Wir vermissen irgendeine positive Zukunftsvision innerhalb eines IT-Spezialgesetzes für die 3. Staatliche Gewalt was einer digitalen Gesellschaft gerecht werden würde. Als digitalaffiner Bürger muss man es mittlerweile als absichtliche Diskriminierung betrachten seine Rechte nur auf toten Bäumen wahrnehmen zu können/dürfen.

Während die 3. Gewalt noch mit den Grundlagen der Digitalisierung kämpft, ist die restliche Gesellschaft mittlerweile im Zeitalter der künstlichen Intelligenz angelangt. Auch wenn diese noch in den Kinderschuhen steckt, so erlaubt diese erstmals die enormen Einsparpotentiale, welche die Digitalisierung immer versprochen hatte, auch zu realisieren. All dies funktioniert allerdings nur wenn auch die Entscheidungsdatenbanken der Gerichte, Verordnungen, Dienstanweisungen, etc.pp als Offene Daten allgemein zugänglich gemacht werden und diese eine semantischer Verschlagwortung, Suche und automatische Benachrichtigungen beinhalten würden, damit KI-Systeme effizient und weitgehend fehlerfrei lernen könnten. Danach könnten wir sicherlich viele Klagen schon automatisch im Vorfeld klären und unnötige Diskussionen vor Gericht vermeiden, da die notwendigen Informationen, die Anforderungen welche ein klagender Bürger/eine klagende Bürgerin beachten muss und ihre zielgruppengerechte Aufarbeitung und Formulierung, beispielsweise in einfacher Sprache oder in einer Fremdsprache, automatisch durch KI-Systeme bereitgestellt werden könnten.

Auch viele allgemeine Transparenzanfragen würden sich automatisiert beantworten lassen, wenn KI-Systeme die Datensätze der täglichen Verwaltungsarbeit verarbeiten könnten. Alles, was dafür heutzutage noch benötigt werden würde, sind mehr offene Daten inkl. eines ausreichenden Datenschutzkonzeptes. Dies wäre nicht nur für die BürgerInnen eine Entlastung, sondern auch für die transparentpflichtigen/-unwilligen Stellen und die jeweils zuständigen Verwaltungsgerichte.

Aus all diesen bürgerschaftlichen IT-Anforderungen ergeben sich natürlich auch neue IT-Sicherheitsanforderungen. Leider können wir weder in dem uns vorliegenden Gesetzestext noch in dessen Vorwort und Begründung Ansätze erkennen, die diesen neuen Anforderungen gerecht werden würden.

Abschließend kann man zusammenfassen, dass die **Intention des Gesetzes gut und richtig** ist, es jedoch an **fachlicher Tiefe und Expertise fehlt** die gewünschte Unabhängigkeit der 3. Staatlichen Gewalt auch im digitalen Zeitalter sicherstellen zu können. Somit sollte sich jeder bereits jetzt auf den Ausfall der Judikativen Gewalt bei allen Fragen rund um die beiden anderen Gewalten vorbereiten. Liest man die tägliche Presse über die Exzesse in der 1. und 2. Gewalt, so hat man sogar den Eindruck, dass dies längst trauriger Alltag ist.

Mit freundlichen digitalen Grüßen aus Jena