Rechtsprechung

>>>> Keine Ende-zu-Ende-Verschlüsselung für das beA erforderlich

BRAO § 31a; RAVPV §§ 19, 20; ZPO §§ 130 IV Nr. 2, 174 III 3

** 1. Das positive Recht erfordert es zur Zeit nicht, das besondere elektronische Anwaltspostfach mit einer Ende-zu-Ende-Verschlüsselung zu konzipieren und zu betreiben.*

** 2. Weder die BRAO noch die ZPO schreiben eine bestimmte Kryptographie oder ein bestimmtes Verfahren für das besondere elektronische Anwaltspostfach vor. Namentlich bestimmen diese Gesetze keinen Vorrang rein kryptographischer Lösungen vor solchen mit organisatorisch-physikalischen Elementen.*

** 3. Auch aus der Systematik sowie aus der Gesetzesgeschichte ergibt sich nichts anderes.*

** 4. Die Architektur des besonderen elektronischen Anwaltspostfachs ist im Rechtssinne sicher.*

AGH Berlin Urt. v. 14.11.2019 – I AGH 6/18 n.rkr.

Aus den Gründen:

A. Die Kl., sieben im Bundesgebiet residierende Rechtsanwälte und Mitglieder verschiedener Rechtsanwaltskammern, wenden sich gegen das besondere elektronische Anwaltspostfach, soweit es nicht über eine Ende-zu-Ende-Verschlüsselung verfügt, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaber befinden.

Verpflichtet durch den Bundesgesetzgeber (§ 31a I BRAO), richtete die Bekl. auf der Grundlage des § 31a I BRAO für jedes im Gesamtverzeichnis eingetragene Mitglied einer RAK ein besonderes elektronisches Anwaltspostfach [beA] empfangsbereit ein. Das System ist seit 3.9.2018 in Betrieb. Für jeden Rechtsanwalt besteht zurzeit eine sogenannte passive Nutzungspflicht: § 31a VI BRAO verpflichtet dazu, die erforderlichen technischen Einrichtungen vorzuhalten und Zustellungen und den Zugang von Mitteilungen über das beA zur Kenntnis zu nehmen. Der Sicherheitsarchitektur des von der Bekl. eingerichteten beA liegt keine „herkömmliche“ Ende-zu-Ende-Verschlüsselung zugrunde, wie sie zum Gegenstand einer europäischen Patentanmeldung (Patentblatt 1998/64 S. 2) geworden ist. Die Funktionsweise des beA ist, grob vereinfacht, vielmehr wie folgt konzipiert:

Die vom Rechtsanwalt zu versendende Nachricht wird vor ihrer Übermittlung auf seinem Computer mit einem zufällig erzeugten sog. symmetrischen Nachrichtenschlüssel verschlüsselt. Dieser Nachrichtenschlüssel wird anschließend mit dem öffentlichen Schlüssel des Empfängerpostfachs verschlüsselt, welcher im sog. SAFE-Verzeichnis der Bekl. hinterlegt ist. Sowohl die verschlüsselte Nachricht als auch der verschlüsselte Nachrichtenschlüssel werden an das Empfängerpostfach übertragen. Hier muss der Empfänger beides nacheinander entschlüsseln, um die Nachricht lesen zu können.

Um, wie es in einer Rechtsanwaltskanzlei regelmäßig erforderlich ist, mehreren Nutzern mit unterschiedlichen Berechtigungen einen Zugriff auf das Postfach zu ermöglichen, kommt ein sog. Hardware Security Module (fortan: HSM) zum Einsatz. Dabei handelt es sich um Hardwarekomponenten, die unter Einsatz krypotgraphischer Schlüssel vordefinierte Funktionen ausführen. Wenn eine Nachricht von einem berechtigten Nutzer gelesen werden soll, muss dieser sich zunächst mit dem öffentlichen Schlüssel seines Sicherheits-Tokens – z.B. seiner Zugangskarte – authentifizieren. Das HSM prüft, ob eine vom Postfachbesitzer kryptographisch signierte Berechtigung hinterlegt ist. Im Bereich des HSM wird sodann nach entsprechender Berechtigungsprüfung des anfragenden öffentlichen Schlüssels der Nachrichtenschlüssel für den jeweils berechtigten Leser umgeschlüsselt. Nach der Konzeption ist nur das HSM in der Lage, Nachrichten umzuschlüsseln, weil die Postfachschlüssel im HSM verschlüsselt abgelegt sind und auch nur dort entschlüsselt werden können. Die verschlüsselte Nachricht und der für den Nutzer umgeschlüsselte Nachrichtenschlüssel werden an den Nutzer übertragen. Dieser kann zunächst den Nachrichtenschlüssel und mit ihm die Nachricht selbst entschlüsseln.

Die Kl. sind der Auffassung, dass das beA mit dieser Sicherheitsarchitektur gegen die „bestehenden gesetzlichen Vorgaben zur technischen Ausgestaltung des beA verstößt“ (I 31), wodurch ungerechtfertigt in ihr Grundrecht auf Berufsausübungsfreiheit eingegriffen werde. Namentlich entspreche das beA nicht den durch § 31a I BRAO, § 174 III 3 i.V.m. § 130 IV Nr. 2 ZPO sowie § 20 I 1 RAVPV normierten Voraussetzungen. Insbesondere dadurch, dass die Bekl. „die privaten Schlüssel der beA-Inhaber zentral in einem HSM“ speichere, habe sie „gegen die gesetzliche Auflage verstoßen, in Gestalt des beA einen sicheren Übermittlungsweg einzurichten“. Aus §§ 19 I 1, 20 I 2 RAVPV ergebe sich zudem die Verpflichtung, das beA (ausschließlich) mit einer Ende-zu-Ende-Verschlüsselung zu betreiben. Angesichts des gesetzlichen Benutzungszwangs und der Bedeutung von Vertraulichkeit und Geheimhaltung bei der anwaltlichen Berufsausübung könne „sicher“ im Rechtssinne nur bedeuten, dass ein Verfahren ohne Vertrauen auf die Integrität des Systembetreibers auskommen müsse.

Die Kl. beantragen:

1. die Bekl. zu verurteilen, es zu unterlassen, für die Kl.in und Kl. ein beA i.S.d. § 31a BRAO ohne Ende-zu-Ende-Verschlüsselung empfangsbereit zu betreiben, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaberinnen und -inhaber befinden,

2. die Bekl. zu verpflichten, für die Kl.in und die Kl. ein beA i.S.d. § 31a BRAO mit einer Ende-zu-Ende-Ver-

schlüsselung empfangsbereit zu betreiben, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaberinnen und -inhaber befinden.

Die Bekl. beantragt, die Klage abzuweisen. Sie führt aus, die zu versendende Nachricht selbst liege zu keiner Zeit unverschlüsselt vor. Dies gelte auch für den Nachrichtenschlüssel. Die Bekl. widerspricht der Einschätzung, gesetzgeberisch sei eine bestimmte technische Architektur – z.B. die Ende-zu-Ende-Verschlüsselung – konzipiert. Vorgegeben sei vielmehr, dass das Verfahren sicher sein und über zwei voneinander unabhängige Sicherungsmittel verfügen müsse. Dies sei durch die sog. Zwei-Faktor-Authentifizierung mit einem Hard- und einem Softwaretoken sowie einer PIN gewährleistet.

B. Die Klage bleibt ohne Erfolg. Die Kl. haben keinen gegen die Bekl. gerichteten Anspruch darauf, dass sie das beA in einer bestimmten Weise konzipiert und betreibt. Namentlich können die Kl. nicht verlangen, dass das beA (ausschließlich) mit einer Ende-zu-Ende-Verschlüsselung betrieben wird (Klageantrag zu 2.). Aus diesem Grund besteht auch kein Anspruch darauf, dass die Bekl. es unterlässt, das beA ohne Ende-zu-Ende-Verschlüsselung zu betreiben (Klageantrag zu 1.).

Das positive Recht erfordert es zurzeit nicht, das beA mit einer Ende-zu-Ende-Verschlüsselung zu konzipieren und zu betreiben.

Keine Vorgabe aus BRAO und ZPO

1. Eine solche konkrete gesetzgeberische Vorgabe ergibt sich zunächst nicht unmittelbar aus den einfachen Gesetzen, namentlich der BRAO oder der ZPO.

Nach § 31a III BRAO hat die Bekl. ein „sicheres Verfahren mit zwei voneinander unabhängigen Sicherungsmitteln“ bereitzustellen. Und nach § 174 III 3 i.V.m. § 130 IV Nr. 2 ZPO sind über das beA zuzustellende Dokumente „gegen unbefugte Kenntnisnahme durch Dritte zu schützen“.

a) Aus dem Wortlaut dieser Vorschriften lässt sich das Erfordernis, das beA mit einer Ende-zu-Ende-Verschlüsselung zu konzipieren, nicht entnehmen. Im Gegenteil ist hier zu konstatieren, dass weder die BRAO noch die ZPO eine bestimmte Kryptographie oder ein bestimmtes Verfahren ausdrücklich vorschreiben. Namentlich bestimmen die

Gesetze keinen Vorrang rein kryptografischer Lösungen vor solchen mit organisatorisch-physikalischen Elementen.

Keine Vorgabe aus Systematik und Gesetzesgeschichte

b) Auch aus der Systematik sowie aus der Gesetzesgeschichte ergibt sich nichts anderes. Der Versuch der Kl., aus den Materialien zu §§ 19, 20 RAVPV etwas anderes herzuleiten, überzeugt nicht. Allerdings heißt es zu § 20 RAVPV: „Zur Gewährleistung einer sicheren Kommunikation mit Ende-zu-Ende-Verschlüsselung hat der Betrieb der besonderen elektronischen Anwaltspostfächer nach Abs. 1 S. 1 auf der Grundlage des Protokollstandards ‚Online Services Computer Interface' (OSCI) oder einem künftig nach dem Stand der Technik an dessen Stelle tretenden Standard zu erfolgen."

Und zu § 19 II RAVPV heißt es: „Soweit auch dabei stets die Beachtung der elementaren Grundelemente des besonderen elektronischen Anwaltspostfachs (wie beispielsweise die Ende-zu-Ende-Verschlüsselung von Nachrichten) sichergestellt sein muss, wird dies dadurch gewährleistet, dass auch für die Kommunikation mit anderen Stellen und Personen die Vorgaben des § 20 I RAVPV gelten."

Jedoch steht bereits in Frage, dass diese Formulierungen die Überzeugung des Verordnungsgebers belegen, das beA *müsse* mit einer Ende-zu-Ende-Verschlüsselung konzipiert werden. Nach Auffassung des Senats ist die Wortwahl vielmehr Ausfluss dessen, dass die Bekl. – ersichtlich zur Erhöhung der Akzeptanz und im Ergebnis irreleitend – über Jahre kommuniziert hat, die von ihr gewählte Architektur enthalte eine Ende-zu-Ende-Verschlüsselung. Dass dieser Terminus Eingang in die Begründung zur RAVPV gefunden hat, dürfte mithin nicht dem Umstand geschuldet sein, dass im Bundesministerium unterschiedliche Sicherheitsarchitekturen durchdacht und ausschließlich kryptografische Lösungen für sicher befunden wurden. Die Erwähnung der Ende-zu-Ende-Verschlüsselung steht nach Auffassung des Senats vielmehr damit im Zusammenhang, dass die mit der Ausarbeitung befassten Beamten die Terminologie der Bekl. übernommen und angenommen haben, das von dieser geplante beA verwende dieses Verschlüsselungs- und Übermittlungskonzept.

Ob die ausdrückliche Bezugnahme auf die Ende-zu-Ende-Verschlüsselung in den Materialien zu §§ 19, 20 RAVPV der Überzeugung entstammte, diese sei zur Erreichung der gesetzlich vorgeschriebenen Sicherheit erforderlich, oder ob es sich um ein auf die Kommunikation der Bekl. zurückgehendes Missverständnis handelte, kann aber im Ergebnis dahinstehen. Denn die RAVPV, für die der erkennende Senat ohnehin nicht die Normverwerfungskompetenz hätte, folgte § 31a III BRAO sowie § 174 III 3 i.V.m. § 130 IV Nr. 2 ZPO sowohl zeitlich als auch normenhierarchisch nach. Die Materialien zur RAVPV können damit weder historisch zur Bestimmung des Willens des Gesetzgebers (der BRAO und der ZPO) noch systematisch zur Auslegung von Vorschriften der BRAO und der ZPO herangezogen werden.

c) Auch aus Sinn und Zweck des § 31a III BRAO sowie § 174 III 3 i.V.m. § 130 IV Nr. 2 ZPO lässt sich keine Verdichtung des Entscheidungsspielraums der Bekl. auf eine bestimmte Konzeption erkennen. Namentlich ist nicht ersichtlich, dass der Gesetzgeber der Bekl. mit seinen weiten und einfachen Formulierungen eine bestimmte technische Lösung zur Sicherheitsoptimierung vorgeben und z.B. einseitig die Ausschöpfung aller kryptografischen Möglichkeiten vorschreiben und gleichzeitig ein Verfahren mit organisatorisch-physikalischen Schutzelementen verhindern wollte.

BRAK-Mitt. 2019, 320

Keine mittelbare Pflicht

2. Das Erfordernis einer Ende-zu-Ende-Verschlüsselung ergibt sich auf der Grundlage des Klägerischen Vortrags auch nicht mittelbar aus dem gesetzlichen Erfordernis eines sicheren Übertragungsweges. Dies wäre der Fall, wenn lediglich die Ende-zu-Ende-Verschlüsslung diese Voraussetzung erfüllte.

a) Der Begriff der Sicherheit unterliegt der uneingeschränkten Nachprüfung durch den AGH. Für die Feststellung der Sicherheit kommt der Bekl. kein gerichtlicher Kontrollbefugnis entzogener Beurteilungsspielraum zu. Dies hat allerdings nicht zur Folge, dass von vornherein logisch von nur *einem* im Rechtssinne sicheren Verfahren ausgegangen werden könnte. Im Rechtssinne sicher ist nicht zwingend ausschließlich das „sicherste" Verfahren. Unter wissenschaftlich gebotener Zugrundelegung eines relativen Sicherheitsbegriffs kann es vielmehr einen „Sicherheitskorridor" geben, so dass ggf. unterschiedliche Sicherheitsarchitekturen als sicher im Rechtssinne angesehen werden können. Dabei können technische Lösungen auch dann als „sicher" gelten, wenn sie zwar anderen Architekturen unterlegen, aber noch in den gewissermaßen unteren Bereich dieses gedachten Sicherheitskorridors einzustufen wären.

b) Klärungsbedürftig ist, was i.S.d. § 31a BRAO als sicher zu gelten hat. Bei dem Terminus der Sicherheit handelt es sich um einen unbestimmten Rechtsbegriff, bei dessen Anwendung und Ausgestaltung auf der Grundlage einer Gesamtbeurteilung Sinn und Zweck des Gesetzes und die geschützten Rechtspositionen der Betroffenen – hier namentlich der Kl. – heranzuziehen sind. Für den Umfang der gerichtlichen Überprüfung ist aber auch die durch die Klage vorgegebene Angriffsrichtung von Belang. Die Klage richtet sich erkennbar nicht gegen die mangelhafte Betriebssicherheit, also die Verfügbarkeit der Anwendung. Die Kl. stellen vielmehr die Bedrohung der Vertraulichkeit und – wohl auch – der Integrität der Anwendung in den Vordergrund. Der Senat sieht sich daher nicht veranlasst, die Betriebs- oder Verfügbarkeitssicherheit des besonderen elektronischen Anwaltspostfachs zu überprüfen, sondern beschränkt seine rechtliche Kontrolle auf die Sicherheit des Verfahrens und der transportierten Daten vor An- und Eingriffen.

Sicherheit ist dabei als nur relativer Zustand der Gefahrenfreiheit anzusehen, so dass Beeinträchtigungen nicht vollständig ausgeschlossen sein müssen. Vielmehr geht der Senat davon aus, dass ein – trotz Anwendung der zur Verfügung stehenden technischen Sicherungsmöglichkeiten – (stets) verbleibendes Risiko eines Angriffs auf übermittelte Daten im überwiegenden Interesse des Gemeinwohls hinzunehmen wäre (vgl. BFHE 235, 151 [juris Rn. 102]; 236, 283 [juris, Rn. 70]; vom BVerfG ausdrücklich für das besondere elektronische Anwaltspostfach angedeutet in BayVBI 2018, 378). Sicherheit erfordert allerdings, dass ein Schadenseintritt hinreichend unwahrscheinlich ist. Insgesamt kann ein Zustand als sicher gelten, der unter Berücksichtigung der Funktionalität und Standards frei von unvertretbaren Risiken ist. Dazu bedarf es einer Risikoermittlung und -bewertung, also der Einschätzung denkbarer Ereignisse und hierauf bezogener Ereigniswahrscheinlichkeiten (vgl. BVerwG, NVwZ-RR 1991, 137 [Flughafenbau Stuttgart]).

beA ist im Rechtssinne sicher

c) Nach diesen Maßgaben beurteilt der Senat die Architektur des beA auf der Grundlage des Sach- und Streitstandes als im Rechtssinne sicher.

aa) Dabei orientiert sich der Senat an dem von beiden Parteien eingereichten Gutachten, das die Bekl. in Auftrag gegeben hatte und die secunet Security Networks AG am 18.6.2018 vorgelegt hat (in der Folge: „Gutachten"). Dieses Gutachten ermittelte die Schwachstellen und unterzog die einer ausführlichen, qualifizierten und nachvollziehbaren Risikobewertung.

Die Kl. haben sich zu der entscheidungserheblichen und vom Senat durch Hinweisbeschluss ausdrücklich aufgeworfenen Frage, „unter welchen Voraussetzungen unbefugte Dritte Kenntnis zuzustellender Dokumente erlangen können und welcher Aufwand hierzu erforderlich wäre", ausdrücklich und ohne Einschränkung auf dieses Gutachten bezogen. Wörtlich haben sie formuliert, die vom Senat aufgeworfene Frage sei bereits „durch das Gutachten der von der Bekl. beauftragten Secunet geklärt". Mit dieser ausdrücklich gegen eine (beabsichtigte) Beweiserhebung gerichteten Erklärung haben die Kl. ihre vorangegangene Bekundung, das Gutachten als „geeignete Grundlage zur Beurteilung der Sicherheit des besonderen elektronischen Anwaltspostfachs" nicht anzuerkennen (I 114), ersetzt, so dass keine Bedenken bestehen, es im zugestandenen

Umfang zur Grundlage einer Entscheidung zu machen. Der Amtsaufklärungsgrundsatz (§ 86 I VwGO) gebietet nichts anderes, weil der Senat – nunmehr ersichtlich in Übereinstimmung mit beiden Parteien – keinen Anlass zur Einschätzung hat, dass eine gerichtlich veranlasste Beweiserhebung zu Bedrohungsszenarien und Schwachstellen des besonderen elektronischen Anwaltspostfachs weitergehende Erkenntnisse zeitigt und signifikant abweichende Bewertungen erfordert. Dies gilt umso mehr, als das Gutachten sich ausdrücklich und ausschließlich auf die hier streitgegenständliche Sicherheit des IT-Verfahrens fokussiert und Fragen der Funktionalität, Ergonomie u.Ä. unbeachtet lässt:

bb) Das Gutachten analysiert und bewertet die „Umsetzung des besonderen elektronischen Anwaltspostfachs hinsichtlich der IT-Sicherheit“ (S. 8). So heißt es: „Ziel der Analyse ist, bereits bekannte technische, organisatorische und konzeptionelle Schwachstellen zu validieren und gegebenenfalls vorhandene neue Schwachstellen zu identifizieren und zu beurteilen.“ (S. 8). Dabei legt das Gutachten ein Angriffsszenario mit aus dem Internet agierendem Angreifer zugrunde (sog. Greybox-Ansatz) sowie eines, die dem der Angreifer mit valider Zugangskarte und dazugehöriger PIN einen einfachen Zugang zum System hat. Weitere Angriffsszenarien werden durch Quelltextanalysen und die konzeptionelle

BRAK-Mitt. 2019, 321

Analyse ergänzt (sog. Whitebox-Ansatz) (S. 28). Konzeptionell geht das Gutachten von dem „erkennbaren Ziel“ aus, „die Sicherheit der Nachrichten ausschließlich durch Kryptographie zu schützen“, das „aber nicht in vollem Umfang erreicht worden“ sei (S. 11). Weiter heißt es hierzu: „An einigen Stellen verlässt sich das beA in seiner dem Gutachten zugrunde liegenden Realisierung auf organisatorisch-physikalischen Schutz wichtiger Systemkomponenten (HSM-Schlüssel, SAFE BRAK), was bei voller Ausnutzung der kryptographischen Möglichkeiten, die das Konzept und die eingesetzte Technik bieten, nicht notwendig wäre.“ Trotz dieser Bewertung führt das Gutachten aus:

Sicherheitsgutachten

„Grundsätzlich ist das dem beA zugrundeliegende Verschlüsselungskonzept geeignet, die Vertraulichkeit der Nachrichten während der Übertragung und Speicherung von Nachrichten durch das beA zu gewährleisten, auch gegenüber dem Betreiber des beA. Nachrichteninhalte liegen unverschlüsselt nur bei den Kommunikationspartnern vor. Die Umverschlüsselung ist in einem HSM gekapselt, schützt daher dort vorübergehend entstehende Schlüsselinformationen in einer besonderen manipulations- und ausspähsicheren Umgebung.“

cc) Allen bei den Angriffsszenarien zutage geförderten Schwachstellen war gemein, dass das HSM keinen ausreichenden Schutz vor Angriffen bot, d.h. Nachrichten bei erfolgreichem Angriff auch außerhalb des HSM entschlüsselt oder dem HSM Leseberechtigungen vorgetäuscht werden konnten. Angriffe konnten nach den Feststellungen nur durch Innentäter oder mit Hilfe von Innentätern, darunter auch Personen mit besonderer Vertrauensstellung, durchgeführt werden, die dabei physikalisch-organisatorische Schutzmaßnahmen unterlaufen müssten. Außentäter, so konstatiert das Gutachten, „können sich in die Position eines Innentäters bringen, wenn es ihnen gelingt, durch Ausnutzung von Schwachstellen der Serverkomponenten in diese einzudringen und die Kontrolle über sie zu übernehmen“. Weiter heißt es: „Nur in einem Fall, einer Täuschung eines beA-Anwenders mittels einer irreführenden EGVP-Adresse, ist auch ein Angriff durch einen Außentäter denkbar, der dafür die beA-Anwendung nicht angreifen muss. Die Ausnutzbarkeit der Schwachstellen ist in der Regel aufgrund des eingeschränkten Täterkreises und einer angenommenen geringen Motivation und besseren Überwachbarkeit von Innentätern gering. Die konzeptionellen Schwachstellen erhalten ihre Bedeutung in der Regel durch ihr hohes (teilweise sehr hohes) Schadenspotential.“

Die hiernach ausgemachten und ausführlich beschriebenen Schwachstellen werden im Gutachten u.a. danach qualifiziert, ob sie „betriebsverhindernd“ („Behebung vor Wiederinbetriebnahme dringend empfohlen“) oder nur „betriebsbehindernd“ („Behebung sobald wie möglich empfohlen“) sind. Diese Einstufung wiederum erfolgt nach dem Ausmaß der Bedrohung der Schutzziele (bei erfolgreichem Angriff eintretende Schäden für „Vertraulichkeit“, „Integrität“ und – hier nicht von Belang – „Verfügbarkeit“) im Verhältnis zur „Ausnutzbarkeit“ (Komplexität eines Angriffs: „hoch – mittel – leicht“). Das Gutachten bekennt sich dazu, die Wahrscheinlichkeit eines Schadenseintritts im Hinblick auf die Motivation eines Angreifers und seine Bereitschaft, die erforderlichen Mittel aufzuwenden und die Risiken einzugehen, „nur sehr grob“ zu berücksichtigen, weil der Nutzen des potentiellen Angreifers mangels Erfahrungswerten nicht qualifizierbar sei (S. 22).

Bei den im Gutachten ausgemachten vier betriebsverhindernden Schwachstellen handelte es sich um „nicht autorisiertes File-Sharing“, „Auslesen von Metadaten dritter Nachrichten“, „Modifikation von signierten Nachrichten“ sowie – bezogen auf die mit den Servern der Anwendung des beA kommunizierende Anwendung beA-Client-Security – „veraltete Softwareelemente“. Bei dem letzten Punkt handelte es sich um „veraltete Javascript-Bibliotheken“.

Sicherheitslücken inzwischen behoben

dd) Die beiden erstgenannten Sicherheitslücken sind, zwischen den Parteien unstreitig, noch vor der Niederlegung des schriftlichen Gutachtens behoben worden. Die beiden weiteren „betriebsverhindernden“ Schwachstellen sind, so ist es von der Bekl. vorgetragen und durch die Vorlage einer Bestätigung der Secunet (A7) bewiesen sowie von den Kl. auch nicht substanziiert in Abrede gestellt, gleichfalls behoben worden, bevor die Anwendung am 3.9.2018 in Betrieb ging. Den von den Kl. damit ausdrücklich in Bezug genommenen im Gutachten beschriebenen und dort zugrunde gelegten Angriffsszenarien hat die Bekl. folglich – ausweislich des Gutachtens – durch Veränderungen verschiedener Art in einer Weise Rechnung getragen, die erfolgsversprechende Angriffe nicht (mehr) befürchten lässt. Vor diesem Hintergrund können auch die vielfältigen klägerischen Verweisungen auf das Gutachten keine *anhaltend sicher bestehenden* Schwachpunkte dartun.

Zwar haben die Kl. ausdrücklich nur auf die im Gutachten beschriebenen Angriffsszenarien und die hierfür zu betreibenden Aufwände Bezug genommen. Sie sind aber der durch die Bestätigung des Gutachtens bekräftigten Behauptung, die sicherheitsrelevanten Schwachstellen seien beseitigt, nicht substanziiert entgegengetreten, so dass der Senat auch unter dem Regime der Amtsaufklärung zuletzt keinen Anlass mehr gesehen hat, ergänzenden Beweis zu erheben. Die Kl. haben sich im Wesentlichen – erfolglos – darauf beschränkt, das Erfordernis einer Ende-zu-Ende-Verschlüsselung unmittelbar aus dem Gesetz ableiten zu wollen; dass das besondere elektronische Anwaltspostfach in seiner jetzigen Konzeption einen sicheren Übermittlungsweg darstellt, wurde nur „hilfsweise bestritten“ (I 113). Hingegen haben sie es versäumt, sich in qualifizierter Weise mit den detaillierten Erkenntnissen und Bewertungen des Gutachtens auseinanderzusetzen, auf das sie zudem zur Ergänzung ihres Vortrags ausdrücklich Bezug genommen haben. Dass im Verfahren vor dem AGH

BRAK-Mitt. 2019, 322

der Amtsaufklärungsgrundsatz voll, die Dispositionsmaxime jedoch nur eingeschränkt gilt, verlangt keine andere Bewertung. Denn wie bereits ausgeführt, hat der Senat keinen Anlass für die Erwartung, dass eine weitere Aufklärung, namentlich die Einholung eines Sachverständigengutachtens zur Sicherheit des jetzt betriebenen Verfahrens und zu weiteren Konzepten, zu Erkenntnissen führt, die über jene des nicht nur ausführlichen, sondern auch ersichtlich sachkritischen Gutachtens entscheidungserheblich hinausgehen.

ee) Die durch die Kl. angedeutete und im Gutachten (S. 85) ausdrücklich nicht evaluierte Möglichkeit, der Betreiber könne „im Rahmen von Beschlagnahmen von Postfächern gezwungen werden“, Nachrichten offenzulegen, stellt, ihr Bestehen unterstellt, keine

Beeinträchtigung der von Gesetztes wegen verlangten Sicherheit des Übertragungsweges dar. Durch diese Möglichkeit bleibt die Integrität der Anwendung ohnehin bestehen, in Frage gestellt sein könnte allenfalls die Sicherheit der Vertraulichkeit. Allerdings versteht es sich von selbst, dass die §§ 31a III BRAO, 130a IV Nr. 2, 174 III ZPO die Bekl. nicht dazu verpflichten, einen elektronischen Kommunikationsweg zu schaffen, der den *rechtmäßigen* Zugriff durch Justiz und Polizeibehörden unmöglich macht. Die durch die Kl. bevorzugte Lösung einer Ende-zu-Ende-Verschlüsselung mag einen derartigen Zugriff ausschließen und damit unter dem Gesichtspunkt der Vertraulichkeitssicherheit der hier gewählten Lösung mit organisatorisch-physikalischen Elementen „objektiv" überlegen sein. Ein solcher auf das Tatsächliche beschränkter Vergleich verbietet sich aber. Da Sicherheit als Rechtsbegriff normativ zu verstehen ist, kann die Möglichkeit eines in einem rechtsstaatlichen Verfahren erlaubten Zugriffs auf Daten keine Beeinträchtigung der Sicherheit im Rechtssinne darstellen. Der Senat lässt es daher ausdrücklich offen, ob das von der Bekl. konzipierte und nun betriebene beA es ermöglicht, dass der Betreiber auf diese Weise zum Zugriff auf Kommunikationsdaten und zu deren Herausgabe veranlasst werden kann. Denn auch wenn eine solche „Kompromittierung" technisch und organisatorisch-physikalisch möglich wäre, würde sie unter den hier maßgeblichen Bedingungen des Rechtsstaats die Sicherheit des Verfahrens im Rechtssinne nicht beeinträchtigen.

3. Für das auf den allgemeinen öffentlich-rechtlichen Unterlassungsanspruch gestützte Unterlassungsbegehren können sich die Kl. auch nicht auf eine drohende oder eingetretene Grundrechtsverletzung stützen. Zwar greift die Verpflichtung, das beA einzurichten, in die durch Art. 12 I 2 GG geschützte Freiheit der Berufsausübung der Kl. ein, Namentlich § 31a BRAO stellt jedoch eine ausreichende gesetzliche Ermächtigungsnorm dar (vgl. BGH, NJW 2018, 2645; WM 2016, 1662); sie lässt Umfang und Grenzen des Eingriffs erkennen. Insbesondere hat der Gesetzgeber mit dem Erfordernis eines „sicheren Verfahrens mit zwei voneinander unabhängigen Sicherungsmitteln" die gesetzlicher Regelung zugängliche wesentliche Entscheidung getroffen. Erforderlich ist nicht, dass sich die Eingriffsvoraussetzungen ohne weiteres aus dem Wortlaut des Gesetzes ergeben müssten; es genügt, dass sie sich mit Hilfe allgemeiner Auslegungsgrundsätze erschließen lassen, insbesondere aus dem Zweck, dem Sinnzusammenhang und der Vorgeschichte der Regelung (vgl. BVerfGE 19, 17; 58, 257; 62, 203; 80, 1; 82,209).

Dies ist bei dem unbestimmten Rechtsbegriff der Sicherheit, zumal hier ergänzt durch das objektivierbare Erfordernis zweier unabhängiger Sicherungsmittel, der Fall (vgl. BGH, a.a.o.). Dass das beA über in diesem Sinn unabhängige Sicherungsmittel verfügt, ist durch die Kl. trotz umfänglichen Sachvortrags zuletzt als „nicht streitgegenständlich" bewertet worden und wird damit ersichtlich nicht (mehr) in Frage gestellt. Die Qualifizierung des von der Bekl. konzipierten beA als im Rechtssinne sicher und damit rechtskonform ist, wie dargelegt wurde, prozessual nicht durchgreifend erschüttert worden.

4. Nach alldem ergibt sich weder aus dem Grundrecht der Berufsausübungsfreiheit der Kl. noch aus den einfachen Gesetzen eine Verpflichtung der Bekl., die über das beA versandten Dokumente ausschließlich durch Kryptographie zu schützen. Die von der Bekl. konzipierte Lösung mit kryptografischem Schwerpunkt und organisatorisch-physischen Schutzelementen genügt – jedenfalls beim gegenwärtigen Streit- und Wissensstand – den gesetzlichen Vorgaben.

Hinweise der Redaktion:

Die Entscheidung ist noch nicht rechtskräftig. Der AGH Berlin hat die Berufung wegen grundsätzlicher Bedeutung der Sache zugelassen.

Anders als das LG unter A. angibt, ging das beA bereits am 28.11.2016 in Betrieb.