BUNDESGERICHTSHOF

IM NAMEN DES VOLKES

URTEIL

AnwZ (Brfg) 2/20

Verkündet am:
22. März 2021
Boppel
Justizamtsinspektor
als Urkundsbeamter
der Geschäftsstelle

in der verwaltungsrechtlichen Anwaltssache

Nachschlagewerk: ja

BGHZ: ja

BGHR: ja

BRAO § 31a Abs. 1 und 6; RAVPV §§ 19, 20

a) Der Bundesrechtsanwaltskammer steht ein Spielraum bei der technischen Ausgestaltung der Nachrichtenübermittlung mittels des besonderen elektronischen Anwaltspostfachs zu, sofern das gewählte System eine im Rechtssinne sichere Kommunikation gewährleistet.

b) Ein Anspruch von Rechtsanwälten gegen die Bundesrechtsanwaltskammer darauf, dass diese das besondere elektronische Anwaltspostfach mit einer Ende-zu-Ende-Verschlüsselung im Sinne der Europäischen Patentschrift EP 0 877 507 B1 versieht und betreibt, besteht nicht. Weder die gesetzlichen Vorgaben für die Errichtung und den Betrieb des besonderen elektronischen Anwaltspostfachs noch die Verfassung gebieten eine derartige Verschlüsselung.

c) Zur Sicherheit der Verschlüsselungstechnik des besonderen elektronischen Anwaltspostfachs.

BGH, Urteil vom 22. März 2021 - AnwZ (Brfg) 2/20 - Anwaltsgerichtshof Berlin

ECLI:DE:BGH:2021:220321UANWZ.BRFG.2.20.0

Der Bundesgerichtshof, Senat für Anwaltssachen, hat auf die mündliche Verhandlung vom 22. März 2021 durch die Präsidentin des Bundesgerichtshofs Limperg, die Richterinnen Dr. Liebert und Ettl, den Rechtsanwalt Dr. Kau und die Rechtsanwältin Merk

für Recht erkannt:

Die Berufung der Kläger gegen das am 14. November 2019 verkündete Urteil des I. Senats des Anwaltsgerichtshofs Berlin wird zurückgewiesen.

Die Kosten des Berufungsverfahrens tragen die Kläger je zur Hälfte.

Der Wert des Berufungsverfahrens wird auf 10.000 Euro festgesetzt.

Tatbestand:

1 Die Kläger sind zugelassene Rechtsanwälte. Die Beklagte richtete auf Grundlage von § 31a Abs. 1 BRAO für sie ein besonderes elektronisches Anwaltspostfach (im Folgenden auch: beA) ein. Nach § 31a Abs. 6 BRAO sind die Kläger verpflichtet, die für dessen Nutzung erforderlichen technischen Einrichtungen vorzuhalten sowie Zustellungen und den Zugang von Mitteilungen über das beA zur Kenntnis zu nehmen.

2 Die Kläger wenden sich gegen die technische Ausgestaltung des beA durch die Beklagte und streben an, dass dieses mit einer Ende-zu-Ende-Verschlüsselung betrieben wird, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaber befinden. Sie berufen sich für die Definition der Ende-zu-Ende-Verschlüsselung auf die europäische Patentanmeldung EP 0 877 507 A 2, die zu dem europäischen Patent EP 0 877 507 B 1 vom 26. September 2007 führte.

3 Kern des Streits ist die Verwendung eines sogenannten Hardware Security Module (im Folgenden: HSM), das bei der Ablage und dem Abruf von Nachrichten vereinfacht wie folgt zum Einsatz kommt: Die versandten, mit einem symmetrischen Nachrichtenschlüssel verschlüsselten Nachrichten werden in verschlüsselter Form im Postfach des Empfängers gespeichert. Symmetrische Verschlüsselung bedeutet hierbei, dass derselbe Schlüssel - hier der sogenannte Nachrichtenschlüssel - verwendet wird, um die Nachricht zu verschlüsseln und auch wieder zu entschlüsseln. Der Empfänger der Nachricht benötigt mithin den Nachrichtenschlüssel, um die Nachricht entschlüsseln zu können. Der Nachrichtenschlüssel ist seinerseits verschlüsselt mit dem öffentlichen Schlüssel des Empfängerpostfachs, der - ebenso wie der zugehörige private Schlüssel des Postfachs - beim Anlegen des Postfachs im HSM erzeugt wurde. Dieser verschlüsselte Nachrichtenschlüssel wird an das HSM übergeben und dort auf den symmetrischen Schlüssel des Postfachs umgeschlüsselt. Der mit dem symmet-

rischen Schlüssel des Postfachs verschlüsselte Nachrichtenschlüssel wird sodann im Postfach gespeichert. Nachdem derjenige, der die Nachricht abrufen möchte (im Folgenden: Client), seine Berechtigung durch die vorgesehene Authentifizierung nachgewiesen hat, wird der verschlüsselte Nachrichteninhalt ohne Veränderung aus dem Postfach an den Client übertragen. Der mit dem symmetrischen Postfachschlüssel verschlüsselte Nachrichtenschlüssel wird im HSM auf einen dem Client zugeordneten symmetrischen sogenannten Kommunikationsschlüssel umgeschlüsselt. Der auf diese Weise verschlüsselte Nachrichtenschlüssel wird sodann an den Client übertragen und kann dort mit Hilfe seines Kommunikationsschlüssels entschlüsselt werden. Mit dem entschlüsselten Nachrichtenschlüssel lässt sich sodann die verschlüsselte Nachricht entschlüsseln.

4 Nachdem bei der Inbetriebnahme des beA technische Probleme aufgetreten waren, nahm die Beklagte das beA Ende 2017 vorübergehend außer Betrieb und beauftragte die s. AG mit der Begutachtung der Sicherheit des beA. Deren Abschlussgutachten vom 18. Juni 2018 ist von beiden Parteien in den Prozess eingeführt worden (im Folgenden: S. -Gutachten).

5 Das S. -Gutachten bewertete das beA als grundsätzlich geeignetes System zur vertraulichen Kommunikation, stellte aber gleichzeitig auch betriebsverhindernde, betriebsbehindernde und sonstige nicht behobene Schwachstellen fest, die behebbar seien. Das Gutachten empfahl, die betriebsverhindernden Schwachstellen vor Wiederaufnahme des beA zu beseitigen, die betriebsbehindernden baldmöglichst danach. Bei Beachtung der Vorgaben sei eine Wiederaufnahme des Betriebs aus sicherheitstechnischer Sicht möglich. Wegen der Einzelheiten wird auf das Gutachten Bezug genommen. Im Spätsommer 2018 nahm die Beklagte das beA wieder in Betrieb.

6 Die Kläger machen geltend, die Beklagte sei verpflichtet, die über das beA geleiteten Nachrichten mittels einer Ende-zu-Ende-Verschlüsselung zu verschlüsseln, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaber befinden. Eine Ende-zu-Ende-Verschlüsselung liege

bei der derzeitigen Struktur insbesondere nicht vor, weil die privaten Schlüssel der beA-Postfachinhaber zentral im HSM erstellt und gespeichert würden und damit nicht - was Voraussetzung einer Ende-zu-Ende-Verschlüsselung sei - in der alleinigen Verfügungsgewalt der sie verwendenden Kommunikationspartner stünden. Mit ihrer Klage wollen sie die Verurteilung der Beklagten zur Unterlassung des Betreibens eines besonderen elektronischen Anwaltspostfachs für sie ohne dementsprechende Ende-zu-Ende-Verschlüsselung erreichen sowie die Verpflichtung der Beklagten zum Betrieb eines besonderen elektronischen Anwaltspostfachs für sie mit einer derartigen Ende-zu-Ende-Verschlüsselung.

7 Wegen der Einzelheiten des Sach- und Streitstands erster Instanz wird auf den Tatbestand des erstinstanzlichen Urteils verwiesen.

8 Der Anwaltsgerichtshof hat die Klage abgewiesen. Die Kläger hätten keinen gegen die Beklagte gerichteten Anspruch darauf, dass diese das besondere elektronische Anwaltspostfach in einer bestimmten Weise konzipiere und betreibe. Namentlich könnten die Kläger nicht verlangen, dass das beA ausschließlich mit einer Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne betrieben werde. Eine entsprechende gesetzgeberische Vorgabe ergebe sich nicht unmittelbar aus den einfachen Gesetzen wie § 31a Abs. 3 BRAO oder § 174 Abs. 3 Satz 3 ZPO in Verbindung mit § 130a Abs. 4 Nr. 2 ZPO. Aus §§ 19, 20 der Verordnung über die Rechtsanwaltsverzeichnisse und die besonderen elektronischen Anwaltspostfächer (Rechtsanwaltsverzeichnis- und -postfachverordnung - RAVPV) sei insoweit nichts Anderes herzuleiten. Das Erfordernis einer Ende-zu-Ende-Verschlüsselung ergebe sich auch nicht mittelbar aus dem gesetzlichen Erfordernis eines sicheren Übertragungswegs. Dies wäre nur der Fall, wenn allein die Ende-zu-Ende-Verschlüsselung diese Voraussetzungen erfüllte. Die Architektur des besonderen elektronischen Anwaltspostfachs sei jedoch sicher im Rechtssinne. Hierbei orientiere sich der Senat an dem von beiden Parteien eingereichten S. -Gutachten, das das beA einer ausführlichen, qualifizierten und nachvollziehbaren Risikobewertung unterzogen habe. Die in dem Gutachten ausgemachten vier betriebsverhindernden Schwachstellen seien

- unbestritten - behoben worden. Damit könnten die klägerischen Verweisungen auf das Gutachten keine anhaltend sicher bestehenden Schwachstellen dartun.

9 Die Kläger könnten das auf den allgemeinen öffentlich-rechtlichen Unterlassungsanspruch gerichtete Unterlassungsbegehren auch nicht auf eine drohende oder eingetretene Grundrechtsverletzung stützen. Zwar greife die Verpflichtung, das besondere elektronische Anwaltspostfach einzurichten, in die durch Art. 12 Abs. 1 GG geschützte Freiheit der Berufsausübung der Kläger ein. § 31a BRAO stelle jedoch eine ausreichende gesetzliche Ermächtigungsnorm dar.

10 Gegen die Abweisung der Klage wenden sich zwei der ursprünglich sieben Kläger mit ihrer vom Anwaltsgerichtshof zugelassenen Berufung. Sie wiederholen und vertiefen ihr erstinstanzliches Vorbringen. Sie tragen insbesondere vor, die Architektur des beA ermögliche ein Ausspähen sämtlicher anwaltlicher Kommunikation mittels eines einzigen Angriffs, eines sogenannten Single Point of Failure. Die Kläger beziehen sich diesbezüglich insbesondere auf die in dem S. -Gutachten unter 5.5.3 genannte, als betriebsbehindernd eingestufte Schwachstelle, wonach alle HSM-Schlüssel auch außerhalb des HSM als verschlüsselte Dateien existierten. Entgegen der Auffassung des Anwaltsgerichtshofs bestehe dieser Fehler weiterhin. Daher sei das beA auch nicht im Rechtssinne sicher. Der Anwaltsgerichtshof habe sich bei seiner Herleitung dessen, was sicher im Rechtssinne sei, sowohl über den Willen des Gesetzgebers und des Verordnungsgebers als auch über die Rechtsprechung des Bundesverfassungsgerichts hinweggesetzt. Die Verpflichtung der Beklagten zur Einrichtung der von den Klägern geforderten Verschlüsselung ergebe sich auch aus der Festlegung des OSCI-Protokollstandards in § 20 Abs. 1 RAVPV. Der Grundsatz der Verhältnismäßigkeit würde die Wahl der sichersten technischen Lösung gebieten. Dies sei die von ihnen geforderte Ende-zu-Ende-Verschlüsselung. Die von der Beklagten gewählte Lösung sei dagegen eine unzulässige minderwertige Lösung.

11 Die Kläger beantragen,

das Urteil des Anwaltsgerichtshofs Berlin vom 14. November 2019 aufzuheben und

1. die Beklagte zu verurteilen, es zu unterlassen, für die Kläger ein besonderes elektronisches Anwaltspostfach im Sinne des § 31a BRAO ohne eine Ende-zu-Ende-Verschlüsselung empfangsbereit zu betreiben, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaberinnen und -inhaber befinden,

2. die Beklagte zu verpflichten, für die Kläger ein besonderes elektronisches Anwaltspostfach im Sinne des § 31a BRAO mit einer Ende-zu-Ende-Verschlüsselung empfangsbereit zu betreiben, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaberinnen und -inhaber befinden.

12 Die Beklagte beantragt,

die Berufung zu verwerfen, hilfsweise diese zurückzuweisen.

13 Sie hält die Berufung bereits für unzulässig, weil die Berufungsbegründung entgegen § 124a Abs. 3 Satz 4 VwGO keinen bestimmten Antrag enthalte. Die Berufung sei zudem unbegründet. Die Beklagte wiederholt und vertieft hierzu ihren erstinstanzlichen Vortrag. Hiernach stehe den Klägern kein direkter Anspruch auf Unterlassung beziehungsweise Leistung aus § 31a BRAO zu, da kein Anspruch bestehe, anders als andere Rechtsanwälte behandelt zu werden, weil das beA-System nur als Ganzes für alle im Gesamtverzeichnis eingetragenen Rechtsanwälte betrieben werden könne. Zudem ergebe sich aus den einschlägigen Normen keine Verpflichtung, das System mit der von den Klägern geforderten Ende-zu-Ende-Verschlüsselung zu betreiben. Die von ihr gewählte Konstruktion sei sicher. Die von den Klägern benannte B-Schwachstelle - HSM-Schlüssel existierten auch außerhalb des HSM - sei zwischenzeitlich behoben.

14 Wegen des weiteren Vorbringens der Parteien wird auf die gewechselten Schriftsätze nebst Anlagen Bezug genommen.

Entscheidungsgründe:

15 Die zulässige Berufung der Kläger bleibt ohne Erfolg. Der Anwaltsgerichtshof hat die Klage zu Recht abgewiesen.

I.

16 Die Berufung ist auf Grund der Zulassung durch den Anwaltsgerichtshof nach § 112e Satz 1 BRAO statthaft und auch im Übrigen gemäß § 112e Satz 2 BRAO, § 124a Abs. 2 und 3 VwGO zulässig.

17 Entgegen der Auffassung der Beklagten enthält die Berufungsbegründung einen hinreichend bestimmten Antrag im Sinne von § 124a Abs. 3 Satz 4 VwGO. Zwar beinhaltet diese keinen ausdrücklich formulierten Antrag. Dies ist indes nicht erforderlich. Dem Antragserfordernis wird bereits entsprochen, wenn in dem einzureichenden Schriftsatz hinreichend deutlich zum Ausdruck kommt, dass, in welchem Umfang und weshalb der Berufungsführer das Berufungsverfahren führt (vgl. BVerwG, Beschluss vom 21. September 2011 - 3 B 56/11, juris Rn. 6 mwN). Dies ist hier der Fall. Der Berufungsbegründung lässt sich jedenfalls im Wege der Auslegung eindeutig entnehmen, dass die Berufungskläger ihre erstinstanzlichen Anträge weiterverfolgen wollen. Hieraus ergibt sich zweifelsfrei, dass mit der Berufung die Klageabweisung vollumfänglich angegriffen wird und die erstinstanzlichen Klageziele aufrechterhalten werden sollen.

II.

18 Die Berufung ist unbegründet. Der Anwaltsgerichtshof hat die Klage zu Recht abgewiesen. Diese ist zwar zulässig, aber unbegründet.

19 1. Die Klage ist hinsichtlich beider Klageanträge als allgemeine Leistungsklage statthaft und auch im Übrigen zulässig. Insbesondere liegt die analog § 112c Abs. 1 Satz 1 BRAO, § 42 Abs. 2 VwGO erforderliche Klagebefugnis (vgl. z.B. BVerwGE 147, 312, 316; BVerwGE 101, 157, 159) vor. Die Klagebefugnis würde nur fehlen, wenn den Klägern die geltend gemachten Rechte offensichtlich und eindeutig nach keiner Betrachtungsweise zustehen könnten (vgl. BVerwG, NVwZ 2019, 69 Rn. 21; BVerwGE 101, 157, 159; jeweils mwN). Dies ist nicht der Fall. Es ist nicht offensichtlich ausgeschlossen, dass den Klägern ein Anspruch auf Unterlassung des Betreibens des beA ohne die von ihnen verlangte Ende-zu-Ende-Verschlüsselung (Klageantrag zu 1) und auf das Betreiben mit der von ihnen geforderten Ende-zu-Ende-Verschlüsselung (Klageantrag zu 2) zustehen könnte. Vielmehr ist es zumindest möglich, dass sich jedenfalls aus § 20 Abs. 1 RAVPV ein entsprechender Anspruch der Kläger ergibt. Hiernach hat die Beklagte die besonderen elektronischen Anwaltspostfächer auf der Grundlage des Protokollstandards "Online Services Computer Interface - OSCI" oder einem künftig nach dem Stand der Technik an dessen Stelle tretenden Standard zu betreiben und fortlaufend zu gewährleisten, dass die in § 19 Abs. 1 RAVPV genannten Personen und Stellen miteinander sicher elektronisch kommunizieren können. Es ist auf Grund des Verweises auf die OSCI-Protokollstandards oder auf Grund des Erfordernisses einer "sicheren" Kommunikation zumindest denkbar, dass sich hieraus - wie die Kläger geltend machen - die Verpflichtung der Beklagten zum Betrieb des beA mit einer Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne ergibt.

20 Jedenfalls die Verpflichtung zur Gewährleistung einer sicheren Kommunikation ist drittschützend, denn sie dient auch dem Schutz der über das beA kommunizierenden Nutzer, indem sie auch in deren Interesse die Vertraulichkeit der hierüber abgewickelten Kommunikation schützt. Zwar statuieren die einfachgesetzlichen Vorgaben zur Errichtung und zum Betrieb des beA in § 31a BRAO und § 20 RAVPV in erster Linie Aufgaben der Beklagten. Doch dienen diese Pflichten der Beklagten zugleich berechtigten Interessen der in das Gesamtverzeichnis

eingetragenen Mitglieder der Rechtsanwaltskammern und damit auch den Klägern. Der so angesprochene Personenkreis ist zwar groß, lässt sich jedoch anhand individualisierter Tatbestandsmerkmale klar von der Allgemeinheit unterscheiden (vgl. Kopp/Schenke, VwGO, 26. Aufl., § 42 Rn. 84). Als Nutzer, für die ein besonderes elektronisches Anwaltspostfach eingerichtet wurde, können die Kläger sich mithin hierauf berufen und hieraus ihre Klagebefugnis ableiten. Der mit dem Klageantrag zu 1 geltend gemachte Anspruch, es zu unterlassen, das beA ohne die im Antrag aufgeführte Ende-zu-Ende-Verschlüsselung empfangsbereit zu betreiben, könnte sich dann möglicherweise aus dem öffentlich-rechtlichen Abwehr- und Unterlassungsanspruch ergeben, der mit dem Klageantrag zu 2 geltend gemachte Anspruch als Leistungsanspruch aus § 20 RAVPV.

21 Im Hinblick hierauf ist die Klage insgesamt zulässig und führt zur umfassenden Sachprüfung unter Berücksichtigung der möglichen Anspruchsgrundlagen, ohne dass es darauf ankommt, ob diese ebenfalls eine Klagebefugnis begründet hätten (vgl. BVerwGE 60, 123, 125). Darauf, ob sich die Klagebefugnis auch aus sonstigen Vorschriften über die Errichtung des beA oder aus einem Eingriff in die Berufsausübungsfreiheit nach Art. 12 Abs. 1 GG ergeben würde, wie die Kläger meinen, kommt es deshalb nicht an.

22 2. Die Klage ist unbegründet. Den Klägern steht weder ein Anspruch darauf zu, dass die Beklagte es unterlässt, das besondere elektronische Anwaltspostfach ohne die von ihnen geforderte Ende-zu-Ende-Verschlüsselung, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaber befinden, zu betreiben, noch ein Anspruch auf ein Betreiben mit genau einer solchen Verschlüsselung.

23 a) Der mit Klageantrag zu 1 geltend gemachte Unterlassungsanspruch besteht nicht.

24 Ein öffentlich-rechtlicher Abwehr- und Unterlassungsanspruch setzt voraus, dass durch eine hoheitliche Maßnahme rechtswidrig in ein subjektiv-öf-

fentliches Recht eingegriffen wird oder zu werden droht, wobei sich das subjektive Recht aus den Grundrechten oder aus einfachem Recht ergeben kann (vgl. Detterbeck/Windthorst/Sproll, Staatshaftungsrecht, § 13 Rn. 12 und 17; Ossenbühl/Cornils, Staatshaftungsrecht, 6. Aufl., S. 373 f.).

25 Diese Voraussetzungen liegen nicht vor. Zwar erfüllt das von der Beklagten eingerichtete System der Nachrichtenübermittlung nicht die Anforderungen an eine Ende-zu-Ende-Verschlüsselung im Sinne der europäischen Patentschrift EP 0 877 507 B1 (hierzu nachfolgend unter aa). Darin liegt jedoch kein rechtswidriger Eingriff in ein subjektiv-öffentliches Recht der Kläger. Denn weder steht den Klägern ein einfachgesetzlich normiertes Recht darauf zu, dass die über das besondere elektronische Anwaltspostfach übermittelten Nachrichten mit einer Ende-zu-Ende-Verschlüsselung in diesem Sinne gesichert werden, noch greift das Betreiben des besonderen elektronischen Anwaltspostfachs ohne Ende-zu-Ende-Verschlüsselung in diesem Sinne rechtswidrig in Grundrechte der Kläger, insbesondere in die von Art. 12 Abs. 1 GG geschützte Berufsausübungsfreiheit, ein (hierzu unter bb).

26 aa) Das von der Beklagten verwendete Verschlüsselungs-System entspricht nicht einer Ende-zu-Ende-Verschlüsselung im Sinne der europäischen Patentschrift (EP 0 877 507 B 1, abrufbar unter: https://register.epo.org/application?number=EP98108118).

27 (a) Charakteristisch für eine Ende-zu-Ende-Verschlüsselung in diesem Sinne ist die Verschlüsselung der Informationen am Ort des Senders und die Entschlüsselung erst beim Empfänger einer Nachricht, wobei der dazwischenliegende Kommunikationskanal keinen Einfluss auf die Chiffrierung besitzt. Innerhalb der digitalen Übertragungskette existiert keine Möglichkeit zur Umwandlung der Nachricht in den ursprünglichen Klartext. Für die Verschlüsselung wird ein symmetrisches Verschlüsselungsverfahren angewendet und der dafür benötigte geheime Schlüssel wird mittels eines asymmetrischen Verschlüsselungsverfahrens zwischen den Kommunikationspartnern ausgetauscht. Einer der Teilnehmer

generiert den geheimen Schlüssel, verschlüsselt diesen mit dem öffentlichen Teil eines privaten Schlüssels des anderen Teilnehmers und übergibt ihn über das Kommunikationssystem an den zweiten Teilnehmer. Dieser entschlüsselt die übergebene, verschlüsselte Größe mit dem geheimen Teil seines Schlüssels und erhält so den geheimen Schlüssel für die Ende-zu-Ende-Verschlüsselung. Die Schlüssel der Ende-zu-Ende-Verschlüsselung sollen dabei zu keiner Zeit außerhalb einer sicheren Umgebung im Klartext erscheinen. Als sichere Umgebung gelten dabei nur die sender- und empfängerseitigen Kommunikationseinrichtungen (Europäische Patentschrift, aaO Rn. [0002], [0004] und [0005]). Die Entschlüsselung des die Nachricht verschlüsselnden Schlüssels erfolgt mithin hiernach bei dem Empfänger der Nachricht mit dessen privatem Schlüssel, der sich ausschließlich in seiner Verfügungsgewalt befindet.

28 (b) Diesen Erfordernissen entspricht der im Rahmen des besonderen elektronischen Anwaltspostfachs verwendete Übermittlungsweg nicht vollständig.

29 (1) Eingehalten ist allerdings - entgegen der Auffassung der Kläger - das Erfordernis, dass die übermittelten Inhalte durchgehend mit demselben Schlüssel verschlüsselt sind, während der gesamten Übertragung durchgängig verschlüsselt bleiben und nur beim Sender und Empfänger unverschlüsselt vorliegen. Weder werden die Nachrichten selbst im HSM umgeschlüsselt noch werden Nachrichten vor der Entschlüsselung durch den berechtigten Empfänger auf dem Übertragungsweg entschlüsselt.

30 Die Beklagte hat den Übermittlungsweg der Nachrichten und das Verschlüsselungssystem mittels des S. -Gutachtens sowie der von der technischen Entwicklerin des beA, der Firma A. GmbH (im Folgenden: A.) erstellten Schaubilder, vorgelegt von der Beklagten als Anlagen A 3a bis 3c, im Detail dargestellt. Hieraus ergibt sich, dass eingehende Nachrichten in verschlüsseltem Zustand direkt an das Postfach des Empfängers und von dort an den jeweils berechtigten Leser weitergeleitet werden, ohne dass diese zu

irgendeinem Zeitpunkt entschlüsselt werden. Umgeschlüsselt wird nur der Nachrichtenschlüssel, mit dem die Nachricht verschlüsselt ist.

31 Es bestehen keine Anhaltspunkte dafür, dass diese Grundstruktur der Übermittlung und Verschlüsselung von Nachrichten über das besondere elektronische Anwaltspostfach in dem S. -Gutachten sowie den von der Betreiberin erstellten Schaubildern unzutreffend dargestellt wäre. Die Kläger haben diese Grundstruktur nicht in Frage gestellt, sondern ihrerseits mehrfach auf das S. -Gutachten Bezug genommen sowie Anlagen vorgelegt, die diese Grundstruktur bestätigen, zum Beispiel als Anlage K 16 einen Artikel von Hanno Böck vom 26. Januar 2018 (www.golem.de), in dem ein Schaubild der A. zur Struktur des Nachrichtenabrufs enthalten ist, aus dem die verschlüsselte Übermittlung der Nachricht aus dem Postfach an den Client ohne Umweg über das HSM sowie die Umschlüsselung lediglich des den Nachrichtenschlüssel verschlüsselnden Schlüssels im HSM hervorgeht. Auch den von den Klägern vorgelegten Unterlagen zum Vortrag von Professor Dr. Frederik Armknecht bei einem Symposium des Deutschen EDV-Gerichtstags zum besonderen elektronischen Anwaltspostfach am 5. März 2018 (vorgelegt als Anlage K 29) ist zu entnehmen, dass eine Umschlüsselung nur des Nachrichtenschlüssels im HSM erfolgt, nicht aber der Nachricht selbst.

32 (1.1) Im Hinblick auf die dargelegte, im Grundsatz unstreitige Struktur der Nachrichtenübermittlung und -verschlüsselung bestehen keine Anhaltspunkte dafür, dass die Nachricht selbst auf dem Übermittlungsweg vom Sender zum Empfänger der Nachricht umgeschlüsselt wird. Die Kläger haben dies zwar in erster Instanz behauptet. Konkrete Anhaltspunkte hierfür sind indes auch dem Klägervortrag nicht zu entnehmen. Im Berufungsverfahren haben die Kläger im Gegenteil selbst vorgetragen, dass im beA nicht die Nachricht, sondern der Verschlüsselungs-Schlüssel der Nachricht entschlüsselt und erneut verschlüsselt werde.

33 (1.2) Keine Anhaltspunkte bestehen auch dafür, dass die Nachrichten nicht durchgängig bis zur Entschlüsselung durch den berechtigten Empfänger verschlüsselt sind. Das S. -Gutachten bestätigt, dass Nachrichtenhinhalte unverschlüsselt nur bei den Kommunikationspartnern vorliegen (S. -Gutachten, S. 11). Die Kläger bestreiten dies zwar. Der betreffende Vortrag ist indes nicht geeignet, die diesbezüglichen Ausführungen im S. -Gutachten in Frage zu stellen. Die Kläger stützen sich insoweit ausschließlich auf einen Beitrag von Hanno Böck vom 10. September 2018 auf golem.de, der sich mit einer im S. -Gutachten unter Punkt 5.4.1. benannten, als betriebsverhindernd kategorisierten A-Schwachstelle und einer Stellungnahme der Beklagten hierzu befasst. S. hatte insoweit beanstandet, dass die beA-Client-Security aus mehreren Teilen bestehe, von denen ein Teil als Javascript-Code vom beA-Server ausgeliefert werde, welcher im Browser des Nutzers ausgeführt werde. Dieser Teil steuere die beA-Client-Security, welche für Verschlüsselung, Entschlüsselung und Authentisierung zuständig sei. Ein Innentäter könne diesen Code in der Absicht modifizieren, Nachrichten beim Versenden unverschlüsselt in eine beliebige Richtung zu versenden (S. -Gutachten, S. 80 unter 5.4.1).

34 Insoweit ging es mithin um eine Sicherheitslücke, die bei einem Angriff durch einen Innentäter dahingehend hätte ausgenutzt werden können, dass Nachrichten unverschlüsselt versendet werden. Unverschlüsselt wären solche Nachrichten mithin nur dann, wenn ein Innentäter das beA-System bewusst und gezielt angreifen würde. Dies ist indes kein geeigneter Maßstab für die Frage, ob das beA seiner Struktur nach eine Verschlüsselung vorsieht, die sicherstellt, dass Nachrichten beim Versender verschlüsselt und erst bei dem berechtigten Empfänger wieder entschlüsselt werden. Die betreffende Sicherheitslücke ändert nichts daran, dass die Nachrichten grundsätzlich und im Normalbetrieb verschlüsselt übertragen und auf dem Übertragungsweg nicht entschlüsselt werden.

35 Die Stellungnahme der Beklagten zu dieser Schwachstelle, die die Kläger dem von ihnen vorgelegten Beitrag von Hanno Böck entnehmen und die die Aus-

sage enthält, dass der Schutzbedarf des begleitenden Nachrichtentextes hinsichtlich der Vertraulichkeit aus fachlicher Sicht als deutlich geringer einzustufen sei als der Schutzbedarf der Anhänge, bezieht sich ebenso nur auf dieses Angriffsszenarium und besagt nicht, dass der begleitende Nachrichtentext grundsätzlich im Normalbetrieb unverschlüsselt ist.

36 Abgesehen davon hat die Beklagte vorgetragen, dass alle A-Schwachstellen vor der Wiederinbetriebnahme des beA am 3. September 2018 behoben worden sind und S. dies begutachtet und bestätigt habe. Aus der von der Beklagten vorgelegten Bestätigung der S. ergibt sich, dass diese sogenannte ReTests der im S. -Gutachten aufgeführten Schwachstellen durchgeführt hat. Zu der dort unter Punkt 5.4.1 genannten A-Schwachstelle heißt es, diese sei verifiziert und behoben. Das vom Hersteller vorgelegte Konzept zur technischen Umsetzung werde als hinreichend sicherer Lösungsvorschlag bewertet. Anhaltspunkte dafür, dass dies nicht zutrifft, bestehen nicht und werden von Klägerseite auch nicht vorgebracht.

37 Auch das aus Sicht der Kläger entscheidende Sicherheitsrisiko, dass die maßgeblichen Schlüssel als verschlüsselte Datei auch außerhalb des HSM vorliegen und hiermit bei missbräuchlicher Verwendung seitens der Beklagten oder der Betreiberin alle Nachrichten entschlüsselt werden könnten, ist für die Beantwortung der Frage, ob die Nachrichten im vorgesehenen Regelbetrieb durchgehend verschlüsselt sind, ohne Bedeutung (siehe zu dieser Schwachstelle unten unter 2 a bb (b) (2.2)).

38 (2) Im Unterschied zu dem in der europäischen Patentschrift dargelegten Verfahren der Ende-zu-Ende-Verschlüsselung wird bei dem von der Beklagten errichteten System der die Nachricht verschlüsselnde Schlüssel allerdings nicht direkt an den Empfänger übermittelt und dort entschlüsselt. Vielmehr wird er mit dem in dem externen HSM hinterlegten privaten Postfachschlüssel des Empfängers entschlüsselt und dort im Ergebnis auf den Schlüssel des oder der leseberechtigten Nutzer umgeschlüsselt. Durch diese Umschlüsselung des Schlüssels

und die hierfür erforderliche Hinterlegung des privaten Postfachschlüssels im HSM ist die der patentierten Ende-zu-Ende-Verschlüsselung immanente Voraussetzung, dass sich die Schlüssel nur bei den Kommunikationspartnern befinden, nicht erfüllt.

39 bb) Den Klägern steht indes kein Anspruch darauf zu, dass die von der Beklagten gewählte Verschlüsselung unterlassen wird, weil sie keine Ende-zu-Ende-Verschlüsselung in oben genanntem Sinne darstellt. Denn die Beklagte war weder nach den einfachgesetzlich normierten Vorgaben noch von Verfassungs wegen verpflichtet, eine derartige Verschlüsselung vorzusehen, so dass durch deren Unterlassen nicht in ein subjektiv-öffentliches Recht der Kläger eingegriffen wird.

40 (a) Aus § 31a Abs. 1 oder 3 BRAO, § 130a Abs. 4 Nr. 2 ZPO und § 174 Abs. 3 Satz 3 und 4 ZPO ergeben sich keine detaillierten Vorgaben für die Bewerkstelligung der Sicherheit der Nachrichtenübermittlung, insbesondere keine Verpflichtung zur Nutzung einer Ende-zu-Ende-Verschlüsselung in oben genanntem Sinne. Denn diese Vorschriften enthalten keine Vorgaben zur technischen Ausgestaltung im Hinblick auf die Sicherheit der Nachrichtenübermittlung, so dass sie den Klägern auch keinen Anspruch auf eine bestimmte Verschlüsselung der zu versendenden Inhalte gewähren.

41 (1) Aus § 31a Abs. 1 Satz 1 BRAO ergibt sich lediglich die Verpflichtung der Beklagten zur empfangsbereiten Einrichtung eines besonderen elektronischen Anwaltspostfachs. Vorgaben für besondere technische Sicherheitsstandards ergeben sich hieraus dagegen nicht.

42 (2) Nach § 31a Abs. 3 Satz 1 BRAO hat die Beklagte sicherzustellen, dass der Zugang zum beA nur durch ein sicheres Verfahren mit zwei voneinander unabhängigen Sicherungsmitteln möglich ist. Die Norm regelt nur die Sicherheit des Zugangs zum Postfach, nicht jedoch die hier streitgegenständliche Sicherheit der Datenübermittlung.

43 (3) § 130a Abs. 4 Nr. 2 ZPO, wonach der Übermittlungsweg zwischen dem besonderen elektronischen Anwaltspostfach und der elektronischen Poststelle des Gerichts als sicher gilt, begründet eine gesetzliche Fallgruppe eines im verfahrensrechtlichen Sinne als sicher geltenden Übermittlungsweges und stellt damit klar, dass Anwälte, die das besondere elektronische Anwaltspostfach nutzen, den Verpflichtungen aus § 130a Abs. 3 ZPO zur Übermittlung über einen sicheren Übermittlungsweg sowie aus § 174 Abs. 3 Satz 4 ZPO zur Eröffnung eines sicheren Übermittlungswegs nachkommen. Aussagen zur technischen Ausgestaltung des besonderen elektronischen Anwaltspostfachs enthält die Vorschrift ebenso wenig, wie sie den Nutzern einen Anspruch auf eine bestimmte Struktur und Technik zuspricht.

44 (4) Nichts Anderes gilt für § 174 Abs. 3 Satz 3 und 4 ZPO. Hieraus ergibt sich - ohne Bezug zum besonderen elektronischen Anwaltspostfach und dessen Sicherheit - lediglich die Verpflichtung, dass eine Zustellung an einen Anwalt beziehungsweise eine der weiteren in § 174 Abs. 1 ZPO genannten Personengruppen über einen sicheren Übermittlungsweg im Sinne des § 130a Abs. 4 ZPO zu erfolgen hat. Zugleich sind die in § 174 Abs. 1 ZPO genannten Personengruppen verpflichtet, einen sicheren Übermittlungsweg für die Zustellung elektronischer Dokumente zu eröffnen. Der Verweis unter anderem auf das besondere elektronische Anwaltspostfach in § 130a Abs. 4 Nr. 2 ZPO stellt dabei klar, dass dieses nach der Auffassung des Gesetzgebers ein zulässiger sicherer Übermittlungsweg ist.

45 Entgegen der Auffassung der Kläger ist auch der Gesetzesbegründung zu § 174 Abs. 3 Satz 3 ZPO nichts dafür zu entnehmen, dass der Gesetzgeber das elektronische Anwaltspostfach nur mit einer Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne zulassen wollte. § 174 Abs. 3 Satz 3 ZPO regelt, dass eine elektronische Zustellung auf einem sicheren Übermittlungsweg im Sinne von § 130a Abs. 4 ZPO zu erfolgen hat. Diese Regelung wurde durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (BGBl. I S. 3786) eingefügt. Der Bundesrat

hatte in seiner Stellungnahme hierzu vorgeschlagen, dass die Bezugnahme in § 174 Abs. 3 Satz 3 und 4 ZPO-E auf "sichere Übermittlungswege im Sinne des § 130a Abs. 4 ZPO-E" entfallen solle, um eine Beschränkung auf die dort genannten Übermittlungswege zu verhindern (BT-Drucks. 17/12634, S. 46).

46 In diesem Zusammenhang steht die von den Klägern in Bezug genommene Passage der Stellungnahme des Bundesrats, wonach die vorgeschlagene Streichung der Bezugnahme auf "sichere Übermittlungswege" im Sinne des § 130a Abs. 4 ZPO-E nicht etwa zur Zulassung unsicherer Übertragungswege führe, da die Anforderung, die Übermittlung "gegen unbefugte Kenntnisnahme Dritter zu schützen", bestehen bleibe und diese beim Einsatz der EGVP-Infrastruktur durch die automatisierte (Ende-zu-Ende-)Verschlüsselung der Daten über das sogenannte OSCI-Protokoll gewährleistet werde (BT-Drucks. 17/12634, S. 46 f.). Abgesehen davon, dass sich die Stellungnahme des Bundesrates nicht auf die Übermittlung mittels des besonderen elektronischen Anwaltspostfachs, sondern im Gegenteil gerade auf die Übermittlung ohne dessen Nutzung bezieht und sich zur technischen Ausgestaltung des besonderen elektronischen Anwaltspostfachs nicht verhält, ist der Änderungsvorschlag des Bundesrats ohnehin nicht übernommen worden. Dessen Stellungnahme bezieht sich mithin auf einen nicht Gesetz gewordenen Regelungsvorschlag und kann schon deshalb zur Ermittlung des Willens des Gesetzgebers nicht herangezogen werden.

47 (b) Eine Verpflichtung zur Verschlüsselung der über besondere elektronische Anwaltspostfächer übermittelten Inhalte durch eine Ende-zu-Ende-Verschlüsselung, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaber befinden und keine Umschlüsselung im HSM stattfindet, ist entgegen der Auffassung der Kläger auch der Rechtsanwaltsverzeichnis- und -postfachverordnung nicht zu entnehmen. Diese Verordnung regelt auf Grundlage von § 31c Nr. 3 BRAO unter anderem Einzelheiten der Einrichtung, der technischen Ausgestaltung, der Führung, der Zugangsberechtigung und der Nutzung der elektronischen Anwaltspostfächer.

48 Nach § 19 Abs. 1 RAVPV dient das besondere elektronische Anwaltspostfach insbesondere der elektronischen Kommunikation mit den Gerichten sowie der Nutzer untereinander auf einem sicheren Übermittlungsweg. Nach § 20 Abs. 1 RAVPV hat die Bundesrechtsanwaltskammer die besonderen elektronischen Anwaltspostfächer auf der Grundlage des Protokollstandards "Online Services Computer Interface - OSCI" oder einem künftig nach dem Stand der Technik an dessen Stelle tretenden Standard zu betreiben und fortlaufend zu gewährleisten, dass die in § 19 Abs. 1 RAVPV genannten Personen und Stellen miteinander sicher elektronisch kommunizieren können.

49 Eine Verpflichtung, im Rahmen des beA eine Ende-zu-Ende-Verschlüsselung in oben genanntem Sinne vorzusehen, enthalten diese Vorschriften nicht. Dies ergibt sich weder aus dem Erfordernis einer sicheren Kommunikation noch aus dem Verweis auf die OSCI-Protokollstandards in § 20 Abs. 1 RAVPV.

50 (1) Die unbestimmten Rechtsbegriffe "sicherer Übermittlungsweg" und "sichere Kommunikation" sind weder in § 19 Abs. 1 RAVPV und § 20 Abs. 1 RAVPV noch an anderer Stelle der Rechtsanwaltsverzeichnis- und -postfachverordnung näher definiert. Sie sind jedenfalls nicht dahingehend auszulegen, dass damit ausschließlich eine Übermittlung mittels einer Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne gemeint ist.

51 (1.1) Der Wortlaut impliziert eine technische Offenheit. Ihm ist nicht zu entnehmen, dass nur eine bestimmte Verschlüsselungsart als sicherer Übermittlungsweg anzusehen ist, vielmehr wird neutral und ohne technische Vorgaben allein auf das ausfüllungsbedürftige Kriterium der Sicherheit abgestellt. Dies spricht dafür, dass für die technische Umsetzung im Detail ein Spielraum besteht, sofern das Kriterium der Sicherheit beachtet wird.

52 (1.2) Sinn und Zweck der Vorschrift bestätigen ebenfalls die technische Offenheit und sprechen gegen eine Festlegung auf eine bestimmte Verschlüsselungstechnik. Bezweckt ist mit diesen Regelungen, dass ein zuverlässiges und sicheres Kommunikationsmittel für den elektronischen Rechtsverkehr zwischen

den Rechtsanwälten und Gerichten sowie zwischen den Rechtsanwälten untereinander zur Verfügung gestellt wird (Begründung zu § 19 RAVPV, BR-Drucks. 417/16, S. 34). Dieser Vorgabe ist nicht zu entnehmen, dass zwingend eine Ende-zu-Ende-Verschlüsselung nach oben genannten Kriterien gegeben sein muss. Die offen gefasste, lediglich auf den Begriff der Sicherheit abstellende Formulierung erlaubt der Beklagten, durch ein technisches Gesamtkonzept den besonderen Erfordernissen der Kommunikation über besondere elektronische Anwaltspostfächer in ihrer Gesamtheit Rechnung zu tragen. Wie aus § 20 Abs. 1 Satz 1 Halbs. 2 RAVPV und § 20 Abs. 1 Satz 2 RAVPV hervorgeht, steht der Beklagten hierbei ein Spielraum zur Anpassung an technische Neuerungen zu.

53 (1.3) Auch die Systematik spricht dafür, dass der Verordnungsgeber die konkrete Art der Verschlüsselung nicht abschließend zugunsten einer bestimmten technischen Lösung regeln, sondern der Beklagten hinsichtlich der technischen Umsetzung einen gewissen Spielraum belassen wollte, solange gemessen am aktuellen Stand der Technik eine sichere Kommunikation gewährleistet ist. Das von der Beklagten zu errichtende System hat nicht nur den Erfordernissen einer sicheren Kommunikation zwischen zwei Kommunikationspartnern zu genügen, sondern muss auch eine Nutzung durch Vertreter, Abwickler und Zustellungsbevollmächtigte ermöglichen (§ 31a Abs. 3 Satz 2 BRAO, § 25 RAVPV) und den vom Postfachinhaber Dritten nach § 23 RAVPV gewährten Zugang zu seinem besonderen elektronischen Postfach sicher regeln. Die Verordnung bestimmt das technische Gesamtkonzept nicht in allen Details, sondern belässt der Beklagten einen Umsetzungsspielraum, wobei vorgegeben wird, durch wen und wozu das System nutzbar sein und welcher Mindeststandard eingehalten sein muss (vgl. für einen Spielraum z.B. § 22 Abs. 3 RAVPV, § 23 Abs. 1 RAVPV und § 24 Abs. 1 RAVPV). Zugleich hat der Verordnungsgeber an anderer Stelle teils sehr konkrete Vorgaben gemacht (vgl. z.B. § 25 Abs. 3 RAVPV). Dem ist zu entnehmen, dass der Verordnungsgeber bewusst teils sehr konkrete Vorgaben in den Verordnungstext aufgenommen hat, an anderer Stelle aber Spielraum für die

technische Umsetzung unter Einhaltung der im Verordnungstext vorgesehenen Standards gewährt.

54 Die technische Nachrichtenübermittlung nach § 20 RAVPV zählt zu den Regelungen, bei denen der Verordnungsgeber erkennbar zwar einen bestimmten Rahmen gesteckt, innerhalb dieses Rahmens jedoch keine detaillierten technischen Vorgaben formuliert hat. Diese Offenheit auch für künftige Entwicklungen zeigt sich unter anderem darin, dass in § 20 Abs. 1 RAVPV auf den OSCI-Standard oder einen künftig nach dem Stand der Technik an dessen Stelle tretenden Standard verwiesen wird. Eine Festlegung auf ein Detail des Gesamtprozesses - wie eine Ende-zu-Ende-Verschlüsselung im Sinne der europäischen Patentschrift EP 0 877 507 B 1 vom 26. September 2007 - widerspräche dem, zumal der Verordnungsgeber die von den Klägern befürwortete Nachrichtenverschlüsselung im Sinne der bei Erlass der Verordnung bereits über einen Zeitraum von 9 Jahren bestehenden europäischen Patentschrift ohne Weiteres verbindlich in § 20 Abs. 1 RAVPV hätte vorgeben können, wenn er dies gewollt hätte. Auch dies spricht dafür, dass der Verordnungsgeber mit Rücksicht auf die technische Komplexität des Gesamtsystems sowie die fortlaufende Weiterentwicklung im Bereich der elektronischen Kommunikation eine technische Offenheit gewährleisten wollte, die es bewusst vermeidet, die Beklagte auf eine bestimmte technische Lösung festzulegen.

55 (1.4) Die historische Entwicklung der RAVPV zeigt, dass dem Verordnungsgeber bei deren Verabschiedung bereits das später in die Praxis umgesetzte System der besonderen elektronischen Anwaltspostfächer bekannt war und dieses von ihm gebilligt und damit als sicherer Kommunikationsweg angesehen wurde. Die Beklagte hat unwidersprochen vorgetragen, dass im Zeitpunkt des Erlasses von §§ 19 und 20 RAVPV die von den Klägern kritisierte Architektur des besonderen elektronischen Anwaltspostfachs einschließlich der Umschlüsselung des Schlüssels im HSM bereits feststand und sie diese immer wieder mit den zuständigen Referatsleitern des Bundesministeriums der Justiz und für Verbraucherschutz erörtert hat. Auch die Kläger gehen davon aus, dass sich das

Ministerium über Jahre hinweg in einem stetigen Austausch mit der Beklagten befand.

56 Der zeitliche Ablauf bestätig dies: Der Entwurf der Verordnung wurde dem Bundesrat am 9. August 2016 zur Zustimmung zugeleitet (vgl. BR-Drucks. 417/16, Anschreiben an den Präsidenten des Bundesrates). Die Verordnung stammt vom 23. September 2016 (BGBl. I S. 2167). Der Verordnungsgeber ging dabei von einem Start des besonderen elektronischen Anwaltspostfachs am 29. September 2016 aus (BR-Drucks. 417/16, S. 18). Dies zeigt, dass die Verordnung in einem Zeitpunkt erstellt wurde, zu dem die Struktur des besonderen elektronischen Anwaltspostfachs bereits feststand. Denn eine Entwicklung des Gesamtkonzepts innerhalb des kurzen Zeitraums zwischen dem Entwurf der Verordnung, deren Erlass und dem avisierten Start des besonderen elektronischen Anwaltspostfachs ist ausgesprochen fernliegend und wird von den Klägern auch nicht behauptet. Dies deckt sich mit den von der Beklagten als Anlagen A 3a bis 3c vorgelegten, von der Firma A. erstellten Schaubildern zur beA-Verschlüsselung aus dem Jahr 2014, aus denen bereits die heute verwirklichte Grundstruktur der Nachrichtenübermittlung einschließlich der Verwendung des HSM hervorgeht.

57 Die Kenntnis des Verordnungsgebers von der bereits erarbeiteten Grundstruktur des besonderen elektronischen Anwaltspostfachs unter Einschluss des HSM vor Erlass der Verordnung spricht dafür, dass der Verordnungsgeber diese Struktur gebilligt hat und diese von seinem Willen umfasst ist. Dies gilt umso mehr, als er in keiner Weise im Rahmen der Verordnung oder deren Begründung zum Ausdruck gebracht hat, dass gegen das damals bereits erarbeitete System bezüglich des vorgesehenen Übermittlungswegs von Nachrichten unter Umschlüsselung des zur Verschlüsselung der Inhalte verwendeten Schlüssels im HSM Bedenken bestehen. Hieraus folgt zugleich, dass der Verordnungsgeber durch die Verwendung der Begriffe "sichere Kommunikation" und "sicherer Übermittlungsweg" nicht ausschließlich eine Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne gemeint hat.

58 (1.5) Nichts Anderes ergibt sich aus den Gesetzesmaterialien.

59 Unstreitig ist zwischen den Parteien, dass die Beklagte bis Februar 2018 öffentlich davon sprach, dass das besondere elektronische Anwaltspostfach eine "Ende-zu-Ende-Verschlüsselung" der Nachrichten vorsehe, obgleich die gewählte Struktur wegen der Umschlüsselung der Schlüssel im HSM nicht der Definition einer Ende-zu-Ende-Verschlüsselung im Sinne des europäischen Patents entsprach (vgl. hierzu oben 2.a.aa). Anhaltspunkte dafür, dass die Beklagte diesen Begriff etwa zur Täuschung des Bundesministeriums der Justiz und für Verbraucherschutz als Verordnungsgeber, der Anwaltschaft oder der allgemeinen Öffentlichkeit über die Sicherheit des Systems bewusst unzutreffend eingesetzt hätte, wie dies die Kläger behaupten, bestehen nicht. Im Gegenteil spricht Vieles dafür, dass mit der Verwendung des Begriffs "Ende-zu-Ende-Verschlüsselung" - zutreffend - vermittelt werden sollte, dass die Nachrichten und Inhalte verschlüsselt übertragen werden, durchgehend verschlüsselt bleiben und nur von dem berechtigten Empfänger entschlüsselt werden können. Dies ist der Kern einer jeden Ende-zu-Ende-Verschlüsselung und die allgemeine Erwartungshaltung an eine derartige Verschlüsselung. Der Unterschied der beA-Struktur zu einer solchen ist, dass sich der Schlüssel, mit dem die Nachricht entschlüsselt wird, bei der Ende-zu-Ende-Verschlüsselung im Sinne der europäischen Patentierung ausschließlich in der Verfügungsgewalt des Empfängers befindet, während bei der von der Beklagten gewählten Struktur der Schlüssel im HSM umgeschlüsselt wird auf die Schlüssel der jeweiligen Leseberechtigten, die diesen in der Folge mittels ausschließlich in ihrer Verfügungsgewalt befindlicher Schlüssel entschlüsseln können. Im Hinblick darauf, dass ein wesentliches Kernelement der Ende-zu-Ende-Verschlüsselung eingehalten war und die Beklagte zugleich das vorgesehene Verschlüsselungssystem und die Verwendung eines HSM öffentlich bekannt gemacht und auf Kammerversammlungen und Veranstaltungen des EDV-Gerichtstags erläutert hat, hält der Senat eine bewusste Täuschung durch die Beklagte für fernliegend.

60 Vor diesem Hintergrund ist § 20 RAVPV eine Verpflichtung zur Ende-zu-Ende-Verschlüsselung ohne Verwendung des HSM auch nicht deshalb zu entnehmen, weil der Verordnungsgeber in seiner Begründung zu § 20 Abs. 1 RAVPV sowie zu § 19 Abs. 2 RAVPV die Ende-zu-Ende-Verschlüsselung erwähnt hat. So wird in der Begründung zu § 20 Abs. 1 RAVPV ausgeführt, dass der Betrieb der besonderen elektronischen Anwaltspostfächer zur Gewährleistung einer sicheren Kommunikation mit Ende-zu-Ende-Verschlüsselung 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 hat (BR-Drucks. 417/16, S. 35). In der Begründung zu § 19 Abs. 2 RAVPV heißt es zur künftigen Ermöglichung einer Kommunikation auch mit Dritten über besondere elektronische Anwaltspostfächer, dass dies insbesondere die Kommunikationsmöglichkeiten erfassen könne, die bereits jetzt in der Struktur des Elektronischen Gerichts- und Verwaltungspostfachs (EGVP), in die auch das besondere elektronische Anwaltspostfach eingebettet sei, vorgesehen seien. Soweit auch dabei stets die Beachtung der elementaren Grundelemente des besonderen elektronischen Anwaltspostfachs (wie beispielsweise die Ende-zu-Ende-Verschlüsselung von Nachrichten) sichergestellt sein müsse, werde dies dadurch gewährleistet, dass auch für die Kommunikation mit anderen Stellen und Personen die Vorgaben des § 20 Abs. 1 RAVPV gelten würden.

61 Es ist indes nicht davon auszugehen, dass der Verordnungsgeber durch die Verwendung des Begriffs "Ende-zu-Ende-Verschlüsselung" das von der Beklagten erstellte, ihm bekannte Konzept für unzulässig erklären und die Einhaltung einer Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne vorschreiben wollte. Vielmehr spricht alles dafür, dass der Verordnungsgeber der öffentlich bis 2018 von der Bundesrechtsanwaltskammer verwendeten, technisch ungenauen Begrifflichkeit einer "Ende-zu-Ende-Verschlüsselung" gefolgt ist und hiermit auch das bereits konzipierte Verfahren gemeint hat, bei dem die Nachrichten verschlüsselt übertragen und nur vom berechtigten Empfänger entschlüsselt werden können, während die Schlüssel im HSM umgeschlüsselt

werden. Die gewählte Formulierung "Ende-zu-Ende-Verschlüsselung von Nachrichten" in der Begründung zu § 19 RAVPV bestätigt diesen Fokus auf die Verschlüsselung der Nachricht an sich, also des Inhalts.

62 Der Senat hält es für ausgeschlossen, dass der Verordnungsgeber allein durch eine nicht in den Verordnungstext aufgenommene Formulierung in der Begründung des Verordnungsentwurfs abweichend von dem ihm bekannten und veröffentlichten Verschlüsselungskonzept unter Einschluss des HSM eine Ende-zu-Ende-Verschlüsselung im Sinne der europäischen Patentschrift vorgeben wollte. Denn eine solche Vorgabe hätte zur Folge gehabt, dass das besondere elektronische Anwaltspostfach in der konzipierten Form nicht hätte in Betrieb genommen werden können und die Grundstruktur grundlegend hätte überarbeitet werden müssen. Es ist anzunehmen, dass der Verordnungsgeber derart gravierende Folgen ausdrücklich thematisiert und kommuniziert hätte, wären diese beabsichtigt gewesen.

63 (1.6) Eine verfassungskonforme Auslegung von §§ 19 und 20 RAVPV dahingehend, dass zwingend eine Ende-zu-Ende-Verschlüsselung im Sinne der europäischen Patentschrift vorzusehen ist, ist nicht geboten. Es genügt den verfassungsrechtlichen Anforderungen, dass die einschlägigen Normen dem Grunde nach ein sicheres Übermittlungsverfahren vorschreiben. Hierdurch ist dem rechtlich geschützten Vertrauensverhältnis zwischen Rechtsanwalt und Mandant (vgl. hierzu BVerfGE 113, 29, 49; Beschluss vom 29. Januar 2015 - 2 BvR 497/12, juris Rn. 18) in ausreichendem Maße Rechnung getragen. Es steht dem Gesetzgeber frei, die technische Konkretisierung des gesetzlich vorgegebenen Maßstabs der Beklagten als Körperschaft des öffentlichen Rechts anzuvertrauen (vgl. für Aufsichtsbehörden im Bereich der Telekommunikation: BVerfGE 125, 260, 327).

64 Entgegen der Auffassung der Kläger ergibt sich auch aus dem Nichtannahmebeschluss des Bundesverfassungsgerichts vom 20. Dezember 2017

(1 BvR 2233/17, juris) nicht, dass §§ 19 und 20 RAVPV verfassungskonform dahingehend auszulegen wären, dass das beA eine Ende-zu-Ende-Verschlüsselung im Sinne der europäischen Patentschrift gewährleisten müsste. Zwar hat das Bundesverfassungsgericht in diesem Beschluss entsprechend der damals von der Beklagten verwendeten, in der Begründung zu § 20 Abs. 1 RAVPV enthaltenen Terminologie von einer Ende-zu-Ende-Verschlüsselung gesprochen. So führt das Bundesverfassungsgericht in diesem Beschluss unter Verweis auf § 20 Abs. 1 RAVPV aus, dass das beA zur sicheren Übermittlung eine so genannte Ende-zu-Ende-Verschlüsselung verwende (BVerfG, Beschluss vom 20. Dezember 2017, aaO Rn. 5). Weiter wird in der Begründung darauf abgestellt, dass es in der Beschwerdeschrift an einer Auseinandersetzung mit den konkret getroffenen Sicherheitsvorkehrungen wie etwa der Ende-zu-Ende-Verschlüsselung fehle (aaO Rn. 14). Damit ist indes nicht gesagt, dass das Bundesverfassungsgericht eine Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne für gegeben sowie für geboten erachtete. Mit den technischen Details der beA-Struktur hat sich das Bundesverfassungsgericht in diesem Beschluss nicht auseinandergesetzt. Erst Recht hat das Bundesverfassungsgericht weder - wie die Kläger meinen - § 20 Abs. 1 RAVPV dahingehend ausgelegt, dass die Beklagte eine Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne gewährleisten müsse noch hat es dies für verfassungsrechtlich geboten erklärt. Der Nichtannahmebeschluss, dem ohnehin als Prozessentscheidung keine Bindungswirkung im Sinne von § 31 Abs. 1 BVerfGG zukommt, befasst sich hiermit schon nicht.

65 (2) Die Beklagte war auch nicht deshalb gehalten, eine Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne unter Verzicht auf eine Umschlüsselung der Schlüssel im HSM vorzusehen, weil einzig hierdurch die von § 20 Abs. 1 RAVPV geforderte sichere Kommunikation gewährleistet werden könnte. Ein Erfolg der Klage unter dem Aspekt der Sicherheit der Kommunikation setzte dies indes voraus. Denn die Klage ist ausdrücklich nur darauf gerichtet, das weitere Betreiben des bestehenden Verschlüsselungssystems im

Hinblick auf die fehlende Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne zu unterlassen sowie das besondere elektronische Anwaltspostfach mit einer derartigen Verschlüsselung zu betreiben. Kann jedoch auch ein anderes System eine hinreichende Sicherheit gewährleisten, besteht kein Anspruch auf die von den Klägern geforderte Verschlüsselungstechnik. Eine sicherheitsrelevante Schwachstelle des bestehenden Systems könnte den von den Klägern geltend gemachten Anspruch auf Nutzung einer bestimmten Verschlüsselungstechnik nur dann begründen, wenn diese nicht behebbar wäre und damit eine fortlaufende Gefahr für die Sicherheit der Kommunikation darstellte. Denn nur in diesem Fall könnte diese Schwachstelle dazu führen, dass das gewählte System seiner Struktur nach keine sichere Kommunikation gewährleisten könnte und die Bundesrechtsanwaltskammer den ihr zustehenden Spielraum für die technische Gestaltung durch die gewählte Technik überschritten hätte. Der von den Klägern geltend gemachte Anspruch auf eine bestimmte Verschlüsselungstechnik könnte sich hieraus nur unter der weiteren Voraussetzung ergeben, dass nicht ein sonstiges hinreichend sicheres System existierte.

66 Es ist auf Grundlage des von beiden Parteien vorgelegen S. -Gutachtens sowie des Parteivorbringens davon auszugehen, dass - in Verbindung mit entsprechenden organisatorischen Sicherheitsvorkehrungen beim Betreiber des beA und der Beklagten - auch das von der Beklagten gewählte System in ausreichendem Maße die erforderliche sichere Kommunikation gewährleisten kann. Nicht behebbare Sicherheitsmängel ergeben sich weder aus dem Sachvortrag der Parteien noch sind sie sonst ersichtlich.

67 Sicherheit ist hierbei nicht im Sinne einer absoluten Sicherheit zu verstehen, die jegliches Risiko ausschließt. Eine solche Sicherheit existiert im Bereich der elektronischen Kommunikation nicht. Zu Recht hat der Anwaltsgerichtshof hierzu ausgeführt, dass Sicherheit nur ein relativer Zustand der Gefahrenfreiheit bedeutet, Beeinträchtigungen nicht vollständig ausgeschlossen werden können und stets ein Restrisiko eines Angriffs auf übermittelte Daten verbleibt.

68 Eine sichere Kommunikation im Rechtssinne setzt demnach nicht eine Freiheit von jeglichen Risiken voraus. Das gewählte Übermittlungssystem muss einen Sicherheitsstandard erreichen, bei dem unter Berücksichtigung der Funktionalität nach dem Stand der Technik die Übermittlung voraussichtlich störungs- und gefahrfrei erfolgt und Risiken für die Vertraulichkeit möglichst weitgehend ausgeschlossen werden. Dementsprechend hat der Anwaltsgerichtshof darauf abgestellt, dass Sicherheit erfordere, dass ein Schadenseintritt hinreichend unwahrscheinlich sei und insgesamt ein Zustand als sicher gelten könne, der unter Berücksichtigung der Funktionalität und Standards frei von unvertretbaren Risiken sei.

69 Der Senat teilt auf Grundlage des Sach- und Streitstandes die Auffassung des Anwaltsgerichtshofs, wonach die Übermittlung von Nachrichten unter Einsatz der besonderen elektronischen Anwaltspostfächer eine Sicherheit in diesem Sinne gewährleisten kann, wobei zu berücksichtigen ist, dass die für die Sicherheitsbeurteilung erforderliche Risikoermittlung und -bewertung stets eine Prognose über mögliche künftige Bedrohungen und deren Eintrittswahrscheinlichkeit bedingt und somit auch insoweit Unsicherheiten beinhaltet. Diese sind indes nicht vermeidbar und deshalb hinzunehmen, sofern die Einschätzung auf Grundlage fachwissenschaftlicher Maßstäbe methodisch fachgerecht erfolgte (vgl. BVerwG, NVwZ-RR 1991, 129, 131 für die Sicherheitsanforderungen beim Flughafenbau).

70 (2.1) Das S. -Gutachten kommt zu dem Ergebnis, dass das dem beA zugrundeliegende Verschlüsselungskonzept geeignet ist, die Vertraulichkeit der Nachrichten während der Übertragung und Speicherung durch das beA zu gewährleisten, auch gegenüber dem Betreiber des beA. Die Umverschlüsselung sei in einem HSM gekapselt und schütze daher dort vorübergehend entstehende Schlüsselinformationen in einer besonderen manipulations- und ausspähsicheren Umgebung (S. -Gutachten, S. 11).

71 Die im Rahmen der gutachterlichen Prüfung aufgezeigten, als betriebsverhindernd eingestuften Schwachstellen sind nach dem Vortrag der Beklagten vor

der Wiederinbetriebnahme des besonderen elektronischen Anwaltspostfachs beseitigt worden, was von der S. nach erneuter Begutachtung bestätigt wurde. Der entsprechenden Feststellung des Anwaltsgerichtshofs sind die Kläger in der Berufungsinstanz nicht entgegengetreten.

72 (2.2) Umstände, die trotz dieser fachwissenschaftlichen Sicherheitsüberprüfung einer Einstufung als sicher im Rechtssinne entgegenstehen und für die Annahme eines nicht hinreichend sicheren Kommunikationswegs sprechen würden, sind nicht ersichtlich. Sie ergeben sich auch nicht aus dem Vorbringen der Kläger. Diese halten es für das entscheidende Sicherheitsrisiko des beA, dass es möglich sei, mit einem einzigen Angriff anwaltliche und gerichtliche Korrespondenz heimlich auszuspähen. Die Kläger beziehen sich hierbei auf die im S. -Gutachten unter 5.5.3 dargelegte Schwachstelle. Dort wird bemängelt, dass die Arbeitsschlüssel, die das HSM zur verschlüsselten Ablage und zur Umverschlüsselung verwendet, sowie die diese Arbeitsschlüssel verschlüsselnden Key Encryption Keys (KEKs) auch außerhalb des HSM als verschlüsselte Datei vorliegen, da diese nach deren Erzeugung vom Betreiber des beA an die Beklagte als Auftraggeberin übergeben worden seien und dort verwahrt würden. Im S. -Gutachten heißt es hierzu, dass die Sicherheit der KEK durch Schlüsselteilung, physikalisch getrennte Verwahrung und physikalisch auf spezifische Mitarbeiter des Auftraggebers, die sogenannten Key Custodians, beschränkten Zugriff geschützt sei. Die beiden Teile des KEK, die nur zusammen die Entschlüsselung und das Einspielen der Master-Schlüssel in ein HSM erlaubten, seien auf Papier in versiegelten Briefumschlägen in Safes verwahrt (S. -Gutachten, S. 78). Wer sich allerdings in den Besitz des Schlüsselmaterials bringe, könne die im beA-System gespeicherten Nachrichten auch ohne HSM entschlüsseln. Der Missbrauch könne auf zwei Arten geschehen: Die Key Custodians der Beklagten und ein Helfer beim Betreiber des beA könnten den verschlüsselten Nachrichtenbestand und die Schlüssel zusammenbringen und dann die Nachrichten entschlüsseln. Die zweite Missbrauchsmöglichkeit sei gegeben, wenn beim Betreiber des beA nach der Erzeugung der Schlüssel und vor der Übergabe

an den Auftraggeber an einer Stelle eine Kopie erstellt worden sei. Dann könne das Personal des Betreibers alleine die Nachrichten entschlüsseln (S. -Gutachten, S. 86).

73 S. hat diese Schwachstelle als betriebsbehindernd eingeordnet. Die Bedrohung der Vertraulichkeit werde als hoch eingeschätzt, weil ein Angriff die umfassende Aufdeckung des Inhalts aller in beA-Postfächern gespeicherten Nachrichten erlaube. Die Ausnutzbarkeit werde dagegen als niedrig bewertet, weil der Angriff nur durch bestimmte Innentäter durchführbar sei, die dabei eine Vertrauensstellung haben müssten, die sie missbrauchten (S. -Gutachten, S. 86).

74 Bereits die von den Parteien nicht in Frage gestellte Schilderung der Manipulationsmöglichkeiten im S. -Gutachten zeigt, dass ein entsprechender Angriff zwar die Vertraulichkeit der Kommunikation in ganz erheblichem Maße verletzen würde, die Gefahr eines solchen Angriffs indes als gering einzustufen ist. Zum einen bedürfte es hierfür des Missbrauchs durch Innentäter, die eine besondere Vertrauensstellung innehaben. Anhaltspunkte für einen bereits im Zuge der damaligen Schlüsselerstellung und -übermittlung erfolgten Missbrauch seitens der Betreiberfirma bestehen nicht. Vor einem zukünftigen Angriff unter Verwendung der externen Schlüsselinformationen schützen erhebliche Sicherheitsvorkehrungen: Die für den Angriff erforderlichen, außerhalb des HSM bei der Beklagten aufbewahrten KEKs sind in zwei Teile aufgeteilt und - mit getrenntem Zugriff auf jeden Teil durch einen Key Custodian - aufbewahrt, so dass ein Zugriff hierauf eines kollusiven Zusammenwirkens mehrerer Vertrauenspersonen bedürfte. Um sodann Zugriff auf die Nachrichten zu erhalten, müssten in weiterem kollusiven Zusammenwirken mit einem Mitarbeiter des Betreibers der verschlüsselte Nachrichtenbestand und die Schlüssel zusammengeführt werden.

75 Die Beklagte hat ergänzend eine Stellungnahme der Betreiberin A. vom Januar 2018 vorgelegt, in der die Schritte, die dafür erforderlich wären, damit sich ein Mitarbeiter der Beklagten oder ein Mitarbeiter der Betreiberin Kenntnis vom

Inhalt von Nachrichten verschaffen kann, im Einzelnen dargelegt sind. Hiernach müsste sich ein solcher Täter zunächst den nach dem Prinzip des splitknowlege in zwei getrennten Teilen sicher bei der Beklagten verwahrten KEK beschaffen, hiermit den verschlüsselten Arbeitsschlüssel, sodann aus der verschlüsselten beA-Datenbank die SAFE-ID eines Anwalts, die mit dem Arbeitsschlüssel verschlüsselten Nachrichtenschlüssel und die Nachrichten für diesen Anwalt. Anschließend müsste er mit dem KEK den Arbeitsschlüssel, mit diesem die Nachrichtenschlüssel und mit den entschlüsselten Nachrichtenschlüsseln die Nachrichten selbst entschlüsseln. A. kommt hierbei zu dem Schluss, dass auf Grund der Vielzahl an notwendigen Schritten und Informationen jeder einzelne Schritt mit Blick auf die jeweiligen Sicherheitsmaßnahmen unwahrscheinlich, das Durchlaufen aller dieser Schritte abwegig und eine Bedrohung daher nicht gegeben sei. Die Kläger sind dem nicht entgegengetreten. Anhaltspunkte dafür, dass demgegenüber das von den Klägern befürchtete Ausspähen der Nachrichten mittels eines gezielten Angriffs auf einfacherem Wege möglich wäre, bestehen auch nach dem Vorbringen der Kläger nicht.

76 Jedenfalls führt diese Schwachstelle unabhängig davon, ob sie - wie die Beklagte im Berufungsverfahren geltend gemacht und zuletzt ausführlich beschrieben hat - zwischenzeitlich behoben ist, nicht dazu, dass die Nachrichtenübermittlung über das beA-System grundsätzlich als nicht sicher anzusehen und deshalb die von den Klägern geforderte Ende-zu-Ende-Verschlüsselung als einzig sichere Verschlüsselungstechnik erforderlich wäre. Denn ein auf den Aspekt der Sicherheit gestützter Anspruch der Kläger auf Unterlassung ohne und Betreiben mit der von ihnen geforderten Verschlüsselungstechnik scheidet trotz der genannten Schwachstelle schon deshalb aus, weil diese nach den unangegriffenen Ausführungen von S. einfach behoben werden kann. Hierzu schlägt S. vor, dass die HSMs die Arbeitsschlüssel selbst erzeugen sollen, diese nur in verschlüsselter Form zur Übertragung auf andere HSMs herausgegeben werden sollen und alle HSM-Schlüssel nur innerhalb speziell gesicherter Hard-

ware (HSM, Chipkarte) gespeichert werden. Die Schwachstelle ist mithin behebbar, indem auf die Verfügbarkeit der Arbeitsschlüssel sowie der KEKs außerhalb des HSM verzichtet wird. Durch die Verwendung von neuem Schlüsselmaterial wäre auch eine Sicherheitsgefahr durch etwaige Schlüsselkopien, die bei Erzeugung der ursprünglichen Schlüssel missbräuchlich erstellt worden sein könnten, gebannt. Nicht überzeugend ist der Einwand der Kläger gegen diese Lösungsmöglichkeit, dass hierdurch immer noch keine Ende-zu-Ende-Verschlüsselung vorgesehen sei und das System deshalb weiter unsicher sei. Denn das nach Auffassung der Kläger maßgebliche und entscheidende Sicherheitsrisiko, das darin bestehe, dass durch die Aufbewahrung der Schlüssel auch außerhalb des HSM die Möglichkeit des Ausspähens der gesamten beA-Kommunikation durch einen einzigen erfolgreichen Angriff ohne weitere Manipulation des HSM geschaffen werde, wäre durch die von S. vorgeschlagene Lösung behoben, ohne dass es hierzu einer Ende-zu-Ende-Verschlüsselung in dem von den Klägern gewünschten Sinn bedürfte.

77 Das im S. -Gutachten im Zusammenhang mit dieser Schwachstelle angesprochene mögliche Risiko, dass der Betreiber im Rahmen von Beschlagnahmen von Postfächern gezwungen werden könne, Nachrichten offenzulegen, stellt - wie der Anwaltsgerichtshof zutreffend ausführt - schon keine Beeinträchtigung der Sicherheit des Übermittlungswegs dar.

78 An dieser Beurteilung ändert sich nichts dadurch, dass in einer von Klägerseite vorgelegten Vorversion des S. -Gutachtens vom 30. Mai 2018 die betreffende Schwachstelle noch als betriebsverhindernd eingestuft und zur Beschreibung der Schwachstelle ein teilweise abweichender Wortlaut verwendet worden war.

79 Zum einen ist eine nicht endgültige Arbeitsversion, die im Zuge der Begutachtung erstellt wurde, nicht maßgeblich. Im Rahmen der Erarbeitung von Schriftstücken wie Schriftsätzen oder Gutachten existieren regelmäßig mehrere Vorversionen. Entscheidende Beurteilungsgrundlage ist nur die letzte, vom Ersteller als

endgültig herausgegebene Version und nicht ein Vorentwurf. Während der noch nicht abgeschlossenen Bearbeitungsphase ergeben sich regelmäßig noch Änderungen. Dies gilt hier schon deshalb, weil S. nicht ein abgeschlossenes System begutachtet hat, sondern fortlaufend während der Begutachtung identifizierte Schwachstellen behoben wurden. Nur die letzte abschließende Version enthält die endgültige Einschätzung des Gutachters, für die dieser einsteht und gegebenenfalls haftet.

80 Abgesehen davon ist die in der Vorversion beschriebene Schwachstelle unabhängig von ihrer Risikoeinstufung mit der im Abschlussgutachtern unter 5.5.3 beschriebenen in technischer Hinsicht identisch und gelten die obigen Ausführungen hierfür gleichermaßen. Beiden Versionen des Gutachtens ist als maßgebliches Sicherheitsrisiko zu entnehmen, dass die entscheidenden Schlüssel auch außerhalb des HSM existieren und hiermit alle Nachrichten entschlüsselt werden könnten. Ein Mitlesen von Nachrichten setzt dabei - wie oben ausgeführt - einen Missbrauch durch Innentäter auf Seiten der Beklagten oder der Betreiberin voraus. Entgegen dem Vorbringen der Kläger führt diese Schwachstelle auch nach der Darstellung in der Vorversion nicht zu einer Missbrauchsmöglichkeit durch eine Vielzahl von - außenstehenden - Dritten. Dies gilt auch dann, wenn die Beklagte - wie die Kläger vortragen - die Erzeugung der Schlüssel nicht überwacht hätte. Bei den möglichen Tätern, die diese Schwachstelle ausnutzen könnten, handelt es sich um - im Einzelnen identifizierbare - Mitarbeiter der Betreiberin oder der Beklagten und damit um eine begrenzte Zahl an potentiellen Innentätern.

81 Auch in der Vorgängerversion des Gutachtens wird diese Schwachstelle zudem durch die in der Endfassung dargelegten, oben dargestellten Maßnahmen als behebbar angesehen. Kann diese Schwachstelle jedoch behoben werden, steht sie einer grundsätzlich gegebenen Sicherheit des beA-Systems nicht entgegen, so dass die Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne nicht auf Grund dieser Schwachstelle als einzig sichere Variante anzusehen ist, die verpflichtend zu verwenden wäre.

82 (2.3) Sonstige weder behobene noch behebbare Sicherheitsmängel, die die Übermittlung mittels des beA als nicht hinreichend sicher erscheinen lassen und die Verwendung der von den Klägern geforderten Verschlüsselungstechnik als einzig sichere Variante gebieten würden, sind nicht ersichtlich und von den Klägern auch nicht vorgetragen. Zwar klingen in den Schriftsätzen der Kläger grundsätzliche Bedenken gegen die Verwendung des HSM an. Das HSM stelle als zentraler Knotenpunkt für die Kommunikation der gesamten Anwaltschaft ein attraktives Angriffsziel dar. Eine tatsächliche Gefährdung der Vertraulichkeit der Kommunikation ergibt sich hieraus indes nicht. Die Beklagte hat ausführlich geschildert, auf welche Weise die Sicherheit des HSM gewährleistet ist, auch im Zuge einer Wartung. Hierzu hat sie auch Erklärungen der A. vorgelegt. Anhaltspunkte dafür, dass diese Sicherheitsvorkehrungen nicht vorlägen, hierdurch keine hinreichende Sicherheit gewährleistet wäre oder sonstige Sicherheitsmängel vorhanden wären, die die Vertraulichkeit der Kommunikation tatsächlich unbehebbar beeinträchtigen oder gefährden würden, sind im vorliegenden Verfahren nicht dargetan.

83 Dafür, dass nur die von den Klägern geforderte Ende-zu-Ende-Verschlüsselung dem Stand der Technik entspräche und diese deshalb von der Beklagten verwendet werden müsste, bestehen keine Anhaltspunkte. Zwar mag diese Ende-zu-Ende-Verschlüsselung weit verbreitet sein. Dies bedeutet indes nicht, dass nicht auch das von der Beklagten gewählte Modell dem Stand der Technik entspricht, wovon der Senat auf Grundlage des S. -Gutachtens ausgeht. Aus diesem Gutachten geht - von den Klägern unwidersprochen - hervor, dass ein HSM auch in weiteren sicherheitsrelevanten Bereichen üblich ist. Das S. -Gutachten hat insoweit darauf verwiesen, dass das von der Beklagten verwendete HSM auch im Bankenwesen Anwendung findet. In dem von den Klägern vorgelegten Schreiben der Beklagten vom 30. Januar 2018 an die Präsidenten der Rechtsanwaltskammern, in dem diese über den beAThon am 26. Januar 2018 berichtet, ist davon die Rede, dass eine große Mehrheit der anwesenden IT-Experten anerkannt hätten, dass das HSM Industriestandard darstelle und ein

hohes Sicherheitsniveau gewährleiste, sofern es entsprechende Verhaltensregeln für den Betreiber der Infrastruktur des beA gebe. Anhaltspunkte dafür, dass dem widersprechend die Verwendung des HSM veraltet und nicht oder nicht mehr dem Stand der Technik entspräche, bestehen nicht.

84 Vor diesem Hintergrund teilt der Senat die Auffassung des Anwaltsgerichtshofs, dass die Einholung eines Sachverständigengutachtens zur Sicherheit des beA - auch unter Berücksichtigung des Amtsermittlungsgrundsatzes - nicht erforderlich ist. Mit dem S. -Gutachten liegt eine Begutachtung durch einen unabhängigen Experten vor, auf die sich im Übrigen beide Parteien im Rahmen dieses Verfahrens mehrfach bezogen haben. Insbesondere haben auch die Kläger die Frage, unter welchen Voraussetzungen unbefugte Dritte Kenntnis zuzustellender Dokumente erlangen könnten, als durch das S. -Gutachten geklärt angesehen, und sich - ebenso wie die Beklagte - ausdrücklich gegen eine von dem Anwaltsgerichtshof zunächst beabsichtigte Einholung eines weiteren Sachverständigengutachtens gewandt.

85 (3) Das Erfordernis einer Ende-zu-Ende-Verschlüsselung ohne Umschlüsselung der Schlüssel im HSM ergibt sich auch nicht daraus, dass § 20 Abs. 1 RAVPV die Beklagte verpflichtet, die besonderen elektronischen Anwaltspostfächer auf der Grundlage des Protokollstandards "Online Services Computer Interface - OSCI" oder einem künftig nach dem Stand der Technik an dessen Stelle tretenden Standard zu betreiben.

86 Die besonderen elektronischen Anwaltspostfächer werden auf Grundlage des Protokollstandards OSCI im Sinne dieser Vorschrift betrieben. Eine Ende-zu-Ende-Verschlüsselung ohne Umschlüsselung der Schlüssel im HSM erfordert dies nicht.

87 (3.1) Der Verweis auf den Protokollstandard OSCI ist so zu verstehen, dass die für die Registrierung als Drittanwendung am OSCI-gestützten elektronischen Rechtsverkehr erforderlichen Voraussetzungen einzuhalten sind.

88 In der Begründung zu § 20 Abs. 1 RAVPV wird ausgeführt, dass der Betrieb auf der Grundlage des OSCI-Standards zur Gewährleistung einer sicheren Kommunikation mit Ende-zu-Ende-Verschlüsselung zu erfolgen hat. Etwaige technische Änderungen seitens der Justiz, aufgrund derer eine sichere elektronische Kommunikation der Inhaber besonderer elektronischer Anwaltspostfächer mit der Justiz nicht mehr jederzeit und vollumfänglich gewährleistet sei, habe die Bundesrechtsanwaltskammer nachzuvollziehen (BR-Drucks. 417/16, S. 35 f.). Auf diese sichere elektronische Kommunikation mit der Justiz bezieht sich auch der Verweis auf den OSCI-Standard. Denn hierfür bedarf es einer Einbindung des elektronischen Anwaltspostfachs in die Infrastruktur des elektronischen Gerichts- und Verwaltungspostfachs (EGVP). Das EGVP ist eine elektronische Kommunikationsinfrastruktur für die verschlüsselte Übertragung von Dokumenten und Akten zwischen authentifizierten Teilnehmern. Dem EGVP liegt der OSCI-Standard zu Grunde. Drittprodukte wie das besondere elektronische Anwaltspostfach, die Sende- und Empfangskomponenten für die Teilnahme an der EGVP-Infrastruktur bereitstellen, müssen für die Teilnahme am OSCI-gestützten elektronischen Rechtsverkehr registriert werden. Dies setzt voraus, dass die für die Teilnahme von Drittanwendern am OSCI-gestützten elektronischen Rechtsverkehr erforderlichen Anforderungen, wie sie von der Arbeitsgruppe "IT-Standards in der Justiz" erstellt wurden (abrufbar unter https://egvp.justiz.de/Drittprodukte/index.php; in der Version 1.1 vorgelegt als Anlage B 2), eingehalten werden. Dort heißt es unter 3.2. zu den Grundlagen des Protokollstandards OSCI, dass OSCI-Transport-Nachrichten einen zweistufigen "Sicherheitscontainer" hätten. Hierdurch sei es möglich, Inhalts- und Nutzungsdaten streng voneinander zu trennen und kryptografisch unterschiedlich zu behandeln. Inhaltsdaten würden vom sogenannten Autor einer OSCI-Nachricht so verschlüsselt, dass nur der berechtigte Leser sie dechiffrieren könne. Es werde hier oft von dem "Prinzip des doppelten Umschlags" gesprochen: Die verschlüsselten Inhaltsdaten seien wiederum in einen verschlüsselten Container eingebettet. Als entscheidendes und für die Registrierung als Drittanwender unabdingbares Sicherheitsmerkmal wird demnach ein zweistufiger Sicherheitscontainer angesehen unter Trennung von

Inhalts- und Nutzerdaten sowie ein durchgehender kryptografischer Schutz der Inhaltsdaten. Eine Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne wird hierbei nicht vorgegeben.

89 Der Verweis in § 20 Abs. 1 RAVPV auf die Grundlagen des OSCI-Standards ist vor diesem Hintergrund als Verweis auf die in dem Anforderungsprofil für die Registrierung als Drittprodukt genannten Grundlagen zu sehen, insbesondere auch auf das als wesentliches Sicherheitsmerkmal angesehene "Container-Modell". Er ist damit so zu verstehen, dass das besondere elektronische Anwaltspostfach die Anforderungen einhalten muss, um seiner vorgesehenen Verwendung entsprechend als Drittanwendung am OSCI-gestützten Rechtsverkehr registriert werden zu können, ohne das es darauf ankommt, ob darüber hinaus jede für die Registrierung nicht geforderte technische Einzelheit der OSCI-Standards eingehalten ist.

90 Dieses Verständnis des Verweises auf den OSCI-Standard bestätigt auch der jüngste Regierungsentwurf eines Gesetzes zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten und zur Änderung weiterer prozessrechtlicher Vorschriften vom 12. Februar 2021 (BR-Drucks. 145/21). Dort wird für das zur Einführung vorgesehene besondere elektronische Bürger- und Organisationspostfach bestimmt, dass dieses auf dem Protokollstandard OSCI oder einem diesen ersetzenden, dem jeweiligen Stand der Technik entsprechenden Protokollstandard beruht (§ 10 Abs. 1 Nr. 1 ERVV-E). In der Begründung hierzu wird erläutert, dass OSCI-Transport-Nachrichten einen zweistufigen "Sicherheitscontainer" hätten. Hierdurch seien Vertraulichkeit, Integrität und Authentizität der Nachrichten gewährleistet. Eine Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne wird dagegen nicht für erforderlich erklärt.

91 Dieses Ergebnis wird dadurch bestätigt, dass - wie oben ausgeführt - die Struktur des besonderen elektronischen Anwaltspostfachs vor Erlass der RAVPV bekannt war und der Verordnungsgeber die Verordnung in Kenntnis und Billigung

dieser Struktur erlassen hat. Deshalb ist nicht davon auszugehen, dass der Verordnungsgeber mit dem Verweis auf die Grundlagen des Protokollstandards OSCI weitergehende oder anderslautende Anforderungen an die Verschlüsselung stellen wollte als das ihm bekannte Konzept, das planmäßig auf die Einhaltung der Anforderungen für die bestimmungsgemäße Registrierung als Drittanwendung ausgerichtet war, dies vorsah.

92 Der oben genannte Regierungsentwurf bestätigt dies: Ausdrücklich wird dort in der Begründung zu § 10 ERVV-E unter Verweis auf § 20 Abs. 1 Satz 1 RAVPV ausgeführt, dass auch die Anwaltschaft derzeit auf Grundlage des OSCI-Protokollstandards kommuniziere (BR-Drucks. 145/21, S. 43). Dem ist zu entnehmen, dass der Verordnungsgeber trotz der in Fachkreisen bekannten Diskussion zur fehlenden Ende-zu-Ende-Verschlüsselung des beA auf Grund der Verwendung des HSM auch weiterhin keine Bedenken gegen die Einhaltung der normierten Vorgaben durch das seitens der Beklagten errichtete System hat und dieses als auf Grundlage der OSCI-Standards errichtet ansieht.

93 (3.2) Wie die erfolgreiche Registrierung der beA-Webanwendung als registriertes Drittprodukt am OSCI-gestützten elektronischen Rechtsverkehr zeigt, erfüllt das besondere elektronische Anwaltspostfach die hierfür erforderlichen Voraussetzungen und wird damit zugleich auf der Grundlage des OSCI-Standards im Sinne von § 20 Abs. 1 RAVPV betrieben.

94 (3.3) Nur ergänzend ist darauf hinzuweisen, dass der OSCI-Standard eine Verschlüsselung ohnehin nicht grundsätzlich vorschreibt, sondern nur als Option ermöglicht (vgl. OSCI-Transport 1.2 - Entwurfsprinzipien, Sicherheitsziele und -mechanismen - der OSCI-Leitstelle, vom 6. Juni 2002, S. 6 unter 1.: "Das Signieren und Verschlüsseln der Inhaltsdaten erfolgt damit bei OSCI optional"; S. 18 unter 5.1.1: "OSCI stellt eine Verschlüsselung der Inhaltsdaten vom Absender zum Empfänger zur Verfügung …"). Auch deshalb besagt der Verweis auf die Grundlagen des Protokollstandards OSCI in § 20 Abs. 1 RAVPV nicht, dass der Beklagten eine bestimmte Verschlüsselungsart zwingend vorgeschrieben wäre.

95 Der Vortrag der Kläger dazu, weshalb die Vorgaben des OSCI-Standards nicht eingehalten seien, überzeugt überdies auch aus anderen Gründen nicht. Die Kläger verweisen auf Passagen der Entwurfsprinzipien, worin zum Thema Vertraulichkeit ausgeführt wird, dass die Verschlüsselung die Vertraulichkeit der Inhaltsdaten während der Übertragung sowie gegenüber dem Intermediär garantieren könne und durch die Trennung von Inhalts- und Nutzungsdaten auch der Intermediär keine Kenntnis von den Inhaltsdaten erhalte und nicht in der Lage sei, diese zu entschlüsseln und somit zu lesen. Diese Voraussetzungen werden grundsätzlich auch bei einer Übermittlung mittels der beA-Anwendung eingehalten, denn es bleiben - wie oben ausgeführt - entgegen dem Vorbringen der Kläger die Inhaltsdaten durchgehend verschlüsselt und es findet eine Umschlüsselung der Inhaltsdaten im HSM nicht statt. Soweit die Kläger darauf verweisen, dass nach dem S. -Gutachten nicht ausgeschlossen sei, dass ein Innentäter, der sich in den Besitz des gesamten Schlüsselmaterials bringe, Nachrichten entschlüsseln könne (S. -Gutachten, B-Schwachstelle Nr. 5.5.3, S. 86), ändert dies an der Erfüllung der von den Klägern genannten Voraussetzungen des OSCI-Standards nichts. Auch insoweit gilt, dass Maßstab für eine Vereinbarkeit der beA-Anwendung mit dem OSCI-Protokoll der Regelbetrieb und nicht ein missbräuchlicher und rechtswidriger Angriff auf das System ist.

96 (c) Ohne Erfolg bleibt auch der Verweis der Kläger darauf, dass die Ende-zu-Ende-Verschlüsselung im Sinne der europäischen Patentschrift aus datenschutzrechtlicher Sicht ein Mindeststandard sei. Es ist weder ersichtlich noch dargetan, dass datenschutzrechtliche Vorschriften für den Bereich der Kommunikation über das besondere elektronische Anwaltspostfach überhaupt eine Verschlüsselung, geschweige denn eine bestimmte Verschlüsselungstechnik vorschreiben.

97 (d) Eine Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne ist auch nicht aus verfassungsrechtlichen Gründen geboten.

98 Wie ausgeführt ist § 20 RAVPV nicht verfassungskonform dahingehend auszulegen, dass eine solche Verschlüsselung vorzusehen ist (hierzu oben unter 2 a bb (b) (1.6)). Es verstößt auch nicht gegen die Verfassung, dass die gesetzlichen Regelungen über die Einrichtung der besonderen elektronischen Anwaltspostfächer einen Nutzungszwang vorsehen, ohne die genaue Art der Verschlüsselung vorzugeben. Die Beklagte ist zudem nicht verpflichtet, aus verfassungsrechtlichen Gründen auch ohne einfachgesetzliche Verpflichtung hierzu das beA nur mit einer Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne zu betreiben.

99 (1) Die Regelungen über die Einrichtung und Nutzung des besonderen elektronischen Rechtsverkehrs stellen bloße Berufsausübungsregeln dar (vgl. BVerfG, Nichtannahmebeschluss vom 20. Dezember 2017 - 1 BvR 2233/17, juris Rn. 10). Dies gilt insbesondere auch für die in § 31a BRAO geregelte Pflicht für Rechtsanwälte, die für die Nutzung des beA erforderlichen technischen Einrichtungen vorzuhalten sowie Zustellungen und den Zugang von Mitteilungen über das beA zur Kenntnis zu nehmen (sog. passive Nutzungspflicht). Regelungen, die lediglich die Berufsausübung betreffen, sind mit Art. 12 Abs. 1 GG vereinbar, soweit vernünftige Erwägungen des Gemeinwohls sie als zweckmäßig erscheinen lassen und das Grundrecht nicht unverhältnismäßig eingeschränkt wird (vgl. BVerfG, Nichtannahmebeschluss vom 20. Dezember 2017, aaO Rn. 11). Gemessen hieran bestehen gegen die Verfassungsmäßigkeit der Normen, die die Einführung sowie die Nutzungspflicht des beA betreffen, keine Bedenken (vgl. hierzu bereits Senat, Urteil vom 11. Januar 2016 - AnwZ (Brfg) 33/15, NJW 2016, 1025 Rn. 16; Beschluss vom 28. Juni 2018 - AnwZ (Brfg) 5/18, NJW 2018, 2645 Rn. 4, 10). Insbesondere ist durch die normierte Verpflichtung der Beklagten, eine sichere Kommunikation zu gewährleisten, dem rechtlich geschützten Vertrauensverhältnis zwischen Rechtsanwalt und Mandant (vgl. hierzu BVerfGE 113, 29, 49; Beschluss vom 29. Januar 2015 - 2 BvR 497/12, juris Rn. 18) in ausreichendem Maße Rechnung getragen. Die Vorgaben an die Bun-

desrechtsanwaltskammer sind insoweit hinreichend bestimmt. Ein aus der Verfassung ableitbarer Anspruch darauf, dass normativ ein bestimmtes Verschlüsselungssystem vorgegeben wird, besteht nicht. Vielmehr steht es dem Gesetzgeber frei, die technische Konkretisierung des gesetzlich vorgegebenen Maßstabs der Beklagten als Körperschaft des öffentlichen Rechts anzuvertrauen (vgl. für Aufsichtsbehörden im Bereich der Telekommunikation: BVerfGE 125, 260, 327).

100 (2) Die technische Ausgestaltung des beA im Bezug auf die Verschlüsselung unter Einsatz des HSM verstößt entgegen der Auffassung der Kläger nicht gegen die Grundrechte, insbesondere nicht gegen Art. 12 Abs. 1 GG. Eine verfassungskonforme Anwendung der Regelungen, die die Beklagte zur Einrichtung des beA verpflichten, gebietet die Verwendung einer Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne nicht.

101 Die Einrichtung des beA unter Verwendung des HSM entspricht - wie ausgeführt - den verfassungsmäßigen gesetzlichen Vorgaben. Soweit die Kläger geltend machen, dass die von der Beklagten vorgenommene Einrichtung des beA ohne Ende-zu-Ende-Verschlüsselung einen ungerechtfertigten Eingriff in die Berufsausübungsfreiheit darstelle, weil sie gegen die bestehenden gesetzlichen Vorgaben zur technischen Ausgestaltung des beA verstießen, ist dies schon deshalb unzutreffend, weil - wie oben ausgeführt - die normativen Vorgaben die Beklagte nicht dazu verpflichten, eine Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne vorzusehen. Dementsprechend stellt das Betreiben ohne die verlangte Ende-zu-Ende-Verschlüsselung entgegen der Auffassung der Kläger auch keinen Eingriff in den Anspruch auf Rechtmäßigkeit staatlichen Handelns dar.

102 Die Einrichtung als solche ist ein technischer Vorgang zur Umsetzung der die Beklagte hierzu verpflichtenden Normen. Sie stellt einen Zwischenschritt dar, der erforderlich ist, damit die gesetzlich normierte passive Nutzungspflicht des § 31a Abs. 6 BRAO eingreifen und das beA überdies aktiv als Übermittlungsweg

im Rahmen der elektronischen Kommunikation genutzt werden kann. Weder verpflichtet die bloße Einrichtung des beA als reiner Realakt diejenigen, für die ein besonderes elektronisches Anwaltspostfach eingerichtet wurde, zu dessen Nutzung noch schränkt diese die Nutzer ein. Für sich genommen hat die gesetzeskonforme technische Errichtung des beA mithin keinen Eingriffscharakter. Dieser ergibt sich grundsätzlich erst durch die gesetzlich normierte Nutzungspflicht, gegen deren Verfassungsmäßigkeit - wie ausgeführt - keine Bedenken bestehen.

103 Soweit die normierten Vorgaben für die Einrichtung des beA der Beklagten Spielraum lassen, bedarf dessen Ausfüllung durch die Beklagte zwar der Berücksichtigung der - mittelbaren - Beeinträchtigung der beruflichen Tätigkeit der Nutzer, die sich aus der passiven Nutzungspflicht des konkret von der Beklagten errichteten Systems ergeben kann. Dem ist die Beklagte indes in ausreichendem Maße nachgekommen. Eine Verletzung der Grundrechte der Kläger, insbesondere der Berufsausübungsfreiheit nach Art. 12 Abs. 1 GG, liegt nicht deshalb vor, weil die Beklagte den ihr zustehenden Spielraum nicht dahingehend genutzt hat, um eine Ende-zu-Ende-Verschlüsselung in dem von den Klägern geforderten Sinne zu verwenden.

104 (2.1) Hierbei ist zunächst zu berücksichtigen, dass der Spielraum der Beklagten sich nur auf die Details der technischen Umsetzung bezog. Die berufsbezogenen Auswirkungen der reinen Ausführung betreffen deshalb nur einen sehr eingeschränkten Bereich des durch die Nutzungspflicht gesetzlich bewirkten Eingriffs in die Berufsausübungsfreiheit. Die mit der Nutzungspflicht an sich verbundenen Einschränkungen der freien Berufsausübung sind mithin für die Beurteilung der Umsetzung nicht relevant, da diese unabhängig von der gewählten technischen Ausführung entstehen.

105 (2.2) Eine Grundrechtsbeeinträchtigung durch die gewählte Verschlüsselungsstruktur ergibt sich auch weder im Hinblick auf die voraussichtlichen Kosten der verpflichtenden Nutzung für die einzelnen Nutzer noch bezüglich der mög-

licherweise erforderlichen Anpassungen der kanzleiinternen oder organisatorischen Abläufe. Denn auch diese Beeinträchtigungen werden von der gewählten Verschlüsselungsstruktur nicht beeinflusst.

106 (2.3) Die Wahl der Verschlüsselungsmethode betrifft allein die Vertraulichkeit der Kommunikation und damit mittelbar das anwaltliche Vertrauensverhältnis zum Mandanten. Zwar ist auch dieser Bereich grundrechtlich geschützt. Indes beeinträchtigt die Wahl einer Verschlüsselungsmethode diese Vertraulichkeit nicht, wenn die gewählte Methode nach obigen Kriterien als sicher anzusehen ist. Vor diesem Hintergrund kann auch dahingestellt bleiben, ob die Behauptung der Kläger zutrifft, dass die von ihnen geforderte Ende-zu-Ende-Verschlüsselung sicherer sei als das von der Beklagten gewählte Modell und dennoch alle Anforderungen an das beA eingehalten werden könnten. Eine Beeinträchtigung der Berufsausübungsfreiheit durch das gewählte System ergibt sich nicht daraus, dass die Beklagte nicht andere mögliche technische Systeme gewählt hat. Die Verfassung gibt nicht detailgenau vor, welche Sicherungsmaßnahmen im Einzelnen geboten sind (vgl. zu § 113a TKG: BVerfGE 125, 260, 326). Entscheidend ist vielmehr, ob das gewählte System zu einer (nicht gerechtfertigten) Beeinträchtigung führt, was bezogen auf die technische Gestaltung der Kommunikationsübermittlung bei der Wahl eines sicheren Übermittlungswegs nicht der Fall ist. Dementsprechend scheidet auch ein auf die Verfassung gestützter Anspruch der Kläger auf Unterlassung des Betreibens ohne die von ihnen geforderte Verschlüsselungsmethode und auf deren Verwendung aus, weil diese nicht die einzige Verschlüsselungsmethode darstellt, die die erforderliche Sicherheit gewährleisten kann. Denn wie ausgeführt ist auf Grundlage des Parteivorbringens sowie des S. -Gutachtens davon auszugehen, dass auch die gewählte Methode hierzu in der Lage ist.

107 Ein Eingriff durch die gewählte Art der Verschlüsselung ergibt sich auch nicht im Hinblick auf die von den Klägern geäußerte Befürchtung, sie könnten bei Nutzung des beA Mandanten verlieren, weil sie eine Vielzahl von Mandanten vertreten würden, die ein besonders gesteigertes Interesse an der Wahrung der

Mandatsgeheimnisse hätten. Diese Gefahr sieht der Senat nicht. Denn zum einen sind alle Anwälte zur - passiven - Nutzung des beA verpflichtet, so dass der Wechsel des Anwalts für die Mandanten insoweit keinen Nutzen brächte. Zum anderen besteht eine Nutzungspflicht im Verhältnis zwischen Mandant und Anwalt nicht, so dass vertrauliche Kommunikation, die in diesem Verhältnis ausgetauscht werden soll, nicht über das beA-System erfolgen muss. Über das beA werden Inhalte ausgetauscht, die bestimmungsgemäß das interne Mandatsverhältnis verlassen und - bei der derzeit allein verpflichtenden passiven Nutzung - vom Gericht oder dem gegnerischen Anwalt stammen sowie - bei aktiver Nutzung - für das Gericht oder den gegnerischen Anwalt beziehungsweise über diesen für die Gegenseite gedacht sind. Die Übermittlung mittels des beA ersetzt somit - ebenso wie die anderen in § 130a Abs. 4 ZPO als sicher anerkannten elektronischen Übermittlungswege - den bisherigen Postweg. Ebenso wie bei dem herkömmlichen Postversand die in den Schriftsätzen enthaltenen sensiblen Daten den Verfügungsbereich des Anwalts verlassen und der Mandant sich auf die Sicherheit der Postübermittlung verlassen muss, muss er dies bei der elektronischen Übermittlung, wobei hierfür indes - wie ausgeführt - mit dem beA ein sicherer Übermittlungsweg zur Verfügung steht, bei dem die Inhaltsdaten - anders als bei der postalischen Übermittlung - durchgängig verschlüsselt sind.

108 Etwas anderes ergibt sich auch nicht aus der von den Klägern vorgelegten Stellungnahme der Beklagten zu einem Entwurf eines Beschlusses des Rats der Europäischen Union vom 3. November 2020, wonach Regelungen für einen Zugriff auch auf verschlüsselte Daten geschaffen werden sollen. Die Beklagte wendet sich im Hinblick auf den Schutz der Vertraulichkeit der anwaltlichen Kommunikation in ihrer Stellungnahme vom 23. November 2020 gegen das von ihr deshalb befürchtete Verbot von Verschlüsselungen. Für die vom Senat zu entscheidenden Frage, welche Verschlüsselungstechnik das beA-System vorsehen muss und ob das gewählte System den gesetzlichen und verfassungsrechtlichen Anforderungen genügt, ist diese Stellungnahme nicht erheblich. Gleiches gilt für die von den Klägern vorgelegte Stellungnahme der Beklagten vom März 2021 zu

dem Entwurf einer Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, in der die Beklagte eine sichere verschlüsselte Online-Kommunikation als unabdingbare Grundvoraussetzung für die Gewährleistung des Mandatsgeheimnisses im digitalen Zeitalter ansieht und sich gegen die Beeinträchtigung der Wirksamkeit einer Ende-zu-Ende-Verschlüsselung wendet. Für die Anforderungen an die Verschlüsselungstechnik des beA ist diese Stellungnahme nicht von Relevanz.

109 b) Die Klage ist auch hinsichtlich des Klageantrags zu 2 unbegründet. Den Klägern steht kein Anspruch darauf zu, dass das beA mit einer Ende-zu-Ende-Verschlüsselung betrieben wird. Weder ergibt sich dieser aus den einfachen Gesetzen noch aus der Verfassung. Denn es verpflichten - wie ausgeführt - weder die Regelungen über die Einrichtung des beA noch die Verfassung die Beklagte dazu, das beA mit der von den Klägern geforderten Ende-zu-Ende-Verschlüsselung zu betreiben.

110 3. Eines Schriftsatzrechts für die Klägerseite auf den Schriftsatz der Beklagten vom 17. März 2021 bedurfte es nicht. Dieser Schriftsatz enthält keinen entscheidungserheblichen neuen Vortrag.

111 4. Die Kostenentscheidung beruht auf § 112c Abs. 1 Satz 1 BRAO, § 154 Abs. 2, § 159 VwGO, § 100 Abs. 1 ZPO. Die Festsetzung des Streitwerts folgt aus § 194 Abs. 1 BRAO, § 52 Abs. 2 GKG.

Limperg Liebert Ettl

Kau Merk

Vorinstanz:
AGH Berlin, Entscheidung vom 14.11.2019 - I AGH 6/18 -