Kanzlei Delhey

Kanzlei Delhey, Hochbaumstraße 20a, 14167 Berlin

Bundesverfassungsgericht
Schlossbezirk 3
76131 Karlsruhe

Dr. iur. Martin Delhey
Rechtsanwalt

Hochbaumstraße 20a
14167 Berlin
Tel.: +49 30 81 78 94 46
Fax: +49 30 81 78 94 53
mail@kanzlei-delhey.de
www.kanzlei-delhey.de

Kontodaten (IBAN/BIC):
DE 57 3002 0900 0510 8404 31
CMCIDEDD

Steuernummer: 25/257/00370
Finanzamt Zehlendorf

Ihr Zeichen: – Kanzleizeichen: M.2021-05-05.1 Dy Berlin, den 20. Mai 2021

V e r f a s s u n g s b e s c h w e r d e

des Rechtsanwalts Daniel Rink, Schwarzer Bär 4, 30449 Hannover

– Beschwerdeführer zu 1. –

sowie des Rechtsanwalts Michael Schinagl, Kurfürstendamm 188, 10707 Berlin

– Beschwerdeführer zu 2. –

beide jeweils alleinvertretungsberechtigt vertreten durch

Rechtsanwalt Dr. Martin Delhey, Hochbaumstraße 20A, 14167 Berlin,

Rechtsanwalt Christoph R. Müller, Riemannstr. 29b, 04107 Leipzig

– Bevollmächtigte –

g e g e n

1. die Einrichtung eines nicht Ende-zu-Ende-verschlüsselten besonderen elektronischen Anwaltspostfaches (beA) durch die Bundesrechtsanwaltskammer;

2. das Urteil des Anwaltsgerichtshofes Berlin vom 14. November 2019 – AGH 6/18 (**Anlage 1**);

3. das Urteil des Bundesgerichtshofes vom 22. März 2021 – AnwZ (Brfg) 2/20 (**Anlage 2**) und

4. mittelbar gegen § 31a sowie § 31c Nr. 3 der Bundesrechtsanwaltsordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 303-8, veröffentlichten bereinigten Fassung, die zuletzt durch Artikel 3 des Gesetzes vom 22. Dezember 2020 (BGBl. I S. 3320) geändert worden ist (BRAO) i. V. m. § 19 und § 20 der Rechtsanwaltsverzeichnis- und -postfachverordnung vom 23. September 2016 (BGBl. I S. 2167), die zuletzt durch Artikel 3 des Gesetzes vom 10. Dezember 2019 (BGBl. I S. 2128) geändert worden ist (RAVPV) sowie

5. unmittelbar gegen
   a. § 130a Absätze 3 und 4 Nrn. 1 und 2 sowie § 130d der Zivilprozessordnung (ZPO) i. d. F. des Artikels 1 Nr. 4 Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten (ERVGerFöG) vom 10. Oktober 2013 (BGBl. I S. 3786, 3787) sowie § 174 ZPO i. d. F. des Artikels 1 Nr. 7 lit. a ERVGerFöG (BGBl. I S. 3786, 3787);
   b. § 14b des Gesetzes über das Verfahren in Familiensachen (FamFG) in der Fassung des Artikels 2 Nr. 4 ERVGerFöG (BGBl. I S. 3786, 3789);

c. § 46c Absätze 3 und 4 Nrn. 1 und 2 sowie § 46g des Arbeitsgerichtsgesetzes (ArbGG) in der Fassung des Artikels 3 Nr. 5 ERVGerFöG (BGBl. I S. 3786, 3790);

d. § 65a Absätze 3 und 4 Nrn. 1 und 2 sowie § 65d SGG in der Fassung des Artikels 4 Nr. 4 ERVGerFöG (BGBl. I S. 3786, 3791 f.);

e. § 55a Absätze 3 und 4 Nrn. 1 und 2 sowie § 55d VwGO in der Fassung des Artikels 5 Nr. 4 ERVGerFöG (BGBl. I S. 3786, 3792 f.);

f. § 52a Absätze 3 und 4 Nrn. 1 und 2 sowie § 52d FGO in der Fassung des Artikels 6 Nr. 4 ERVGerFöG (BGBl. I S. 3786, 3794 f.) (**Anlagenkonvolut 3**);

w e g e n

Verletzung der Grundrechte der Beschwerdeführer aus Artikel 2 Absatz 1, Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1, Artikel 10 Absatz 1, Artikel 12 Absatz 1 (i. V. m. Artikel 20 Absätze 2 und 3) sowie Artikel 14 Absatz 1 des Grundgesetzes für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 u. 2 Satz 2 des Gesetzes vom 29. September 2020 (BGBl. I S. 2048) geändert worden ist (GG).

Namens und in Vollmacht (**Anlagen 4a und 4b**) der Beschwerdeführer erheben die Bevollmächtigten hiermit Verfassungsbeschwerde im vorstehend bezeichneten Umfang.

GLIEDERUNG

A. SACHVERHALT

I. AUSGANGSPUNKT: FEHLENDE ENDE-ZU-ENDE-VERSCHLÜSSELUNG DES BESONDEREN ELEKTRONISCHEN ANWALTSPOSTFACHS

Die Beschwerdeführer sind in der Bundesrepublik Deutschland zugelassene Rechtsanwälte. Als solche sind sie gemäß § 31a Absatz 6 BRAO dazu verpflichtet, im Rahmen des elektronischen Rechtsverkehrs insbesondere mit den Gerichten das sog. „besondere elektronische Anwaltspostfach“ (beA) zu nutzen.

Das beA wurde von der Bundesrechtsanwaltskammer (BRAK) auf Grundlage des § 31a Absatz 1 BRAO für die gesamte Anwaltschaft eingerichtet. Dabei konstruierte sie das beA dergestalt, dass sämtliche Nachrichten über ein sog. „Hardware Security Module“ (HSM) übermittelt werden. Der Bundesgerichtshof hat das Verfahren wie folgt vereinfacht zusammengefasst:

> „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 symmetrischen 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“.
>
> BGH Urteil des Bundesgerichtshofes vom 22. März 2021 – AnwZ (Brfg) 2/20, Rn. 3.

Mit dieser Konstruktion hat sich die BRAK gegen eine Einrichtung des beAs mit einer sog. „Ende-zu-Ende-Verschlüsselung“ entschieden, deren wesentliches Merkmal es ist, dass nur die miteinander Kommunizierenden ihre ausgetauschten Nachrichten entschlüsseln können. Dies ist nur dann der Fall, wenn sich die sog. „privaten Schlüssel“, mit denen Nachrichten wieder lesbar gemacht werden können, ausschließlich in der Verfügungsgewalt der Inhaberinnen und Inhaber der beA-Postfächer, mithin namentlich der Rechtsanwältinnen und Rechtsanwälte, befinden. Nur so ist eine technisch und rechtlich sichere Kommunikation über das beA gewährleistet.

Stattdessen hat die BRAK durch den Einsatz des HSMs einen äußerst sensiblen zentralen Angriffspunkt (sog. „Single Point of Failure“) geschaffen. Sämtliche beA-Schlüssel liegen bei der BRAK und nicht bei den Rechtsanwältinnen und Rechtsanwälten, die zur Nutzung des beAs verpflichtet sind. Mit nur einem einzigen gezielten Angriff könnte die gesamte über das beA stattfindende anwaltliche Kommunikation dauerhaft und unbemerkt mitgelesen werden.

II. GERICHTSVERFAHREN

In den der Verfassungsbeschwerde vorausgegangenen Gerichtsverfahren, zunächst erstinstanzlich vor dem Anwaltsgerichtshof Berlin (Urteil vom 14. November 2019 – AGH 6/18) und sodann im Berufungsverfahren vor dem Anwaltssenat des Bundesgerichtshofes (Urteil vom 22. März 2021 – AnwZ (Brfg) 2/20), begehrten die Beschwerdeführer, dass das beA von der BRAK mit einer Ende-zu-Ende-Verschlüsselung eingerichtet wird, um die verfassungsrechtlich gebotene, hinreichend sichere Kommunikation zwischen Anwaltschaft und Gerichten zu gewährleisten respektive

dass es die BRAK zu unterlassen habe, das beA ohne eine solche Ende-zu-Ende-Verschlüsselung zu betreiben, weil dies einen ungerechtfertigten Grundrechtseingriff insbesondere in ihre Berufsfreiheit nach Artikel 12 Absatz 1 GG darstelle.

1. VERFAHREN VOR DEM ANWALTSGERICHTSHOF BERLIN

Der Anwaltsgerichtshof Berlin wies die Klage der Beschwerdeführer indes ab (AGH Berlin, Urteil vom 14. November 2019 – AGH 6/18). Diese hätten keinen gegen die BRAK gerichteten Anspruch darauf, dass diese das beA in der von den Beschwerdeführern begehrten Weise mit der vorstehend beschriebenen Ende-zu-Ende-Verschlüsselung einrichte und betreibe. Eine entsprechende gesetzgeberische Vorgabe ergebe sich weder unmittelbar aus den einfachgesetzlichen Vorschriften wie § 31a Abs. 3 BRAO oder § 174 Abs. 3 Satz 3 ZPO in Verbindung mit § 130a Abs. 4 Nr. 2 ZPO noch aus den Regelungen der aufgrund des § 31c Nr. 3 BRAO ergangenen §§ 19, 20 RAVPV. Auch könne das Erfordernis einer Ende-zu-Ende-Verschlüsselung auch nicht mittelbar aus dem gesetzlichen Erfordernis eines sicheren Übertragungswegs abgeleitet werden. Die Architektur des beAs sei vielmehr „sicher im Rechtssinne". Daher könnten die Beschwerdeführer ihr auf den allgemeinen öffentlich-rechtlichen Unterlassungsanspruch gerichtetes Unterlassungsbegehren auch nicht auf eine drohende oder eingetretene Grundrechtsverletzung stützen. Zwar greife die Verpflichtung, das besondere elektronische Anwaltspostfach einzurichten, in die durch Artikel 12 Absatz 1 GG geschützte Freiheit der Berufsausübung der Kläger ein. § 31a BRAO stelle jedoch eine ausreichende gesetzliche Ermächtigungsnorm dar.

Im Übrigen wird auf die Urteilsbegründung (**Anlage 1**) sowie die Schriftsätze zum Klageverfahren verwiesen (**Anlagenkonvolut 1a**)

2. Berufungsverfahren vor dem Anwaltssenats des Bundesgerichtshofes

Gegen die Abweisung der Klage durch den Anwaltsgerichtshof Berlin legten die Beschwerdeführer Berufung beim Anwaltssenat des Bundesgerichtshofes ein. Dabei trugen sie insbesondere abermals vor, dass die Architektur des beAs ein Ausspähen sämtlicher anwaltlicher Kommunikation mittels eines einzigen Angriffs, eines sog. „Single Point of Failure", ermögliche. Entgegen der Auffassung des Anwaltsgerichtshofs Berlin bestehe dieser Fehler auch weiterhin. Daher sei das beA 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. Der Grundsatz der Verhältnismäßigkeit gebiete in Anbetracht der besonderen Schutzbedürftigkeit der anwaltlichen Berufsfreiheit und der für ihre Ausübung essentiellen Verschwiegenheit die Wahl nicht nur einer „irgendwie sicheren", sondern der sichersten technischen Lösung. Dies sei allein die von ihnen geforderte Ende-zu-Ende-Verschlüsselung, während die von der BRAK gewählte Lösung dagegen eine unzulässige, weil minderwertige Lösung darstelle.

Der Bundesgerichtshof wies die Berufung indes zurück (BGH, Urteil vom 22. März 2021 – AnwZ <Brfg> 2/20). Den Beschwerdeführern stehe weder ein Anspruch darauf zu, dass die BRAK es unterlässt, das beA ohne die von ihnen geforderte Ende-zu-Ende-Verschlüsselung zu betreiben, noch ein Anspruch auf ein Betreiben mit einer eben solchen Verschlüsselung.

a. „Sicher im Rechtssinne"

Im Wesentlichen begründet das Gericht dies damit, dass die von der BRAK gewählte HSM-Konzeption zwar nicht über die begehrte Ende-zu-Ende-Verschlüsselung

verfüge, dies jedoch auch nicht erforderlich sei, weil die derzeitige Konstruktion gemäß der vorinstanzlich vom Anwaltsgerichtshof Berlin entwickelten Formel „sicher im Rechtssinne“ sei. Behebbare, wenngleich auch nicht behobene Schwachstellen stünden einer grundsätzlich gegebenen Sicherheit des beA-Systems nicht entgegen.

B. Ende-zu-Ende-Verschlüsselung nicht gesetzlich gefordert

Weder aus § 31a Absatz 1 oder 3 BRAO, § 130a Absatz 4 Nr. 2 ZPO oder § 174 Absatz 3 Satz 3 und 4 ZPO noch aus den §§ 19 und 20 RAVPV ergeben sich nach Ansicht des Bundesgerichtshofes detaillierte Vorgaben für die Bewerkstelligung der Sicherheit der Nachrichtenübermittlung, insbesondere keine Verpflichtung zur Nutzung einer Ende-zu-Ende-Verschlüsselung in der von den Beschwerdeführern begehrten Form. Auch sei keine dahingehende verfassungskonforme Auslegung geboten.

C. Ende-zu-Ende-Verschlüsselung nicht verfassungsrechtlich geboten

Die Ausstattung des beAs mit einer Ende-zu-Ende-Verschlüsselung sei auch verfassungsrechtlich nicht geboten. Es verstoße nicht gegen die Verfassung, dass die gesetzlichen Regelungen über die Einrichtung des beAs einen Nutzungszwang vorsehen, ohne die genaue Art der Verschlüsselung und deren Implementierung vorzugeben. Die gesetzlichen Vorgaben seien hinreichend bestimmt. Ein aus der Verfassung ableitbarer Anspruch darauf, dass normativ ein bestimmtes Verschlüsselungssystem vorgegeben wird, bestehe nicht. Vielmehr stehe es dem Gesetzgeber frei, die technische Konkretisierung des gesetzlich vorgegebenen Maßstabs der BRAK anzuvertrauen. Eine verfassungskonforme Anwendung der Regelungen, die die BRAK zur Einrichtung des beAs verpflichten, gebiete nicht die Verwendung einer Ende-zu-Ende-Verschlüsselung. Eine Verletzung der Grundrechte der Beschwerdeführer, insbesondere

der Berufsausübungsfreiheit nach Artikel 12 Absatz 1 GG, liege nicht vor, weil die BRAK im Rahmen des ihr zustehenden Spielraum nicht verpflichtet gewesen sei, das beA mit einer Ende-zu-Ende-Verschlüsselung einzurichten. Die Verfassung gebe nicht vor, welche Sicherungsmaßnahmen im Einzelnen geboten sind.

Im Übrigen wird auf die Entscheidungsgründe (**Anlage 2**) sowie die Schriftsätze zum Klageverfahren verwiesen (**Anlagenkonvolut 2a**).

III. MITTELBAR GERÜGTE RECHTSVORSCHRIFTEN

Soweit sich die Verfassungsbeschwerde gegen das Urteil des Bundesgerichtshofes (a. a. O.) richtet, werden mittelbar die dem Urteil zugrundeliegenden, entscheidungserheblichen Rechtsvorschriften über die Einrichtung des beAs sowie die Pflicht, dieses zum Empfang von Nachrichten zu nutzen, als mit der Verfassung unvereinbar gerügt.

Aus der Bundesrechtsanwaltsordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 303-8, veröffentlichten bereinigten Fassung, die zuletzt durch Artikel 3 des Gesetzes vom 22. Dezember 2020 (BGBl. I S. 3320) geändert worden ist, sind dies (siehe auch Anlagenkonvolut 3):

> **§ 31a Besonderes elektronisches Anwaltspostfach**
> (1) Die Bundesrechtsanwaltskammer richtet für jedes im Gesamtverzeichnis eingetragene Mitglied einer Rechtsanwaltskammer ein besonderes elektronisches Anwaltspostfach empfangsbereit ein.
> (…)
> (3) Die Bundesrechtsanwaltskammer hat sicherzustellen, dass der Zugang zu dem besonderen elektronischen Anwaltspostfach nur durch ein sicheres Verfahren mit zwei voneinander unabhängigen Sicherungsmitteln möglich ist.
> (…)
> (6) Der Inhaber des besonderen elektronischen Anwaltspostfachs ist verpflichtet, die für dessen Nutzung erforderlichen technischen Einrichtungen vorzuhalten sowie Zustellungen und den Zugang von Mitteilungen über das besondere elektronische Anwaltspostfach zur Kenntnis zu nehmen.

> **§ 31c Verordnungsermächtigung**
> Das Bundesministerium der Justiz und für Verbraucherschutz regelt durch Rechtsverordnung mit Zustimmung des Bundesrates die Einzelheiten
> (…)
> 3. der besonderen elektronischen Anwaltspostfächer, insbesondere Einzelheiten
> a) ihrer Einrichtung und der hierzu erforderlichen Datenübermittlung,
> b) ihrer technischen Ausgestaltung einschließlich ihrer Barrierefreiheit,
> c) ihrer Führung,
> d) der Zugangsberechtigung und der Nutzung,
> e) des Löschens von Nachrichten und
> f) ihrer Löschung,
> 4. des Abrufs des Gesamtverzeichnisses über das Europäische Rechtsanwaltsverzeichnis.

Aus der Rechtsanwaltsverzeichnis- und -postfachverordnung vom 23. September 2016 (BGBl. I S. 2167), die zuletzt durch Artikel 3 des Gesetzes vom 10. Dezember 2019 (BGBl. I S. 2128) geändert worden ist, sind dies:

> **§ 19 Besonderes elektronisches Anwaltspostfach**
> (1) Das besondere elektronische Anwaltspostfach dient der elektronischen Kommunikation der in das Gesamtverzeichnis eingetragenen Mitglieder der Rechtsanwaltskammern, der Rechtsanwaltskammern und der Bundesrechtsanwaltskammer mit den Gerichten auf einem sicheren Übermittlungsweg. Ebenso dient es der elektronischen Kommunikation der Mitglieder der Rechtsanwaltskammern, der Rechtsanwaltskammern und der Bundesrechtsanwaltskammer untereinander.
> (…)
>
> **§ 20 Führung der besonderen elektronischen Postfächer**
> (1) Die Bundesrechtsanwaltskammer hat 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. Die Bundesrechtsanwaltskammer hat fortlaufend zu gewährleisten, dass die in § 19 Absatz 1 genannten Personen und Stellen miteinander sicher elektronisch kommunizieren können.
> (…)

IV. UNMITTELBAR GERÜGTE RECHTSVORSCHRIFTEN

Des Weiteren rügen die Beschwerdeführer gesondert und unmittelbar die Verfassungswidrigkeit der nachstehend bezeichneten weiteren Rechtsvorschriften, die

gemäß Artikel 26 Absatz 7 des Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (BGBl. I S. 3786), das durch Artikel 31 des Gesetzes vom 5. Juli 2017 (BGBl. I S. 2208) geändert worden ist (ERVGerFöG) grundsätzlich spätestens zum 01. Januar 2022 in Kraft treten werden (siehe auch Anlagenkonvolut 3).

§ 130a Absätze 3 und 4 Nrn. 1 und 2 ZPO in der Fassung des Artikels 1 Nr. 4 ERVGerFöG (BGBl. I S. 3786):

> **§ 130a Elektronisches Dokument**
> (3) Das elektronische Dokument muss mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.
> (4) Sichere Übermittlungswege sind
> 1. der Postfach- und Versanddienst eines De-Mail-Kontos, wenn der Absender bei Versand der Nachricht sicher im Sinne des § 4 Absatz 1Satz 2 des De-Mail-Gesetzes angemeldet ist und er sich die sichere Anmeldung gemäß § 5Absatz 5 des De-Mail-Gesetzes bestätigen lässt,
> 2. der Übermittlungsweg zwischen dem besonderen elektronischen Anwaltspostfach nach § 31ader Bundesrechtsanwaltsordnung oder einem entsprechenden, auf gesetzlicher Grundlageerrichteten elektronischen Postfach und der elektronischen Poststelle des Gerichts (…).

§ 130d ZPO in der Fassung des Artikels 1 Nr. 4 ERVGerFöG (BGBl. I S. 3786, 3787):

> **§ 130d Nutzungspflicht für Rechtsanwälte und Behörden**
> Vorbereitende Schriftsätze und deren Anlagen sowie schriftlich einzureichende Anträge und Erklärungen, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument zu übermitteln. Ist dies aus technischen Gründen vorübergehend nicht möglich, bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig. Die vorübergehende Unmöglichkeit ist bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen; auf Anforderung ist ein elektronisches Dokument nachzureichen; (…).

§ 174 Absatz 3 ZPO in der Fassung des Artikels 1 Nr. 4 ERVGerFöG (BGBl. I S. 3786, 3787):

> **§174 Zustellung gegen Empfangsbekenntnis oder automatisierte Eingangsbestätigung**
> (3) Das Dokument ist auf einem sicheren Übermittlungsweg im Sinne des § 130a Absatz 4 zu übermitteln und gegen unbefugte Kenntnisnahme Dritter zu schützen. Die in Absatz 1 Genannten haben einen sicheren Übermittlungsweg für die Zustellung elektronischer Dokumente zu eröffnen".

§ 14b FamFG in der Fassung des Artikels 2 Nr. 4 ERVGerFöG (BGBl. I S. 3786, 3789):

> **§ 14b Nutzungspflicht für Rechtsanwälte, Notare und Behörden**
> Werden Anträge und Erklärungen durch einen Rechtsanwalt, einen Notar, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht, so sind sie als elektronisches Dokument zu übermitteln. Ist eine Übermittlung aus technischen Gründen vorübergehend nicht möglich, bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig. Die vor übergehende Unmöglichkeit ist bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen; auf Anforderung ist ein elektronisches Dokument nachzureichen; (…).

§ 46c Absätze 3 und 4 Nrn. 1 und 2 ArbGG in der Fassung des Artikels 3 Nr. 5 ERVGerFöG (BGBl. I S. 3786, 3790):

> **§ 46c Elektronisches Dokument**
> (3) Das elektronische Dokument muss mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.
> (4) Sichere Übermittlungswege sind
> 1. der Postfach- und Versanddienst eines De-Mail-Kontos, wenn der Absender bei Versand der Nachricht sicher im Sinne des § 4 Absatz 1Satz 2 des De-Mail-Gesetzes angemeldet ist und er sich die sichere Anmeldung gemäß § 5Absatz 5 des De-Mail-Gesetzes bestätigen lässt,
> 2. der Übermittlungsweg zwischen dem besonderen elektronischen Anwaltspostfach nach § 31a der Bundesrechtsanwaltsordnung oder einem entsprechenden, auf gesetzlicher Grundlage errichteten elektronischen Postfach und der elektronischen Poststelle des Gerichts (…).

§ 46g ArbGG in der Fassung des Artikels 3 Nr. 5 ERVGerFöG (BGBl. I S. 3786, 3790):

> **§46g Nutzungspflicht für Rechtsanwälte, Behörden und vertretungsberechtigte Personen**
> Vorbereitende Schriftsätze und deren Anlagen sowie schriftlich einzureichende Anträge und Erklärungen, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument zu übermitteln. Gleiches gilt für die nach diesem Gesetz vertretungsberechtigten Personen, für die ein sicherer Übermittlungsweg nach § 46c Absatz 4 Nummer 2 zur Verfügung steht. Ist eine Übermittlung aus technischen Gründen vorübergehend nicht möglich, bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig. Die vorübergehende Unmöglichkeit ist bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen; auf Anforderung ist ein elektronisches Dokument nachzureichen; (…).

§ 65a Absätze 3 und 4 Nrn. 1 und 2 SGG in der Fassung des Artikels 4 Nr. 4 ERVGerFöG (BGBl. I S. 3786, 3791):

> **§ 65a SGG**
> (3) Das elektronische Dokument muss mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.
> (4) Sichere Übermittlungswege sind
> 1. der Postfach- und Versanddienst eines De-Mail-Kontos, wenn der Absender bei Versand der Nachricht sicher im Sinne des § 4 Absatz 1Satz 2 des De-Mail-Gesetzes angemeldet ist und er sich die sichere Anmeldung gemäß § 5Absatz 5 des De-Mail-Gesetzes bestätigen lässt,
> 2. der Übermittlungsweg zwischen dem besonderen elektronischen Anwaltspostfach nach § 31a der Bundesrechtsanwaltsordnung oder einem entsprechenden, auf gesetzlicher Grundlage errichteten elektronischen Postfach und der elektronischen Poststelle des Gerichts (…).

§ 65d SGG in der Fassung des Artikels 4 Nr. 4 ERVGerFöG (BGBl. I S. 3786, 3792):

> **§ 65d Nutzungspflicht für Rechtsanwälte, Behörden und vertretungsberechtigte Personen**
> Vorbereitende Schriftsätze und deren Anlagen sowie schriftlich einzureichende Anträge und Erklärungen, die durch einen Rechtsanwalt, durch eine

Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument zu übermitteln. Gleiches gilt für die nach diesem Gesetz vertretungsberechtigten Personen, für die ein sicherer Übermittlungsweg nach § 65a Absatz 4 Nummer 2 zur Verfügung steht. Ist eine Übermittlung aus technischen Gründen vorübergehend nicht möglich, bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig. Die vorübergehende Unmöglichkeit ist bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen; auf Anforderung ist ein elektronisches Dokument nachzureichen; (…).

§ 55a VwGO in der Fassung des Artikels 5 Nr. 4 ERVGerFöG (BGBl. I S. 3786, 3792):

§ 55a VwGO
(3) Das elektronische Dokument muss mit einer qualifizierten elektroni-schen Signatur der verantwortenden Person versehen sein oder von der ver-antwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.
(4) Sichere Übermittlungswege sind
1. der Postfach- und Versanddienst eines De-Mail-Kontos, wenn der Ab-sender bei Versand der Nachricht sicher im Sinne des § 4 Absatz 1Satz 2 des De-Mail-Gesetzes angemeldet ist und er sich die sichere Anmeldung gemäß § 5Absatz 5 des De-Mail-Gesetzes bestätigen lässt,
2. der Übermittlungsweg zwischen dem besonderen elektronischen Anwaltspostfach nach § 31a der Bundesrechtsanwaltsordnung oder einem entsprechenden, auf gesetzlicher Grundlage errichteten elektronischen Postfach und der elektronischen Poststelle des Gerichts (…).

§ 55d VwGO in der Fassung des Artikels 5 Nr. 4 ERVGerFöG (BGBl. I S. 3786, 3793):

§ 55d Nutzungspflicht für Rechtsanwälte, Behörden und vertretungsberechtigte Personen
Vorbereitende Schriftsätze und deren Anlagen sowie schriftlich einzureichende Anträge und Erklärungen, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument zu übermitteln. Gleiches gilt für die nach diesem Gesetz vertretungsberechtigten Personen, für die ein sicherer Übermittlungsweg nach § 55a Absatz 4 Nummer 2 zur Verfügung steht. Ist eine Übermittlung aus technischen Gründen vorübergehend nicht möglich, bleibt die Übermittlung nach den allgemeinen

Vorschriften zulässig. Die vorübergehende Unmöglichkeit ist bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen; auf Anforderung ist ein elektronisches Dokument nachzureichen; (…).

§ 52a FGO in der Fassung des Artikels 6 Nr. 4 ERVGerFöG (BGBl. I S. 3786, 3794):

§ 52a FGO
(3) Das elektronische Dokument muss mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.
(4) Sichere Übermittlungswege sind
1. der Postfach- und Versanddienst eines De-Mail-Kontos, wenn der Ab-sender bei Versand der Nachricht sicher im Sinne des § 4 Absatz 1Satz 2 des De-Mail-Gesetzes angemeldet ist und er sich die sichere Anmeldung gemäß § 5Absatz 5 des De-Mail-Gesetzes bestätigen lässt,
2. der Übermittlungsweg zwischen dem besonderen elektronischen Anwaltspostfach nach § 31a der Bundesrechtsanwaltsordnung oder einem entsprechenden, auf gesetzlicher Grundlage errichteten elektronischen Postfach und der elektronischen Poststelle des Gerichts (…).

§ 52d FGO in der Fassung des Artikels 6 Nr. 4 ERVGerFöG (BGBl. I S. 3786, 3794 f.):

§ 52d Nutzungspflicht für Rechtsanwälte, Behörden und vertretungsberechtigte Personen
Vorbereitende Schriftsätze und deren Anlagen sowie schriftlich einzureichende Anträge und Erklärungen, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument zu übermitteln. Gleiches gilt für die nach diesem Gesetz vertretungsberechtigten Personen, für die ein sicherer Übermittlungsweg nach § 52a Absatz 4 Nummer 2 zur Verfügung steht. Ist eine Übermittlung aus technischen Gründen vorübergehend nicht möglich, bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig. Die vorübergehende Unmöglichkeit ist bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen; auf Anforderung ist ein elektronisches Dokument nachzureichen.

B. Rechtliche Würdigung

Die Verfassungsbeschwerde ist zulässig und begründet.

Die Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung seitens der BRAK, die dies für verfassungsmäßig erachtenden Entscheidungen des Anwaltsgerichtshofes Berlin (Urteil vom 14. November 2019 – AGH 6/18, siehe Anlage 1) sowie des Bundesgerichtshofes (Urteil vom 22. März 2021 – AnwZ (Brfg) 2/20, siehe Anlage 2) sowie die zugrunde liegenden Rechtsvorschriften über die Sicherheitsanforderungen an das beA in Verbindung mit der gesetzlich vorgeschriebenen Nutzungspflicht (siehe A.III und A.IV sowie Anlagenkonvolut 3) verletzen die Beschwerdeführer in ihren Grundrechten aus Artikel 2 Absatz 1, Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1, Artikel 10 Absatz 1, Artikel 12 Absatz 1 und Artikel 12 Absatz 1 i. V. m. Artikel 20 Absätze 2 und 3 sowie Artikel 14 Absatz 1 GG.

I. Zulässigkeit

Die Verfassungsbeschwerde ist zulässig sowohl gegen die Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung als auch gegen die Urteile des Anwaltsgerichtshofes Berlin und des Bundesgerichtshofes sowie damit verbunden mittelbar gegen die den Gerichtsentscheidungen zugrunde liegenden Rechtsvorschriften und schließlich auch unmittelbar gegen die weiteren gerügten Rechtsvorschriften zur Einrichtung des beAs und der Pflicht, dieses zu nutzen.

1. Beschwerdefähigkeit

Die Beschwerdeführer sind als natürliche Personen beschwerdefähig im Sinne von § 90 Absatz 1 des Bundesverfassungsgerichtsgesetz in der Fassung der Bekanntmachung vom 11. August 1993 (BGBl. I S. 1473), das zuletzt durch Artikel 4 des

Gesetzes vom 20. November 2019 (BGBl. I S. 1724) geändert worden ist (im Folgenden: BVerfGG).

Auch können sich die Beschwerdeführer auf Artikel 12 Absatz 1 GG berufen. Der Beschwerdeführer zu 1. ist deutscher Staatsangehöriger, sodass er sich unmittelbar auch auf das Grundrecht der Berufsfreiheit berufen kann. Der Beschwerdeführer zu 2. ist österreichischer Staatsangehöriger und damit Unionsbürger. Für ihn ist der Grundrechtsschutz aus Artikel 12 Absatz 1 GG in Anbetracht des europarechtlichen Verbots der Diskriminierung wegen der Staatsangehörigkeit nach Artikel 18 AEUV sowie des Anwendungsvorrangs der Grundfreiheiten im Binnenmarkt gemäß Artikel 26 Absatz 2 AEUV ebenfalls gegeben (vgl. BVerfG, Beschluss vom 19. Juli 2011 – 1 BvR 1916/09). In jedem Falle muss dem Beschwerdeführer zu 2. zumindest im Wege einer unionsrechtskonformen Auslegung des Artikels 2 Absatz 1 GG derselbe Schutz gewährleistet werden, der deutschen Grundrechtsträgern durch Artikel 12 Absatz 1 GG zukommt (BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 04. November 2015 – 2 BvR 282/13, Rn. 11).

2. BESCHWERDEGEGENSTAND

Die Beschwerdeführer wenden sich mit ihrer Verfassungsbeschwerde gegen die im Rubrum bezeichneten verschiedenen Akte der öffentlichen Gewalt aus den Bereichen der Exekutive, Judikative und Legislative (siehe auch oben A.II., A.III. und A.IV.).

Zunächst rügen die Beschwerdeführer die Verletzung ihrer Grundrechte durch die Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung. Bei der Einrichtung handelt es sich um einen Realakt der BRAK. Dieser stellt einen Akt der öffentlichen Gewalt i. S. d. Artikels 93 Absatz 1 Nr. 4a GG dar, da er sowohl verbindlich ist als auch Außenwirkung entfaltet. Die Verbindlichkeit resultiert aus der insbesondere von § 31a Absatz 6 BRAO statuierten ausnahmslosen Pflicht aller zugelassenen Rechtsanwäl-

tinnen und Rechtsanwälte zur Nutzung des beAs. Obgleich die Anwaltschaft gemäß § 1 BRAO ein „Organ der Rechtspflege“ ist, wirkt die Einrichtung des beAs auch nicht nur „staatsintern“, da es sich bei der Ausübung der anwaltlichen Tätigkeit jedenfalls auch um einen grundrechtlich insbesondere durch Artikel 12 Absatz 1 GG geschützten Beruf handelt. Die Einrichtung des verpflichtend zu nutzenden beAs ist somit im Hinblick auf die Grundrechtsträgerschaft der Beschwerdeführer als hoheitliches Verwaltungshandeln mit Außenwirkung anzusehen.

Bei den gerügten Urteilen des Anwaltsgerichtshofes Berlin und des Bundesgerichtshofes sowie bei den mittelbar und unmittelbar gerügten Rechtsvorschriften handelt es sich unzweifelhaft um Akte der öffentlichen Gewalt.

3. FRISTWAHRUNG

Die sich aus § 93 Absatz 1 Satz 1 BVerfGG ergebende Frist zur Erhebung der Verfassungsbeschwerde gegen das Urteil des Bundesgerichtshofes ist gewahrt. Sie begann gemäß § 93 Absatz 1 Satz 2 BVerfGG mit der Zustellung des Urteils am 26. April 2021.

Soweit sich die Verfassungsbeschwerde unmittelbar gegen Rechtsvorschriften zur Nutzung des beAs richtet (siehe oben A.IV), hat die Jahresfrist nach § 93 Absatz 3 BVerfGG zum einen teilweise noch nicht zu laufen begonnen, weil die Vorschriften grundsätzlich gemäß Artikel 26 Absatz 7 ERVGerFöG erst zum 01. Januar 2022 in Kraft treten werden; gleichwohl ist anerkannt, dass die Erhebung der Verfassungsbeschwerde bereits zum jetzigen Zeitpunkt zulässig ist (BVerfGE 101, 54 <74>; BVerfGE 108, 370 <385>; siehe auch hierzu noch ausführlicher unten B.I.4.c).

Soweit der § 46g ArbGG sowie die §§ 64 Absatz 6 und 78 Satz 1 ArbGG i. V. m. § 130d ZPO, der § 65d SGG sowie der § 52d FGO, alle in der Fassung des

ERVGerFöG, im Bundesland Bremen durch die auf Grundlage des Artikels 24 Absatz 2 Satz 1 ERVGerFöG ergangene Verordnung über die Pflicht zur Nutzung des elektronischen Rechtsverkehrs für die Fachgerichtsbarkeiten mit Ausnahme des Landessozialgerichts Niedersachsen-Bremen und der Verwaltungsgerichtsbarkeit zum 1. Januar 2021 vom 8. Dezember 2020 (GBl. 2020, 500) bereits zum 01. Januar 2021 in Kraft getreten sind, ist die Jahresfrist noch nicht abgelaufen.

Soweit der § 46g ArbGG in der Fassung des ERVGerFöG im Bundesland Schleswig-Holstein durch die auf Grundlage des Artikels 24 Absatz 2 Satz 1 ERVGerFöG ergangene Landesverordnung über die Pflicht zur Nutzung des elektronischen Rechtsverkehrs vom 13. Dezember 2019 (GVOBl. 2019, 782) bereits zum 01. Januar 2020 in Kraft getreten ist, ist die Jahresfrist zur Erhebung der Verfassungsbeschwerde gegen diese Vorschrift ebenfalls insoweit noch nicht abgelaufen, als die Vorschrift in allen übrigen Bundesländern erst zum 01. Januar 2022 in Kraft treten wird. Die Beschwerdeführer sind im Übrigen von dem Inkrafttreten der Vorschrift im Bundesland Schleswig-Holstein bislang nicht betroffen, weil sie dort bislang kein Verfahren vor der Arbeitsgerichtsbarkeit geführt haben.

4. BESCHWERDEBEFUGNIS

Die Zulässigkeit einer Verfassungsbeschwerde setzt nach der Rechtsprechung des Bundesverfassungsgerichts „die Behauptung des Beschwerdeführers voraus, durch einen Akt der öffentlichen Gewalt in seinen Grundrechten verletzt zu sein. Das schließt ein, dass der Akt geeignet sein muss, den Beschwerdeführer selbst, unmittelbar und gegenwärtig in seiner grundrechtlich geschützten Rechtsposition zu beeinträchtigen“ (st. Rspr., siehe nur: BVerfGE 53, 30 <48>; 60, 360 <370>; 88, 384 <399f.>). Dies ist sowohl im Hinblick auf die Einrichtung des beAs durch die BRAK, die diesbezüglichen Gerichtsentscheidungen als auch die einschlägigen Rechtsvorschriften der Fall.

A) EINRICHTUNG DES BEAS

Die BRAK hat für die Beschwerdeführer, die in der Bundesrepublik Deutschland zugelassene Rechtsanwälte sind, gemäß dem in § 31a BRAO vorgesehenen Verfahren jeweils ein beA-Postfach, einschließlich der privaten Schlüssel der Beschwerdeführer, eingerichtet. Dies geschah direkt ohne weitere Umsetzungsakte und insbesondere unabhängig vom Willen der Beschwerdeführer. Die Postfächer bestehen auch immer noch und verfügen weiterhin nicht über eine Ende-zu-Ende-Verschlüsselung, bei der sich die privaten Schlüssel in der Verfügungsgewalt der Beschwerdeführer befinden.

B) URTEILE ZUR EINRICHTUNG DES BEAS UND INZIDENTE NORMENKONTROLLE

In den hier gerügten Gerichtsverfahren vor dem Anwaltsgerichtshof Berlin sowie vor dem Bundesgerichtshof (siehe oben A.II sowie Anlagen 1 und 2 nebst Anlagenkonvoluten 1a und 2a) traten die Beschwerdeführer als Kläger auf, sodass sie von den Urteilen selbst und unmittelbar betroffen sind. Auch entfalten die Entscheidungen auch gegenwärtig Rechtswirkung gegenüber den in den Klageverfahren unterlegenen Beschwerdeführern, indem sie es der BRAK weiterhin gestatten, das beA ohne Ende-zu-Ende-Verschlüsselung zu betreiben.

Soweit sich die Kläger im Rahmen ihrer unmittelbar gegen die bezeichneten Gerichtsurteile gerichteten Verfassungsbeschwerde auch mittelbar gegen die den Entscheidungen zugrunde liegenden Rechtsvorschriften wenden (siehe oben A.III), die von den Gerichten einer unzureichenden und unzutreffenden Verfassungsmäßigkeitsprüfung unterzogen wurden, ist dies im Licht des § 95 Absatz 3 Satz 2 BVerfGG sowie nach gefestigter Rechtsprechung des Bundesverfassungsgerichts ebenfalls zulässig.

> „Darüber hinaus kann auch der einzelne Staatsbürger im Wege der Verfassungsbeschwerde eine verfassungsgerichtliche Überprüfung von Normen

> erreichen. Dies geschieht regelmäßig in der Weise, daß er eine zu seinen Lasten ergangene Entscheidung mit der Begründung angreift, die in dieser Entscheidung angewandten Vorschriften verletzten ihn in seinen Grundrechten (inzidente Normenkontrolle)".
>
> BVerfGE 60, 360 (369).

Die von den Gerichten vorgenommene konkrete Anwendung der von den Beschwerdeführern als grundrechtsverletzend gerügten Normen führt zu einem „aktuellen Eingriff in die Rechtssphäre" der Beschwerdeführer (vgl. BVerfGE 72, 1 <5>).

C) RECHTSVORSCHRIFTEN ZUR NUTZUNG DES BEAS

Des Weiteren ist die Verfassungsbeschwerde der Beschwerdeführer auch zulässig, soweit sie sich unmittelbar gegen weitere sie in ihrer Eigenschaft als Rechtsanwälte adressierende Rechtsvorschriften richtet (siehe oben A.IV), die eine verpflichtende Nutzung des beAs als vermeintlich „sicheren Übermittlungsweg" vorsehen, obgleich diese überwiegend gemäß Artikel 26 Absatz 7 ERVGerFöG erst zum 01. Januar 2022 in Kraft treten werden (siehe zum unterschiedlichen Inkrafttreten oben B.I.3).

Es entspricht ständiger Rechtsprechung des Bundesverfassungsgerichts, dass eine gegenwärtige Betroffenheit von einer Norm bereits dann gegeben ist, wenn diese schon verkündet wurde, aber erst zu einem späteren, indes konkret bestimmten Datum in Kraft treten wird. Dass die Normen insofern „materielle Rechtswirkungen erst in der Zukunft erzeugen" werden, stehe der gegenwärtigen Betroffenheit „nicht entgegen", da die „künftige(n) Rechtswirkungen schon jetzt klar abzusehen und für (die Beschwerdeführer) gewi(ss) sind" (BVerfGE 101, 54 <74> m. w. N.).

Zudem hätte vom Gesetzgeber das Ziel einer zeitlich gestaffelten Inkraftsetzung eines im Ganzen zusammenhängenden Normkomplexes „auch anders erreicht werden können, etwa durch eine materiellrechtliche Regelung der zeitlichen Stufung bei sofortigem In-Kraft-Treten des Gesetzes" (BVerfGE 108, 370 <385>; vgl. auch

BVerfGE 101, 54 <74>). „Die Vorschriften wären dann zwar in Kraft gesetzt worden, hätten jedoch erst bei Erreichen der jeweiligen Stufe Wirksamkeit erlangt. In dem einen wie in dem anderen Fall sind aber die künftigen Rechtswirkungen bereits gegenwärtig klar abzusehen und für die Beschwerdeführer gewiss“. Daher entspreche es dem „Gebot effektiven Grundrechtsschutzes, ungeachtet der vom Gesetzgeber gewählten Konstruktion schon jetzt im Zusammenhang des gesamten Komplexes die Prüfung der zukünftig maßgeblich werdenden Regelungen zu ermöglichen“ (BVerfGE 108, 370 <385>).

So liegt es auch hier. Der Gesetzgeber hat sich vorliegend für eine zeitlich abgestufte Einführung und Intensivierung der anwaltlichen Pflicht zur Nutzung des beAs entschieden, die er auch dergestalt hätte herbeiführen können, dass er sämtliche Normen zugleich hätte in Kraft treten lassen und dabei den zeitlichen Eintritt ihrer Wirkung materiell-rechtlich festlegen können. Da die gesetzlichen Regelungen bereits verkündet und somit der Gesetzgebungsprozess final abgeschlossen ist (Artikel 82 Absatz 1 Satz 1 GG), ist schon gegenwärtig klar absehbar, dass die Beschwerdeführer von den normierten Pflichten betroffen sein werden.

Die gerügten Normen greifen auch unmittelbar in die Grundrechte der Beschwerdeführer ein, indem sie das beA direkt, insbesondere ohne ein weiteres zwischengeschaltetes behördliches Zertifizierungs- und Anerkennungsverfahren, als „sicheren Übermittlungsweg“ deklarieren und die Beschwerdeführer unmittelbar zur Nutzung verpflichten.

Dabei ist hervorzuheben, dass obgleich die Rechtsvorschriften vorsehen, dass das beA nur ein alternativer „sicherer Übermittlungsweg“ neben einem De-Mail-Konto ist, dies nichts daran ändert, dass die Vorschriften jederzeit und mit hinreichender Wahrscheinlichkeit eine konkrete Nutzungspflicht des beAs begründen können. So sieht § 130d ZPO – stellvertretend für die gleichlautenden Vorschriften in den anderen

Prozessordnungen (siehe oben A.IV.) – vor, dass nur dann eine nicht-elektronische Übermittlung zulässig ist, wenn die elektronische Übermittlung über einen sicheren Übermittlungsweg „aus technischen Gründen vorübergehend nicht möglich“ ist, wobei dies „unverzüglich danach glaubhaft zu machen“ ist und „auf Anforderung“ zudem „ein elektronisches Dokument nachzureichen“ ist. Bei „Nichteinhaltung ist die Prozesserklärung nicht wirksam“ und auf die „Einhaltung kann auch der Gegner weder verzichten noch sich rügelos einlassen (§ 295 Absatz 2 ZPO)“ (so die Gesetzesbegründung zu § 130d ZPO, BT-Drs. 17/12634, S. 27).

Da zurzeit neben dem beA nur ein De-Mail-Konto als „sicherer Übermittlungsweg“ im Sinne der gerügten Vorschriften – hier exemplarisch: § 130a Absätze 3, 4 ZPO – genutzt werden kann, wären die Beschwerdeführer folglich zur Nutzung des beAs verpflichtet, sobald es ihnen aus technischen Gründen vorübergehend nicht möglich sein sollte, ein Dokument per De-Mail zu übermitteln. Da die BRAK gemäß § 31a Absatz 1 BRAO für sämtliche Rechtsanwältinnen und Rechtsanwälte ein beA eingerichtet hat und die Beschwerdeführer durch § 31a Absatz 6 BRAO dazu verpflichtet sind, stets die für die Nutzung des beAs erforderlichen technischen Einrichtungen vorzuhalten, können sie sich einer derartigen „Alternativnutzungspflicht“ des beAs bei einem vorübergehenden technischen Ausfall von De-Mail auch nicht entziehen.

Des Weiteren verfügt auch De-Mail nicht über eine Ende-zu-Ende-Verschlüsselung, wie sie die Beschwerdeführer für geboten halten, um eine verfassungskonforme sichere elektronische Kommunikation zu gewährleisten. Vielmehr müsste eine solche erst zusätzlich unter Verwendung weiterer spezieller Software eingerichtet werden.

> „**2.6 Ende-zu-Ende-Verschlüsselung**
> Für besonders sensible Nachrichten können zusätzlich zu dem Transportkanal auch die Inhalte der De-Mail verschlüsselt werden. Um diese so genannte Ende-zu-Ende-Verschlüsselung verwenden zu können, benötigen Sie ebenso wie der Empfänger Ihrer Nachricht entsprechende Verschlüsselungssoftware, die auf den eigenen Rechnern installiert sein muss. Mit dieser Software verschlüsseln Sie Ihre De-Mail persönlich vor dem Versand. Entschlüsselt wird

> sie erst durch den Empfänger auf dessen Rechner. Eine automatische Prüfung auf Schadprogramme kann in diesem Fall nicht erfolgen, da der De-Mail-Anbieter keinen Zugriff auf die Nachrichteninhalte hat. Die Nutzung der Ende-zu-Ende-Verschlüsselung wird durch einen Verzeichnisdienst erleichtert, den alle De-Mail-Anbieter zur Verfügung stellen müssen. Der Empfänger Ihrer De-Mail kann hier seinen öffentlichen Schlüssel hinterlegen, den Sie verwenden, um Ihre De-Mail zu verschlüsseln. Zur Entschlüsselung Ihrer De-Mail nutzt der Empfänger anschließend seinen privaten, nur ihm bekannten Schlüssel. Die De-Mail-Anbieter vereinfachen Ihnen die Ende-zu-Ende-Verschlüsselung durch kostenlose Zusatzprogramme, die Sie auch ohne Vorkenntnisse nutzen können. Die Zusatzprogramme nutzen den weltweit anerkannten Standard „Pretty Good Privacy“ (PGP) und werden in der gewohnten Browser-Oberfläche des De-Mail-Kontos verwendet. Wenn Sie sich eingehender mit dem Thema Ende-zu-Ende-Verschlüsselung beschäftigen möchten, finden Sie auf der Internetseite www.bsi-fuer-buerger.de detailliertere Informationen“.
>
> Bundesamt für Sicherheit in der Informationstechnik, De-Mail – Sicherer elektronischer Nachrichtenverkehr – einfach, nachweislich, vertraulich; zuletzt abgerufen am 11. Mai 2021 unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/moderne-verwaltung/e-government/bsi-broschuere-de-mail.pdf?__blob=publicationFile&v=4 (Herv. d. Verf.).

Soweit bekannt ist es allerdings im Rahmen der Kommunikation mit Gerichten mittels De-Mail auch nicht möglich, eine zusätzlich implementierte Ende-zu-Ende-Verschlüsselung zu verwenden, sodass eine Ende-zu-Ende-verschlüsselte Kommunikation mit Gerichten auch über De-Mail letztlich faktisch ausgeschlossen ist.

Insofern rügen die Beschwerdeführer eine Verletzung ihrer Grundrechte aus denselben Gründen mit denen sie sich gegen die Einrichtung und Pflicht zur Nutzung des beAs wenden auch in Bezug auf die vorgeschriebene Nutzung von De-Mail. In beiden Fällen handelt es sich um Kommunikationsmittel, die nicht über die aus Sicht der Beschwerdeführer verfassungsrechtlich gebotene Ende-zu-Ende-Verschlüsselung verfügen.

D) MÖGLICHE GRUNDRECHTSVERLETZUNGEN

Die Beschwerdeführer behaupten, dass sie durch die bezeichneten Akte der öffentlichen Gewalt (siehe oben A.I-IV) in ihren Grundrechten aus Artikel 2 Absatz 1, Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1, Artikel 10 Absatz 1, Artikel 12 Absatz 1 und Artikel 12 Absatz 1 i. V. m. Artikel 20 Absätze 2 und 3 sowie Artikel 14 Absatz 1 des GG verletzt werden.

Nach der ständigen Rechtsprechung des Bundesverfassungsgerichts muss eine Grundrechtsverletzung jedenfalls möglich erscheinen und darf nicht von vornherein ausgeschlossen sein (statt vieler BVerfGE 52, 303 <327>; BVerfGE 114, 258 <274>). Dies ist hier der Fall.

Die gerügten Akte der öffentlichen Gewalt – von der Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung über die hierzu gegen die Beschwerdeführer als vormalige Kläger ergangenen Urteile des Anwaltsgerichtshofes Berlin und des Bundesgerichtshofes bis hin zu den Rechtsvorschriften über die Einrichtung sowie die Pflicht zur Nutzung des beAs (siehe oben A.I-IV) – lassen eine Verletzung der genannten Grundrechte der Beschwerdeführer zumindest möglich erscheinen. Sie greifen insbesondere in verfassungswidriger Weise in die grundrechtlich durch Artikel 12 Absatz 1 GG geschützte Berufsfreiheit der Beschwerdeführer ein.

AA) ANFORDERUNGEN DES BUNDESVERFASSUNGSGERICHTS AN DARLEGUNG DER UNSICHERHEIT DES BEAS ERFÜLLT

In einem Nichtannahmebeschluss zu einer Verfassungsbeschwerde gegen die gesetzliche Pflicht zur Nutzung des beAs aus dem Jahre 2017 führte das Bundesverfassungsgericht zur Möglichkeit einer hierdurch bedingten Verletzung der Berufsausübungsfreiheit aus:

> „Im Hinblick auf die Behauptung, dass über das beA eine sichere Kommunikation nicht möglich, sondern vielmehr zu befürchten sei, dass Unbefugte Daten ausspähen könnten, fehlt es bereits an der Berücksichtigung des Umstands, dass entgegen der Ansicht des Beschwerdeführers nicht jeder beliebige Dritte ohne Weiteres an dem elektronischen Rechtsverkehr über das beA teilnehmen kann; jedenfalls aber fehlt es an einer Auseinandersetzung mit den konkret getroffenen Sicherheitsvorkehrungen wie etwa der Ende-zu-Ende-Verschlüsselung“.
>
> BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 20. Dezember 2017 – 1 BvR 2233/17, Rn. 14 (Herv. d. Verf.)

Eben jene damals vom Bundesverfassungsgericht begehrte „Auseinandersetzung mit den konkret getroffenen Sicherheitsvorkehrungen“ des beAs, insbesondere „der Ende-zu-Ende-Verschlüsselung“, kann nunmehr erfolgen. Denn am selben Tage noch, an dem der Nichtannahmebeschluss erging, musste das beA wegen erheblicher Sicherheitsmängel vollständig abgeschaltet werden. Erst dann erfolgte auch im Nachgang eine gutachterliche Überprüfung der Sicherheit des beAs durch die von der BRAK beauftragte Secunet AG..

BB) GUTACHTERLICH ERWIESENE UNSICHERHEIT DES BEAS MANGELS ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Mit dem Gutachten wurde erstmals öffentlich bekannt, dass das beA – entgegen der damaligen Aussagen der BRAK – nicht über eine Ende-zu-Ende-Verschlüsselung verfügt, sondern stattdessen über eine technische Konstruktion, bei der sämtliche Nachrichten über ein HSM übermittelt werden. So wurde in dem Gutachten festgestellt:

> „Elementar geht es um die Sicherheit der verschlüsselten Arbeitsschlüssel (Master-Key-Sets) für die verschiedenen Zwecke desHSM und der Schlüssel (Key Encryption Keys, KEKs), mit denen die Arbeitsschlüssel verschlüsselt sind, sowie die Verwahrung der mit den KEKs verschlüsselten Master-Key-Sets. Wer sich in den Besitz dieses Schlüsselmaterials bringt, kann die im beA-System gespeicherten Nachrichten auch ohne HSM entschlüsseln, unverzüglich und umfassend, d.h. jede Nachricht kann davon betroffen sein.
>
> (…)

> Damit sie (die Praxis des Einsatzes eines HSMs, Anm. d. Verf.) für das beA geeignet ist, ist es erforderlich, dass die beA-Anwender als potentiell vom Bruch der Vertraulichkeit Bedrohte dem Auftraggeber und dem Betreiber des beA ausreichend vertrauen. Ob dies der Fall ist, kann im Rahmen dieses Gutachtens nicht beurteilt werden. Ist ausreichendes Vertrauen vorhanden, kann die hier aus technischer Sicht (Möglichkeit und Umfang des Schadens) als betriebsbehindernd riskant bewertete Praxis fortgesetzt werden.
>
> (…)
>
> Risikobewertung: B-Betriebsbehindernd
>
> Ausnutzbarkeit:
> Der Angriff ist nur durch bestimmte Innentäter durchführbar, die dabei ei-ne Vertrauensstellung haben müssen, die sie missbrauchen. Die Aus-nutzbarkeit ist daher niedrig.
>
> Bewertung der Ausnutzbarkeit: niedrig
> Bewertung der Bedrohung:
> Der Angriff erlaubt die umfassende Aufdeckung des Inhalts aller in beA-Postfächern gespeicherten Nachrichten. Die Bedrohung wird daher als hoch eingeschätzt.
>
> Bedrohung Integrität: niedrig
>
> Bedrohung Verfügbarkeit: niedrig
>
> Bedrohung Vertraulichkeit: hoch
>
> Secunet AG, Technische Analyse und Konzeptprüfung des beA, Abschlussgutachten im Auftrag der Bundesrechtsanwaltskammer, Körperschaft des öffentlichen Rechts, Littenstraße 910179 Berlin, Version 1.0, Stand: 18.06.2018, S. 86 f. (Herv. d. Verf.; im Folgenden: veröffentlichtes Secunet-Gutachten, enthalten im Anlagenkonvolut 1a)

Hierzu sei sogleich angemerkt, dass sich zudem späterhin durch ein erst vor Kurzem erfolgreich abgeschlossenes Klageverfahren gegen die BRAK auf Herausgabe der ursprünglichen Endversion des Gutachtens (OVG Berlin-Brandenburg, Beschluss vom 25.08.2020 – 12 N 151.19) herausstellte, dass die Risikobewertung eigentlich wie folgt lautete:

> „Bedrohung Vertraulichkeit: hoch
>
> Es besteht die Möglichkeit für Dritte als auch für die BRAK sich Zugriff auf die Nachrichten und deren Inhalte zu verschaffen, ohne dabei das HSM manipulieren zu müssen. Somit ist nicht gewährleistet, dass ausschließlich Absender und Empfänger Zugriff auf die Nachrichteninhalte haben.
>
> (…)
>
> Anmerkung: Die Bewertung „A-Betriebsverhindernde Schwachstelle" erscheint dann begründet, wenn die Nutzer des beA einen technischen Schutz gegen ein unberechtigtes Ausspähen von Nachrichten durch den Betreiber des beA oder gegen Beschlagnahme von Nachrichten im beA verlangen können".
>
> Secunet AG, Technische Analyse und Konzeptprüfung des beA, Ab-schlussgutachten im Auftrag der Bundesrechtsanwaltskammer, Körperschaft des öffentlichen Rechts, Littenstraße 910179 Berlin, Version 1.0, Stand: 30.05.2018, S. 50 (Herv. d. Verf; im Folgenden: ursprüngliches Secunet-Gutachten)

Dem Nichtannahmebeschluss des Bundesverfassungsgerichts ist zweifelsfrei zu entnehmen, dass die Richterinnen und Richter zum Zeitpunkt der Entscheidung davon ausgingen, dass das beA über eine Ende-zu-Ende-Verschlüsselung verfügt. Dies wird nicht nur aus der bereits zitierten Stelle deutlich, sondern auch aus der Sachverhaltsdarstellung, wenn die Kammer wörtlich und unmissverständlich ausführte:

> „Das beA verwendet zur sicheren Übermittlung eine so genannte Ende-zu-Ende-Verschlüsselung (vgl. § 20 Abs. 1 RAVPV)".
>
> BVerfG a. a. O., Rn. 3.

cc) Gerichtlich festgestellte Konstruktion des beAs ohne Ende-zu-Ende-Verschlüsselung

Hierzu stellte der Bundesgerichtshof – insoweit zutreffend – nunmehr klar, dass das beA nicht über eine Ende-zu-Ende-Verschlüsselung verfügt:

> „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/applica-tion?number=EP98108118).

> (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. (…) 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.
> (b) Diesen Erfordernissen entspricht der im Rahmen des besonderen elektronischen Anwaltspostfachs verwendete Übermittlungsweg nicht vollstän-dig.
> (…)
> 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".
>
> BGH, Urteil vom 22. März 2021 - AnwZ (Brfg) 2/20, Rn. 26-28, 38 (Herv. d. Verf.).

Diese Informationen konnten erst im Nachgang zu dem Nichtannahmebeschluss des Bundesverfassungsgerichts aus dem Jahre 2017 durch mehrere Gerichtsverfahren sowie die im Auftrag der BRAK durchgeführte Begutachtung des beAs durch die Secunet AG erworben werden. Dem damals von der 1. Kammer des Bundesverfassungsgerichts aufgestellten Begründungserfordernis näher darzulegen, weshalb das beA keine sichere Kommunikation gewährleistet und daher in verfassungswidriger Weise in Grundrechte eingreift, kann nach alledem nunmehr Genüge getan werden.

DD) GERICHTLICH FESTGESTELLTE MÖGLICHKEIT EINER ZENTRALEN KOMPROMITTIERUNG SÄMTLICHER ANWALTLICHER KOMMUNIKATION ÜBER DAS BEA MANGELS ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Es ist nicht nur gutachterlich erwiesen, dass die gewählte HSM-Konstruktion einen zentralen Angriffspunkt („Single Point of Failure“) schafft, der es ermöglicht, dass sämtliche über das beA ausgetauschten Nachrichten von allen Postfachinhaberinnern und -inhabern – mithin der gesamten Anwaltschaft – mit nur einem Zugriff kompromittiert werden können (siehe ursprüngliches Secunet-Gutachten, S. 50 f. sowie das veröffentlichte Secunet-Gutachten, S. 86 f.). Diese Feststellungen wurden vielmehr auch vom Bundesgerichtshof bestätigt (BGH a. a. O., Rn.72-81), wenngleich sie letztlich aus Sicht der Beschwerdeführer im Ergebnis in erkennbar verfassungswidriger Weise als hinnehmbar bewertet wurden.

EE) WEITERHIN BESTEHENDES ERHEBLICHES SICHERHEITSRISIKO WEGEN FEHLENDER ENDE-ZU-ENDE-VERSCHLÜSSELUNG DES BEAS

Wie dargelegt – und inzwischen sowohl gutachterlich als auch gerichtlich festgestellt – verfügt das beA nach nicht über eine Ende-zu-Ende-Verschlüsselung, bei der sich die zum Entschlüsseln der ausgetauschten Nachrichten erforderlichen Schlüssel ausschließlich in der Verfügungsgewalt der miteinander Kommunizierenden befinden, was aber conditio sine qua non für eine sichere, insbesondere vertrauliche elektronische Kommunikation ist. Stattdessen findet beim beA eine zentrale „Umschlüsselung“ in dem von der BRAK eingesetzten HSM statt.

Dabei spielt es auch keine Rolle, wie oft und in welcher Art und Weise bei der Umschlüsselung im HSM bestimmte Schlüssel verwendet werden, die ihrerseits wiederum verschlüsselt werden und so weiter und so fort (siehe BGH a. a. O., Rn. 3). Einzig entscheidend ist, dass das Schlüsselmaterial nicht allein bei den beA-

Postfachinhaberinnen und -inhabern liegt – so wie es bei einer Ende-zu-Ende-Verschlüsselung zwingend geboten ist, um eine vertrauliche Kommunikation zu gewährleisten –, sondern dass stattdessen das Schlüsselmaterial zentral im HSM der BRAK erzeugt und gespeichert wird. Die BRAK beziehungsweise ihre Auftragnehmer agieren demnach als „Man in the Middle", als zwischengeschaltete Instanz.

Wie in dem veröffentlichten Secunet-Gutachten zutreffend festgestellt, führt diese Konstruktion dazu, dass die Beschwerdeführer bei Nutzung des beAs der BRAK beziehungsweise deren Auftragnehmern vertrauen müssen; insofern nochmals:

> „Damit sie (die Praxis des Einsatzes eines HSMs, Anm. d. Verf.) für das beA geeignet ist, ist es erforderlich, dass die beA-Anwender als potentiell vom Bruch der Vertraulichkeit Bedrohte dem Auftraggeber und dem Betreiber des beA ausreichend vertrauen. Ob dies der Fall ist, kann im Rahmen dieses Gutachtens nicht beurteilt werden. Ist ausreichendes Vertrauen vorhanden, kann die hier aus technischer Sicht (Möglichkeit und Umfang des Schadens) als betriebsbehindernd riskant bewertete Praxis fortgesetzt werden".
>
> Veröffentlichtes Secunet-Gutachten a. a. O., S. 86 (Herv. d. Verf.).

Dies ist aber genau das, was durch eine Ende-zu-Ende-Verschlüsselung zur Gewährleistung der Vertraulichkeit des Nachrichtenaustausches unbedingt vermieden werden soll. Die miteinander Kommunizierenden sollen auf sicherem Wege miteinander Nachrichten auszutauschen können, gerade ohne dabei auf eine zwischengeschaltete Instanz vertrauen zu müssen.

Gleichwohl wurde dies in allen Instanzen nicht hinreichend berücksichtigt und im Lichte der besonderen verfassungsrechtlichen Anforderungen an vertrauliche Anwaltskommunikation zum Schutze des Anwaltsgeheimnisses unzutreffend bewertet.

ff) Besondere verfassungsrechtliche Anforderungen an Sicherheit des beAs

Nach alledem erscheint es jedenfalls möglich, dass das beA in seiner nunmehr bekannten tatsächlichen Ausgestaltung ohne eine Ende-zu-Ende-Verschlüsselung nicht die Voraussetzungen für einen sicheren Kommunikationsweg erfüllt, weil damit – nunmehr gerichtlich und gutachterlich geklärt – nachweislich eine zentrale Kompromittierung sämtlicher beA-Nachrichten nicht ausgeschlossen werden kann, obwohl dies technisch möglich wäre.

Eine Verletzung der Beschwerdeführer in ihren Grundrechten, insbesondere in ihrer Berufsausübungsfreiheit nach Artikel 12 Absatz 1 GG, ist damit zumindest möglich. Denn die Beschwerdeführer sind gegenwärtig gesetzlich verpflichtet, das von der BRAK ohne Ende-zu-Ende-Verschlüsselung eingerichtete beA zu nutzen, nachdem zunächst der Anwaltsgerichtshof Berlin und sodann zuletzt der Bundesgerichtshof dies gebilligt haben, indem sie die bestehenden Vorschriften dahingehend ausgelegt haben, dass der Betrieb des beAs auch ohne Ende-zu-Ende-Verschlüsselung rechtmäßig sei. Somit wirken alle vorliegend gerügten Akte der öffentlichen Gewalt (siehe oben A.II.-IV.) zusammen und lassen eine gegenwärtige und unmittelbare Grundrechtsverletzung der Beschwerdeführer möglich erscheinen.

Denn essentielles Wesenselement der freien Ausübung des Anwaltsberufes ist die anwaltliche Verschwiegenheit. Sie ist anwaltliche Grundpflicht nach § 43a Absatz 2 BRAO. Sie ist Grundpfeiler der rechtsstaatlich vorausgesetzten freien und unabhängigen Advokatur (Artikel 20 Absatz 3 GG). Sie ist „Grundlage des notwendigen Vertrauensverhältnisses zum Mandanten“ (BVerfG, Beschluss des Ersten Senats vom 12. Januar 2016 – 1 BvL 6/13, Rn. 55).

Nach der gefestigten Rechtsprechung des Bundesverfassungsgerichts wird „(d)ie anwaltliche Berufsausübung (…) seit einem Jahrhundert durch den Grundsatz der freien Advokatur gekennzeichnet, der einer staatlichen Kontrolle und Bevormundung grundsätzlich entgegensteht“ (BVerfGE 34, 293 <302>; 50, 16 <29>). Dabei hat das Bundesverfassungsgericht wiederholt auf die „fundamentale objektive Bedeutung“ der freien Advokatur hingewiesen und die historische Wandlung der vor-mals „staatsdienerähnlichen Ausgestaltung des Advokatenstands in einen vom Staat unabhängigen freien Beruf“ hervorgehoben (BVerfGE 63, 266 <282–286>; siehe auch 15, 226 <234>; 34, 293 <302>; 37, 67 <78>; 50, 16 <29>):

> „Die Herauslösung des Anwaltsberufs aus beamtenähnlichen Bindungen und seine Anerkennung als ein vom Staat unabhängiger freier Beruf kann als ein wesentliches Element des Bemühens um rechtsstaatliche Begrenzung der staatlichen Macht angesehen werden, das der Verfassungsgeber vorgefunden und in seinen Willen aufgenommen hat. Es entspricht dem Rechtsstaatsgedanken und dient der Rechtspflege, dass dem Bürger schon aus Gründen der Chancen- und Waffengleichheit Rechtskundige zur Verfügung stehen, zu denen er Vertrauen hat und die seine Interessen möglichst frei und unabhängig von staatlicher Einflussnahme wahrnehmen können“
>
> BVerfGE 63, 266 (283 f.).

Demnach sind von Verfassung wegen besonders hohe Anforderungen an die Gewährleistung einer freien anwaltlichen Berufsausübung und dabei insbesondere an den Schutz der anwaltlichen Verschwiegenheit zu stellen. Dem wird das beA in seiner technischen Ausgestaltung ohne eine Ende-zu-Ende-Verschlüsselung, die es den Rechtanwältinnen und Rechtsanwälten erlaubt, selbst die Vertraulichkeit ihrer Kommunikation sicherzustellen – und nicht auf die BRAK oder deren Auftragnehmer als „Man in the Middle“ vertrauen zu müssen –, nicht gerecht.

Nach der Rechtsprechung des Bundesverfassungsgerichts gibt die Verfassung zwar „nicht detailgenau vor, welche Sicherheitsmaßgaben im Einzelnen geboten sind“, jedoch muss „ein Standard gewährleistet werden, der unter spezifischer Berücksichti-

gung der Besonderheiten (…) ein besonders hohes Maß an Sicherheit gewährleistet“ (BVerfG, Urteil des Ersten Senats vom 02.03.2010 – 1 BvR 256/08, Rn. 224). In Anbetracht dessen, dass über das beA besonders schutzwürdige, der anwaltlichen Verschwiegenheit unterliegende, teils hochsensible Mandantengeheimnisse auszutauschen sind, muss daher in Bezug auf das beA in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts ein besonders hohes Maß an Sicherheit gewährleistet werden. Und dieses besteht wie dargelegt und gutachterlich festgestellt nur bei Einrichtung einer Ende-zu-Ende-Verschlüsselung.

> So auch vorgetragen im Berufungsverfahren vor dem Bundesgerichtshof mit Schriftsatz vom 18. März 2020, S. 9 (Anlagenkonvolut 1a).

GG) MÖGLICHE GRUNDRECHTSVERLETZUNG DURCH EINRICHTUNG DES BEAS

Vor diesem Hintergrund erscheint es zumindest möglich, dass die Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung nicht verfassungskonform ist und die Beschwerdeführer in ihren Grundrechten, insbesondere auf freie und unabhängige Ausübung ihres Anwaltsberufes (Artikel 12 Absatz 1 GG) verletzt.

HH) MÖGLICHE GRUNDRECHTSVERLETZUNG DURCH DIE URTEILE DES ANWALTSGERICHTSHOFES BERLIN UND DES BUNDESGERICHTSHOFES

Ebenso erscheint es nach alledem zumindest möglich, dass der Anwaltsgerichtshof Berlin und zuletzt der Bundesgerichtshof die verfassungsrechtlichen Anforderungen an die Sicherheit des beAs erkennbar nicht zutreffend bewertet haben, indem sie insbesondere dem Umstand, dass durch nur einen einzigen gezielten Angriff die gesamte beA-Korrespondenz aller Rechtsanwältinnen und Rechtsanwälte unbemerkt und dauerhaft kompromittiert werden kann, nicht hinreichend gewichtet haben mit Blick auf die unter besonderem verfassungsrechtlichen Schutz stehende anwaltliche Verschwiegenheitspflicht als Kernelement einer rechtsstaatlich gebotenen freien und

unabhängigen Advokatur. Insofern erscheint es möglich, dass die Gerichte den Schutzbereich des Artikels 12 Absatz 1 GG nur unvollkommen bestimmt haben, indem sie die besondere Bedeutung einer freien und unabhängigen Anwaltschaft im Rechtsstaat außer Acht gelassen haben und zudem das Gewicht des Grundrechts der Beschwerdeführer auf freie und unabhängige Ausübung ihres Anwaltsberufes unrichtig eingeschätzt haben (vgl. st. Rspr. BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 18. April 2018 – 2 BvR 883/17, Rn. 24).

II) Mögliche Grundrechtsverletzung durch Rechtsvorschriften zur Einrichtung und verpflichtenden Nutzung des beAs

Des Weiteren erscheint es möglich, dass die einschlägigen Rechtsvorschriften (siehe oben A.III und A.IV) verfassungswidrig sind, sofern sie eine Auslegung dahingehend zulassen sollten, wie sie zuletzt der Bundesgerichtshof vorgenommen hat.

Danach solle es nur auf eine – tautologisch-zirkelschlüssige und damit inhaltsleere und undefinierbare – „Sicherheit im Rechtssinne“ ankommen (BGH a. a. O., Rn. 68, 72), die nach Ansicht des Bundesgerichtshofes zudem schon immer dann gegeben sein soll, wenn nicht „unbehebbare Sicherheitsmängel“ vorliegen (BGH a. a. O., Rn. 81 f.). Dies würde letztlich nicht ausschließen, dass selbst erhebliche Sicherheitsmängel nicht zu einer „Unsicherheit im Rechtssinne“ führen würden, sofern sie nur – irgendwie und irgendwann – behebbar sein sollten. Ferner dürften „unbehebbare Sicherheitsmängel“ stets einem ohnehin unerheblichen Restrisikobereich zuzuordnen sein, wenn sie nach aktuellem Stand der Technik gerade nicht ausgeschlossen werden können. Im Ergebnis wäre damit bei Zugrundelegung dieser richterlichen Auslegung das beA also schlechterdings immer „sicher im Rechtssinne“.

Sollte eine derartige Auslegung nicht erkennbar grob verfassungswidrig sein – was die Beschwerdeführer zunächst und in erster Linie vertreten –, so erscheint es zumindest

möglich, dass die einschlägigen Rechtsvorschriften (siehe oben A.III und A.IV) zu unbestimmt sind, um den verfassungsrechtlichen Anforderungen an die Bestimmung der Sicherheit des beAs zu genügen. Dabei wiegt umso schwerer, dass zudem eine gesetzliche Pflicht zur Nutzung des beAs besteht.

Es erscheint daher zumindest möglich, dass jedenfalls die Kombination aus Unbestimmtheit bezüglich der Sicherheitsanforderungen an das beA und der zugleich vorgeschriebenen Nutzungspflicht insofern zu einer „kollusiven", nachteilig-zusammenwirkenden Grundrechtsverletzung der Beschwerdeführer führen.

JJ) MÖGLICHE WEITERE GRUNDRECHTSVERLETZUNGEN

Aus den vorstehend benannten Gründen erscheint im Übrigen nicht nur eine Verletzung des Grundrechts auf Berufsfreiheit nach Artikel 12 Absatz 1 GG (i. V. m. Artikel 20 Absätze 2 und 3 GG) möglich, sondern auch gleichermaßen die Verletzung des von Artikel 14 Absatz 1 GG geschützten Rechts der Beschwerdeführer am eingerichteten und ausgeübten Betrieb ihrer Kanzleien. Zudem erscheint es zumindest möglich, dass die Beschwerdeführer durch die bestehende Pflicht zur Nutzung des ohne Ende-zu-Ende-Verschlüsselung ausgestatteten beAs auch in ihrem Grundrecht auf Unverletzlichkeit des Fernmeldegeheimnisses (Artikel 10 Absatz 1 GG) sowie in ihrem Grundrecht auf informationelle Selbstbestimmung und Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG) verletzt sind. Schließlich kommt jedenfalls auch eine Verletzung der von Artikel 2 Absatz 1 GG geschützten allgemeinen Handlungsfreiheit der Beschwerdeführer in Betracht; des Weiteren ist ferner auch eine Verletzung des Rechts auf Achtung der Kommunikation aus Artikel 8 EMRK sowie des Rechts auf Kommunikation und Schutz personenbezogener Daten nach den Artikeln 7 und 8 GRCh möglich (siehe unten B.II.1.d)).

5. Subsidiarität

Mit Beschreiten des Klageweges gegen die Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung zunächst vor dem Anwaltsgerichtshof Berlin und sodann letztinstanzlich vor dem Bundesgerichtshof haben die Beschwerdeführer den Rechtsweg erschöpft. Insbesondere haben sie gegen das Berufungsurteil des Bundesgerichtshofes zuletzt auch Anhörungsrüge erhoben; über diese wurde noch nicht entschieden.

Des Weiteren haben die Beschwerdeführer die Verfassungswidrigkeit der Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung in den Gerichtsverfahren mehrfach und ausführlich gerügt.

> Siehe etwa Schriftsatz zum AGH Berlin vom 15. Juni 2018, S. 47 f., 53 f.; Schriftsatz zum AGH Berlin vom 11. April 2019, S. 1-3; Schriftsatz an BGH vom 18. März 2020, S. 8 f. (Anlagenkonvolute 1a und 2a).

6. Annahmevoraussetzungen

Die Verfassungsbeschwerde erfüllt die Annahmevoraussetzungen des § 93a Absatz 2 BVerfGG, da ihr grundsätzliche verfassungsrechtliche Bedeutung zukommt und sie zur Durchsetzung der Grundrechte der Beschwerdeführer angezeigt ist, insbesondere weil ihnen bei Versagung der Entscheidung zur Sache ein besonders schwerer Nachteil entstehen würde.

a) Grundsätzliche verfassungsrechtliche Bedeutung

Nach der Rechtsprechung des Bundesverfassungsgerichts ist eine Verfassungsbeschwerde von grundsätzlicher verfassungsrechtlicher Bedeutung, wenn sie eine verfassungsrechtliche Frage aufwirft, die in der Rechtsprechung des Bundesverfassungsgerichts noch nicht geklärt ist und über den Einzelfall hinaus bedeutsam sowie

entscheidungserheblich ist (vgl. BVerfGE 90, 22 <24 f.>; 96, 245 <248>). Diese Voraussetzungen sind vorliegend erfüllt.

Die Frage, welche verfassungsrechtlichen Anforderungen an die Sicherheit des beAs als verpflichtend zu nutzendem, zentralen Kommunikationsmittel der Anwaltschaft zu stellen sind, ist bislang noch nicht durch das Bundesverfassungsgericht geklärt. Insbesondere hat das Bundesverfassungsgericht im Jahre 2017 die damals erhobene Verfassungsbeschwerde gegen die gesetzliche Pflicht zur Nutzung des beAs nicht zur Entscheidung angenommen und sich daher nicht weiter insbesondere mit der Sicherheit des beAs befasst (siehe oben B.I.3.d)aa)). Dies ist nunmehr möglich, nachdem gutachterlich und gerichtlich erwiesen ist, dass das beA – entgegen der damaligen Annahme des Bundesverfassungsgerichts – nicht über eine Ende-zu-Ende-Verschlüsselung verfügt.

Es stellt sich somit die bislang unbeantwortete – aber dringend klärungsbedürftige – verfassungsrechtliche Frage, welche Anforderungen an die Integrität und Vertraulichkeit des beAs als zentralem, verpflichtend zu nutzendem elektronischen Kommunikationssystem zu stellen sind, insbesondere im Hinblick auf den grundrechtlich gebotenen Schutz der anwaltlichen Berufsausübung unter besonderer Beachtung der anwaltlichen Verschwiegenheit als essentiellem Wesensmerkmal sowie dem von Verfassung wegen gebotenen Schutz des rechtsstaatlichen Instituts der freien und unabhängigen Advokatur.

Die Bedeutung dieser verfassungsrechtlichen Fragestellung ist dabei nicht nur in quantitativer Hinsicht von grundsätzlicher Bedeutung, da sie neben den Beschwerdeführern sämtliche über 150.000 zugelassene Rechtsanwältinnen und Rechtsanwälte – sowie alle künftig zugelassenen Rechtsanwältinnen und Rechtsanwälte – grundrechtswesentlich betrifft, sondern auch in qualitativer Hinsicht, weil es sich vorliegend um eine rechtsstaatlich bedeutsame Frage des verfassungsrechtlichen Schutzes des

rechtsstaatlich verbürgten Instituts der freien Advokatur handelt, die schließlich mittelbar auch alle Bürgerinnen und Bürger betrifft, die anwaltlichen Rechtsbeistand in Anspruch nehmen.

B) ZUR DURCHSETZUNG DER GRUNDRECHTE ANGEZEIGT; SCHWERE NACHTEILE

Die Verfassungsbeschwerde ist auch zur Durchsetzung der von den Beschwerdeführern geltend gemachten Grundrechte angezeigt, da ihnen durch die Versagung der Entscheidung zur Sache ein besonders schwerer Nachteil entstünde.

Nach der Rechtsprechung des Bundesverfassungsgerichts kann sich die „existentielle Betroffenheit eines Beschwerdeführers (…) vor allem aus dem Gegenstand der angegriffenen Entscheidung oder seiner aus ihr folgenden Belastung ergeben“ (BVerfGE 96, 245 <248>; vgl. auch BVerfGE 90, 22 <25 f.>). Wie bereits dargelegt, greift die Verpflichtung zur Nutzung des ohne Ende-zu-Ende-Verschlüsselung eingerichteten beAs tief in die Grundrechte der Beschwerdeführer, insbesondere in ihr Grundrecht auf freie Ausübung ihres Anwaltsberufes nach Artikel 12 Absatz 1 GG, indem in das Kernelement ihrer freien anwaltlichen Tätigkeit, die Verschwiegenheitspflicht als beruflicher Grundpflicht (§ 43a Absatz 2 BRAO), eingegriffen wird. Würden sich die Beschwerdeführer zudem weigern, dass beA zu nutzen, so zöge dies berufsrechtliche Konsequenzen bis letztlich hin zur Ausschließung von der Rechtsanwaltschaft nach sich, § 113 Absatz 1 i. V. m. § 114 Absatz 1 Nr. 5 BRAO.

II. BEGRÜNDETHEIT

Die Verfassungsbeschwerde ist auch begründet.

Sowohl die Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung als auch die hierzu ergangenen, dieses Verwaltungshandeln der BRAK billigenden Gerichtsurteile des Anwaltsgerichtshofes Berlin und des Bundesgerichtshofes (siehe oben A.I.-IV.) missachten grundlegend die hohen verfassungsrechtlichen Anforderungen, die an die Sicherheit des beAs als zentralem und verpflichtend zu nutzenden Kommunikationssystems für die Anwaltschaft zu stellen sind (siehe hierzu sogleich unten B.II.1.).

Der Bundesgerichtshof hat zudem in seinem letztinstanzlichen Berufungsurteil, ebenso wie vorinstanzlich der Anwaltsgerichtshof Berlin, bei der Beurteilung der Anforderungen an die Sicherheit des beAs die Reichweite und das Gewicht der Grundrechte der Beschwerdeführer, insbesondere des Grundrechts auf freiheitliche Ausübung ihres Anwaltsberufes unter besonderer Berücksichtigung des rechtsstaatlichen Instituts der freien und unabhängigen Advokatur im Rahmen seiner Auslegung der Rechtsvorschriften über die Einrichtung des beAs grob verkannt (siehe hierzu unten B.II.2). Zur Vermeidung von Wiederholungen und zur besseren Verständlichkeit wird dies im Folgenden vornehmlich ausgehend von dem letztinstanzlichen Berufungsurteil des Bundesgerichtshofes eingehend dargelegt.

Zudem rügen die Beschwerdeführer die Verfassungswidrigkeit der einschlägigen Rechtsvorschriften über die Einrichtung und Nutzungspflicht sowie die Sicherheitsanforderungen des beAs (siehe oben A.III. und A.IV.), weil sie insbesondere gegen den Vorbehalt des Gesetzes verstoßen und nicht dem rechtsstaatlichen Bestimmtheitsgebot gerecht werden. Dies gilt sowohl für die inzident gerügten, dem Urteil des Bundesgerichtshofes zugrunde liegenden als auch für die unmittelbar gerügten

Rechtsvorschriften, weshalb dies insoweit zusammengefasst dargelegt werden kann (B.II.3.).

1. Verfassungsrechtliche Anforderungen an die Sicherheit des beAs als zentralem und verpflichtend zu nutzenden Kommunikationssystem für die Anwaltschaft

Durch die Inbetriebnahme des beAs mit der beschriebenen HSM-Konstruktion, die ein zentrales Kompromittieren der gesamten anwaltlichen Kommunikation zulässt und den damit einhergegangenen Verzicht auf eine Ende-zu-Ende-Verschlüsselung hat die BRAK das beA in verfassungswidriger Weise eingerichtet. Der Anwaltsgerichtshof Berlin sowie nachgehend der Bundesgerichtshof haben dies unter Verkennung der Reichweite und Gewichtung der Grundrechte der Beschwerdeführer, insbesondere ihres Grundrechtes auf die freie Ausübung des Anwaltsberufes, für verfassungsgemäß erachtet.

a) Besonderer Schutz der freien und unabhängigen Advokatur

Wie bereits erörtert, sind von Verfassung wegen an die Sicherheit des beAs besonders gesteigerte Anforderungen zu stellen. Dies resultiert zum einen daraus, dass es sich bei dem beA um ein von allen Rechtsanwältinnen und Rechtsanwälten verpflichtend zu nutzendes, zentrales Kommunikationssystem handelt. Zum anderen ist die anwaltliche Verschwiegenheit, deren Schutz unmittelbar von der Sicherheit des beA-Systems abhängt, eine anwaltliche Grundpflicht (§ 43a Absatz 2 BRAO). Darüber hinaus ist sie – dies sei an dieser Stelle nochmals wiederholt – Grundpfeiler des rechtsstaatlich zu garantierenden Instituts der freien und unabhängigen Advokatur (Artikel 20 Absatz 3 GG) sowie „Grundlage des notwendigen Vertrauensverhältnisses zum Mandanten“ (BVerfG, Beschluss des Ersten Senats vom 12. Januar 2016 – 1 BvL 6/13, Rn. 55):

> „Der Rechtsanwalt ist als Organ der Rechtspflege (vgl. §§ 1 und 3 BRAO) dazu berufen, das Interesse seiner Mandanten zu vertreten (vgl. BVerfGE 10, 185 <198>). Seine Tätigkeit dient zugleich dem Allgemeininteresse an einer wirksamen und geordneten Rechtspflege (vgl. BVerfGE 15, 226 <234>; 34, 293 <302>; 37, 67 <77 ff.>; 72, 51 <63 ff.>). Voraussetzung für die Erfüllung dieser Aufgabe ist ein Vertrauensverhältnis zwischen Rechtsanwalt und Mandant (vgl. BVerfGE 110, 226 <252>)".
>
> BVerfG, Beschluss des Ersten Senats vom 13. Juni 2007 – 1 BvR 1550/03, Rn. 163.

> „Das Bundesverfassungsgericht hat mehrfach die fundamentale objektive Bedeutung der "freien Advokatur" hervorgehoben (vgl. BVerfGE 63, 266 <282> m. w. N.). Diese objektiv-rechtliche Bedeutung der anwaltlichen Tätigkeit und des rechtlich geschützten Vertrauensverhältnisses zwischen Rechtsanwalt und Mandant wird jedenfalls dann berührt, wenn wegen der Gefahr eines unbeschränkten Datenzugriffs ein Mandatsverhältnis von Anfang an mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet wird".
>
> BVerfGE 113, 29 (49).

Das nicht mit einer Ende-zu-Ende-Verschlüsselung eingerichtete beA beeinträchtigt das wie dargelegt verfassungsrechtlich besonders geschützte Vertrauensverhältnis zwischen Rechtsanwalt und Mandant nachhaltig, indem es die Gefahr eines unbeschränkten unzulässigen Datenzugriffs begründet.

B) SYSTEMWIDRIGE SUBSTITUTION ANWALTLICHER VERTRAULICHKEIT

Damit verträgt es sich erkennbar nicht, dass nunmehr an die Stelle der anwaltlichen Vertraulichkeit – für die immer die Rechtsanwältinnen und Rechtsanwälte selbst Garanten waren – nunmehr ein bloßes Vertrauen in die BRAK treten soll. Genau das ist es, was die BRAK selbst letztlich herbeigeführt hat, indem sie das beA so konzipiert hat, dass die gesamte Kommunikation über ein von ihr beziehungsweise ihren Dienstleistern betriebenes HSM gesteuert wird. Nochmals sei in diesem Zusammenhang die so anschauliche Formulierung aus dem von der BRAK selbst in Auftrag gegebenen Gutachten wiedergegeben:

> „Damit sie (die Praxis des Einsatzes eines HSMs, Anm. d. Verf.) für das beA geeignet ist, ist es erforderlich, dass die beA-Anwender als potentiell vom Bruch der Vertraulichkeit Bedrohte dem Auftraggeber und dem Betreiber des beA ausreichend vertrauen. Ob dies der Fall ist, kann im Rahmen dieses Gutachtens nicht beurteilt werden. Ist ausreichendes Vertrauen vorhanden, kann die hier aus technischer Sicht (Möglichkeit und Umfang des Schadens) als betriebsbehindernd riskant bewertete Praxis fortgesetzt werden".
>
> Veröffentlichtes Secunet-Gutachten a. a. O., S. 86 (Herv. d. Verf.)

Nicht nur die Rechtsanwältinnen und Rechtsanwälte als „beA-Anwender" sollen nunmehr der BRAK zu vertrauen haben, auch ihre Mandantinnen und Mandanten – mithin potentiell alle Bürgerinnen und Bürger – wären hierauf zurückgeworfen.

Ein Vertrauen in die BRAK – so vertrauenswürdig sie als Zusammenschluss der Rechtsanwaltskammern und Körperschaft des öffentlichen Rechts (§§ 176 f. BRAO) auch sein sollte – ist aber kein gleichwertiges „aliud" zur anwaltlichen Vertraulichkeit. Sie kann insoweit nur „minus" sein. Denn die BRAK ist nicht gleichermaßen an die anwaltlichen Berufspflichten gebunden wie die Rechtsanwältinnen und Rechtsanwälte. Sie steht auch in keiner unmittelbaren Mandantenbeziehung. Sie ist insofern kein direkter Teilnehmer am Rechtsverkehr.

Die Zwischenschaltung der BRAK als zentrale Kommunikationsinstanz im Rahmen des beAs und die damit einhergehende Substitution der anwaltlichen Vertraulichkeit durch eine Art „kammerliche Vertraulichkeit" muss insofern systemwidrig und damit auch verfassungswidrig erscheinen.

Der Entzug der anwaltlichen Selbstverantwortung, eigenständig über die Vertraulichkeit der eigenen Kommunikation entscheiden und diese sicherstellen zu können, verletzt die anwaltliche Berufsfreiheit bis ins Mark hinein und beschädigt das rechtsstaatlich vorausgesetzte Institut der freien und unabhängigen Advokatur nachhaltig.

So hat auch das Bundesverfassungsgericht insofern zutreffend festgestellt:

> „Ein verfassungsrechtlich geschütztes Vertrauen kann der Mandant eines Rechtsanwalts in dessen Verschwiegenheit jedenfalls nur insoweit entwickeln, als der Rechtsanwalt über entsprechende tatsächliche Möglichkeiten der Einflussnahme verfügt".
>
> BVerfG, Beschluss des Ersten Senats vom 13. Juni 2007 – 1 BvR 1550/03, Rn. 166.

Wird den Beschwerdeführern – sowie sämtlichen Rechtsanwältinnen und Rechtsanwälten – durch die Pflicht zur Nutzung des nicht Ende-zu-Ende-verschlüsselten beAs die tatsächliche Möglichkeit der Einflussnahme auf die anwaltliche Verschwiegenheit entzogen, so wird diese letztlich verfassungsrechtlich vollständig „entkernt".

c) Fortbestand anwaltlicher Vertraulichkeit nur bei Ende-zu-Ende-Verschlüsselung

Dabei ist es möglich, die anwaltliche Vertraulichkeit auch bei Nutzung moderner elektronischer Kommunikation zu wahren. Die Ende-zu-Ende-Verschlüsselung böte hierfür die technische Möglichkeit. Sie würde gewährleisten, dass die Verantwortung für den Schutz von Nachrichteninhalten bei den Rechtsanwältinnen und Rechtsanwälten verbleibt, indem nur diesen das Ver- und Entschlüsseln ihrer Nachrichten möglich wäre. Das Vertrauen würde mithin gerade nicht auf eine externe Instanz – wie im Falle des beAs: die BRAK – verlagert werden.

Die Ende-zu-Ende-Verschlüsselung ist die derzeit einzige technische Entwicklung, die eine vertrauliche und damit sichere elektronische Kommunikation gewährleisten kann. Es ist von Verfassung wegen geboten, sie gerade beim beA einzusetzen, um eine freiheitliche und unabhängige anwaltliche Berufsausübung auch im digitalen Zeitalter zu gewährleisten.

D) WEITERE VERLETZTE RECHTE

Während im Folgenden zur Vermeidung von Wiederholungen die Verfassungswidrigkeit der gerügten Akte der öffentlichen Gewalt in Bezug auf die Pflicht zur Nutzung des ohne Ende-zu-Ende-Verschlüsselung eingerichteten beAs vornehmlich an dem zuvörderst betroffenen Grundrecht der Beschwerdeführer auf anwaltliche Berufsfreiheit nach Artikel 12 Absatz 1 GG dargelegt wird, rügen die Beschwerdeführer aus denselben Gründen auch die Verletzung der folgenden Grundrechte, deren Schutzbereiche vorliegend eröffnet sind:

AA) RECHT AM EINGERICHTETEN UND AUSGEÜBTEN KANZLEIBETRIEB (ARTIKEL 14 ABSATZ 1 GG)

Das Bundesverfassungsgericht hat soweit ersichtlich bislang offen gelassen, ob der Betrieb einer Rechtsanwaltskanzlei von Artikel 14 Absatz 1 GG geschützt ist (BVerfG, Nichtannahmebeschluss vom 15. März 2000 – 1 BvR 230/00, juris-Rn. 18; BVerfGE 45, 272 <296>). In Literatur und Rechtsprechung wird eine Einbeziehung von Freiberuflern in den Schutzbereich des Artikels 14 Absatz 1 GG ganz herrschend anerkannt (vgl. zum Schutz einer Arztpraxis durch Artikel 14 Absatz 1 GG etwa BGHZ 81, 21 <33> m. w. N.; zum Schutz einer Anwaltskanzlei durch Artikel 14 Absatz 1 GG siehe Leisner, NJW 1974, 478).

Jedenfalls ist der Rechtsprechung des Bundesverfassungsgerichts zu entnehmen, dass eine Verletzung des Grundrechts am eingerichteten und ausgeübten Betrieb einer Rechtsanwaltskanzlei dann gegeben sein kann, wenn ein ungerechtfertigter Eingriff in die „Substanz der Anwaltskanzlei“ vorliegt (BVerfGE 45, 272 <296>). Dies ist vorliegend der Fall.

Entsprechend der Rechtsprechung des Bundesgerichtshofes zur Arztpraxis gehört zum geschützten Gewerbebetrieb die „Gesamtheit alles dessen, was die gegenständliche und personelle Grundlage der Tätigkeit des praktizierenden (hier: Rechtsanwalts) bei der Erfüllung der ihm obliegenden Aufgabe bildet“ (BGHZ 81, 21 <33>).

Die Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung beeinträchtigt insofern den Kanzleibetrieb der Beschwerdeführer nachhaltig, weil sie zu dessen Nutzung gesetzlich verpflichtet sind. Das beA stellt damit eine zentrale Grundlage anwaltlicher Tätigkeit dar.

BB) RECHT AUF UNVERLETZLICHKEIT DES FERNMELDEGEHEIMNISSES (ARTIKEL 10 ABSATZ 1 GG)

Des Weiteren ist auch das Grundrecht der Beschwerdeführer auf Unverletzlichkeit des Fernmeldegeheimnisses (Artikel 10 Absatz 1 GG) beeinträchtigt.

Den Schutzbereich des von Artikel 10 Absatz 1 GG grundrechtlich verbürgten Fernmeldegeheimnisses definiert das Bundesverfassungsgericht wie folgt:

> „Brief-, Post- und Fernmeldegeheimnis gewährleisten die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Informationen und schützen damit zugleich die Würde des Menschen (vgl. BVerfGE 67, 157 [171]; 106, 28 [35]; 110, 33 [53]; Dürig, in: Maunz/Dürig, Grundgesetz, Loseblatt [Stand: Dezember 1973], Art. 10 Rn. 1).
>
> Art. 10 GG schützt die private Fernkommunikation. Brief-, Post- und Fernmeldegeheimnis gewährleisten die Vertraulichkeit der individuellen Kommunikation, wenn diese wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen ist und deshalb in besonderer Weise einen Zugriff Dritter – einschließlich staatlicher Stellen – ermöglicht. Brief-, Post- und Fernmeldegeheimnis sind wesentlicher Bestandteil des Schutzes der Privatsphäre; sie schützen vor ungewollter Informationserhebung und gewährleisten eine Privatheit auf Distanz (vgl. Gusy, in: v. Mangoldt/Klein/Starck, Grundgesetz, 5.Aufl. [2005], Art. 10 Rn. 19).

> Das Fernmeldegeheimnis schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs (vgl. BVerfGE 67, 157 [172]; 106, 28 [35 f.]). Die Beteiligten sollen weitestgehend so gestellt werden, wie sie bei einer Kommunikation unter Anwesenden stünden.
>
> Das Grundrecht ist entwicklungsoffen und umfasst nicht nur die bei Entstehung des Gesetzes bekannten Arten der Nachrichtenübertragung, sondern auch neuartige Übertragungstechniken (vgl. BVerfGE 46, 120 [144]). Die Reichweite des Grundrechts beschränkt sich daher nicht auf die früher von der Deutschen Bundespost angebotenen Fernmeldedienste, sondern erstreckt sich auf jede Übermittlung von Informationen mit Hilfe der verfügbaren Telekommunikationstechniken. Auf die konkrete Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung) und Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) kommt es nicht an (vgl. BVerfGE 106, 28 [36]).
>
> (…)
>
> Das Fernmeldegeheimnis schützt in erster Linie die Vertraulichkeit der ausgetauschten Informationen und damit den Kommunikationsinhalt gegen unbefugte Kenntniserlangung durch Dritte.
>
> BVerfGE 115, 166 (182 f.).

Bei dem beA handelt es sich um ein elektronisches Fernkommunikationsmittel im vorstehend beschriebenen Sinne. Die Pflicht zur Nutzung des beAs verbunden mit dem Umstand, dass dieses ohne Ende-zu-Ende-Verschlüsselung eingerichtet ist, beeinträchtigt die Vertraulichkeit der über das beA abzuwickelnden anwaltlichen Kommunikation. Insofern ist auch der Schutzbereich des Artikels 10 Absatz 1 GG vorliegend betroffen.

cc) Recht auf informationelle Selbstbestimmung (Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG)

Weiter ist auch das Grundrecht der Beschwerdeführer auf informationelle Selbstbestimmung nach Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG beeinträchtigt.

In seinem grundlegenden „Volkszählungs"-Urteil hat das Bundesverfassungsgericht das sog. Grundrecht auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht nach Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG abgeleitet und Schutzbereich wie Eingriffsvoraussetzungen wie folgt abgesteckt:

> „1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des GG Art 2 Abs 1 in Verbindung mit GG Art 1 Abs 1 umfa(ss)t. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.
>
> 2. Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen mu(ss). Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken".
>
> BVerfGE 65, 1 (Leitsätze 1 und 2; Herv d. Verf.).

Insofern ist an dieser Stelle bereits vorzugreifen, dass der Gesetzgeber keine hinreichenden „organisatorische(n) und verfahrensrechtliche(n) Vorkehrungen" betreffend die Sicherheit des beAs getroffen hat, „welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken" könnten (siehe hierzu ausführlich unten B.II.3.).

DD) RECHT AUF GEWÄHRUNG DER VERTRAULICHKEIT UND INTEGRITÄT INFORMATIONSTECHNISCHER SYSTEME (ARTIKEL 2 ABSATZ 1 I. V. M. ARTIKEL 1 ABSATZ 1 GG)

Ausgehend von dem Grundrecht auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht zudem das noch weitergehende Grundrecht auf Gewährung

der Vertraulichkeit und Integrität informationstechnischer Systeme wie folgt entwickelt:

> „Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist (…) anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.
>
> (…)
>
> Geschützt vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.
>
> (…)
>
> Der grundrechtliche Schutz der Vertraulichkeits- und Integritätserwartung besteht unabhängig davon, ob der Zugriff auf das informationstechnische System leicht oder nur mit erheblichem Aufwand möglich ist. Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht allerdings nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt. Soweit die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf.
>
> BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07, Rn. 203-206 (Herv. d. Verf.).

Auch insofern haben die Beschwerdeführer ein grundrechtlich geschütztes Interesse daran, dass die von ihnen über das beA verpflichtend auszutauschenden Nachrichten vertraulich bleiben.

EE) RECHT AUF ALLGEMEINE HANDLUNGSFREIHEIT (ARTIKEL 2 ABSATZ 1 GG)

Im Übrigen wird gerügt, dass die Beschwerdeführer jedenfalls durch die mit der Verfassungsbeschwerde angegriffenen Ake der öffentlichen Gewalt in ihrem Grundrecht auf allgemeine Handlungsfreiheit aus Artikel 2 Absatz 1 GG verletzt werden, das generell vor rechtwidrigen, insbesondere unverhältnismäßigen staatlichen Maßnahmen schützt. Dies gilt insbesondere, soweit eine Verletzung des Rechtsstaatsprinzips (Artikel 20 Absatz 3 GG) durch Missachtung des Instituts der freien Advokatur geltend gemacht wird sowie ferner in Bezug auf den Beschwerdeführer zu 2., sofern ihm als Unionsbürger der Schutz aus Artikel 12 Absatz 1 GG nicht unmittelbar, sondern mittelbar über Artikel 2 Absatz 1 GG gewährt werden sollte (siehe hierzu oben B.I.1.).

FF) RECHT AUF ACHTUNG DER KORRESPONDENZ (ARTIKEL 8 ABSATZ 1 EMRK)

Die Einrichtung des beAs ohne Ende-zu-Ende-Verschlüsselung in Verbindung mit der gesetzlich angeordneten Nutzungspflicht verletzt die Beschwerdeführer ferner ihrem Recht auf Achtung ihrer Korrespondenz aus Artikel 8 Absatz 1 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 04. November 1950, zuletzt geändert durch Protokoll Nr. 14 vom 13. Mai 2004(EMRK).

Nach der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) schützt Artikel 8 Absatz 1 EMRK die elektronische Korrespondenz und die Daten einer Rechtsanwaltskanzlei (EGMR, Urteil vom 16. Oktober 2007 – 74336/01 Wieser u. a. vs. Österreich , Rn. 42-46; EGMR, Urteil vom 03. April 2007 – 62617/00 Copland vs. Vereinigtes Königreich, Rn. 41). Die elektronische anwaltliche Korrespondenz über das beA unterfällt damit dem Anwendungsbereich des Artikels 8 Absatz 1 EMRK.

Artikel 8 Absatz 2 EMRK verlangt, dass ein Eingriff in die Achtung der Korrespondenz "notwendig" ist und nicht nur "nützlich" oder "wünschenswert" (vgl. EGMR, Urteil vom 29. April 1999 – 25088/94 Chassagnou u. a. vs. Frankreich, Rn. 112). Insofern kann die Einrichtung des beAs – allzumal ohne sichere Ende-zu-Ende-Verschlüsselung – sowie der ausnahmslose gesetzliche Zwang zur Nutzung des beAs unter keinem Gesichtspunkt als „notwendig“ angesehen werden. Eine sichere Kommunikation mit den Gerichten kann zweifelsfrei auch ohne – und gerade ohne – das beA stattfinden, sei es auf dem herkömmlichen Postwege oder auch über ein – bei Erfolg der Verfassungsbeschwerde – künftig Ende-zu-Ende-verschlüsseltes beA.

Des Weiteren ist es auch in der Rechtsprechung des EGMR anerkannt, dass die anwaltliche Korrespondenz – insbesondere im Hinblick auf die Wahrung des Mandatsgeheimnisses – durch die anwaltliche Schweigepflicht (vgl. EGMR, Urteil vom 16. Dezember 2007 – 74336/01 Wieser u. a. vs. Österreich, Rn. 66 f.) in gesteigertem Maße schutzbedürftig ist und daher an eingreifende staatliche Maßnahmen besonders hohe Anforderungen zu stellen und diese entsprechend streng zu prüfen sind (vgl. EGMR, Urteil vom 09. April 2009 – 19856/04 Kolesnichenko vs. Russland, Rn. 31).

Bezüglich der Rechtsverletzung durch das ohne Ende-zu-Ende-Verschlüsselung eingerichtete, verpflichtend zu nutzende beA sowie die dies für rechtmäßig erachtenden Gerichtsurteile gelten die übrigen Ausführungen zu den Grundrechtseingriffen entsprechend (vgl. oben B.I.4.d) und B.II.1.a)-c) sowie B.II.2. und B.II.3.).

GG) RECHT AUF ACHTUNG DER KORRESPONDENZ UND AUF SCHUTZ PERSONENBEZOGENER DATEN (ARTIKEL 7 UND ARTIKEL 8 GRCH)

Ferner wird, insbesondere mit Blick auf die österreichische Staatsangehörigkeit des Beschwerdeführers zu 2.. die Verletzung des Rechts auf Achtung der Korrespondenz aus Artikel 7 der Charta der Grundrechte der Europäischen Union (ABl. EU C

326/391 vom 26. Oktober 2012; im Folgenden: GRCh) sowie des Rechts auf Schutz personenbezogener Daten nach Artikel 8 Absatz 1 GRCh gerügt. Die beiden Grundrechte bilden eine „einheitliche Schutzverbürgung", die sich insbesondere auch auf eine „berufliche Tätigkeit" erstreckt (BVerfG, Beschluss des Ersten Senats vom 06. November 2019 – 1 BvR 276/17, Rn. 99 m. w. N.).

Bezüglich der Verletzung der Rechte durch das ohne Ende-zu-Ende-Verschlüsselung eingerichtete, verpflichtend zu nutzende beA sowie die dies für rechtmäßig erachtenden Gerichtsurteile gelten die übrigen Ausführungen zu den Grundrechtseingriffen entsprechend (vgl. oben B.I.4.d) und B.II.1.a)-c) sowie B.II.2. und B.II.3.).

2. Missachtung der verfassungsrechtlichen Anforderungen an das beA durch den Bundesgerichtshof

Der Bundesgerichtshof hat die vorstehend beschriebenen verfassungsrechtlichen Anforderungen an die technische Ausgestaltung des beAs zur Gewährleistung einer sicheren elektronischen Kommunikation, die geeignet ist, die anwaltliche Vertraulichkeit zu schützen, grob verkannt und dabei insbesondere auch die Reichweite sowie das Gewicht des Grundrechts der Beschwerdeführer auf freie Ausübung des Anwaltsberufes nicht zutreffend erfasst.

Wie wenig intensiv sich das Gericht mit den verfassungsrechtlichen und grundrechtlichen Anforderungen an die Sicherheit des beAs befasst hat, zeigt sich bereits daran, dass es diesem Komplex in seinem 109 Randnummern umfassenden Urteil letztlich nur eine einzige Randnummer gewidmet hat; diese lautet wie folgt:

> „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".
>
> BGH a. a. O., Rn. 106 (Herv. d. Verf.)

Soweit das Gericht hier auf die – von ihm selbst aufgestellten – Kriterien verweist, nach denen sich seines Erachtens soll beurteilen lassen können, ob das beA „sicher" ist, seien noch die folgenden Passagen zitiert:

> „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".
>
> BGH a. a. O., Rn. 68 (Herv. d. Verf.).
>
> „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.
>
> BGH a. a. O., Rn. 72 (Herv. d. Verf.)

> 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.
>
> BGH a. a. O., Rn. 81 (Herv. d. Verf.).

A) VERKÜRZTE ANWENDUNG VERFASSUNGSGERICHTLICHER RECHTSPRECHUNG ZU SICHERHEITSANFORDERUNGEN

Der Bundesgerichtshof hat bei seiner Beurteilung der verfassungsmäßigen Anforderungen an die Sicherheit des beAs die von ihm in Bezug genommene Rechtsprechung des Bundesverfassungsgerichts (BVerfGE 125, 260 <326>) verkürzt wiedergegeben (a. a. O., Rn. 106), indem er lediglich den Satz zitiert hat:

> „Die Verfassung gibt nicht detailgenau vor, welche Sicherheitsmaßgaben im Einzelnen geboten sind (vgl. zu § 113a TKG: BVerfGE 125, 260, 326)".
>
> BGH a. a. O., Rn. 106.

Indes führt das Bundesverfassungsgericht im unmittelbar nachfolgenden Satz weiter aus:

> „Im Ergebnis muss jedoch ein Standard gewährleistet werden, der unter spezifischer Berücksichtigung der Besonderheiten (…) ein besonders hohes Maß an Sicherheit gewährleistet".
>
> BVerfGE 125, 260 (326).

Dabei wurde das vorstehend wiedergegebene vollständige Zitat von den Bevollmächtigten vollumfänglich vorgetragen.

> Schriftsatz zum BGH vom 18. März 2020, S. 9.

Indem der Bundesgerichtshof lediglich auf die aus dem Zusammenhang gerissene Aussage des Bundesverfassungsgerichtes abstellt, dass die Verfassung keine „detailgenauen“ Vorgaben für die Sicherheit von IT-Systemen enthalte, verkennt er die tatsächliche Reichweite der verfassungsrechtlichen Anforderungen, wie sie das Bundesverfassungsgericht für geboten erachtet. Der Umstand, dass die Verfassung nicht „detailgenau“ vorgibt, welche konkreten Sicherheitsanforderungen im Einzelfall bestehen müssen, bedeutet schließlich nicht – anders als es der Bundesgerichtshof auch im Weiteren versucht darzustellen –, dass die Verfassung keinerlei Anforderungen an die Sicherheit von IT-Systemen stellt. Dies wird eben durch den vom Bundesgerichtshof vernachlässigten Nachsatz des Bundesverfassungsgerichts deutlich, der klarstellt, dass – gleichwohl – unter bestimmten Umständen ein „besonders hohes Maß an Sicherheit“ gewährleistet werden muss.

Und genau solche besonderen Umstände liegen in Bezug auf das beA vor. Wie dargelegt, sind an die Sicherheit des beAs besonders hohe Sicherheitsanforderungen zu stellen, weil es sich um ein zentrales, verpflichtend von allen Rechtsanwältinnen und Rechtsanwälten zu nutzendes Kommunikationssystem handelt. Daher muss das beA in besonderer Weise den Schutz der anwaltlichen Vertraulichkeit – des Kernelements der grundrechtlich von Artikel 12 Absatz 1 GG geschützten anwaltlichen Berufsfreiheit – gewährleisten.

Der Bundesgerichtshof hat mithin offenkundig verkannt, dass von Verfassung wegen in Einklang mit der Rechtsprechung des Bundesverfassungsgerichts in Bezug auf das beA „ein besonders hohes Maß an Sicherheit“ gewährleistet sein muss.

B) UNZULÄNGLICHKEIT DER RICHTERLICH ENTWICKELTEN RECHTSFIGUR „SICHER IM RECHTSSINNE“

Stattdessen hat der Bundesgerichtshof im Anschluss an den Anwaltsgerichtshof Berlin durch eine Art richterliche Rechtsfortbildung die Formel der „Sicherheit im Rechtssinne“ zum Ausgangspunkt seiner Entscheidung gemacht (BGH a. a. O., Rn. 68, 72). Diese setze insbesondere „nicht eine Freiheit von jeglichen Risiken voraus“, sondern nur, „dass ein Schadenseintritt hinreichend unwahrscheinlich“ sei, sodass „insgesamt ein Zustand als sicher gelten könne, der unter Berücksichtigung der Funktionalität und Standards frei von unvertretbaren Risiken sei“ (BGH a. a. O., Rn. 68). Risiken für die Vertraulichkeit müssten nur „möglichst weitgehend ausgeschlossen“ sein (BGH a. a. O., Rn. 68).

Diese Formel wird der soeben zitierten Rechtsprechung des Bundesverfassungsgerichts (BVerfGE 125, 260 <326>) nicht gerecht. Sie verkennt schon dem Grunde nach, das vorliegend aufgrund der bereits dargelegten Besonderheit des beAs und seiner damit einhergehenden Relevanz für den Schutz der anwaltlichen Berufsfreiheit sowie der rechtsstaatlich zu garantierenden freien Advokatur besonders hohe Anforderungen an die Sicherheit des beAs zu stellen sind.

Es reicht daher gerade nicht aus, dass Risiken für die Vertraulichkeit der anwaltlichen Kommunikation lediglich „möglichst weitgehend“ ausgeschlossen sind, vielmehr müssen sie soweit wie nur möglich ausgeschlossen sein.

Das bedeutet konkret, dass entgegen der Ansicht des Bundesgerichtshofes (a. a. O., Rn. 106) immer dann, wenn wie vorliegend mit der Ende-zu-Ende-Verschlüsselung eine Technologie zur Verfügung steht, die geeignet ist, die anwaltliche Vertraulichkeit in besonders hohem Maße zu schützen, diese auch einzusetzen ist. Insoweit reduziert

sich das vom Bundesgerichtshof eingeräumte Ermessen der BRAK bezüglich der Sicherheitsanforderungen an das beA auf Null.

Die vom Bundesgerichtshof bemühten Kriterien „hinreichend unwahrscheinlich“ und „unvertretbares Risiko“ sind zudem ihrerseits vollkommen unbestimmt und damit vollends ungeeignet, um die Sicherheit des beAs im Lichte der Verfassung und insbesondere der Grundrechte der Beschwerdeführer angemessen beurteilen zu können. Die richterlich vom Anwaltsgerichthof Berlin entwickelte und vom Bundesgerichtshof übernommene Formel „sicher im Rechtssinne“ bleibt letztlich ein zirkelschlüssiges und inhaltsleeres Konstrukt.

Dies wird umso deutlicher, wenn der Bundesgerichtshof die Formel noch dahingehend erweitert, dass das beA stets als „sicher im Rechtssinne“ anzusehen sei, solange es sich um Sicherheitsrisiken handele, die „behebbar“ sind (BGH a. a. O., Rn. 81). Positiv formuliert ist damit „sicher im Rechtssinne“ auch was unsicher ist, aber sicher sein könnte. Selbst gravierende Sicherheitsmängel würden danach nicht ausreichen, um eine „Unsicherheit im Rechtssinne“ zu begründen, solange sie nur – irgendwie, irgendwann – behebbar sind.

c) Unzureichende Risikobeurteilung nach Maßgabe verfassungsgerichtlicher Rechtsprechung

Die Risikobeurteilung des Bundesgerichtshofes weist zudem einen weiteren „blinden Fleck“ auf. So betrachtet der Bundesgerichtshof lediglich die Eintrittswahrscheinlichkeit eines möglichen Schadens aufgrund eines Sicherheitsmangels, lässt dabei aber das Schadensausmaß weitgehend unbeachtet (vgl. oben BGH a. a. O., Rn. 68, 106). Dies lässt bereits die abwertend klingende Formulierung erkennen, mit der die verfassungsrechtliche Beurteilung eingeleitet wird:

> „Die Wahl der Verschlüsselungsmethode betrifft allein die Vertraulichkeit der Kommunikation und damit mittelbar das anwaltliche Vertrauensverhältnis zum Mandanten“.
>
> BGH a. a. O., Rn. 106 (Herv. d. Verf.).

Die Hervorhebung, dass die Nachrichten-Verschlüsselung im beA „allein“, mithin „nur“, die Vertraulichkeit der Anwaltskommunikation betreffe, zeugt davon, welch geringen Wert der Bundesgerichtshof offenbar diesem Kernelement freier anwaltlicher Berufstätigkeit zuzusprechen geneigt ist.

Der Bundesgerichtshof verkennt damit offenkundig, dass eine zentrale Kompromittierung der gesamten anwaltlichen über das beA verpflichtend abzuwickelnden Kommunikation – die gutachterlich erwiesen ist und auch von ihm selbst nicht bestritten wird (siehe oben B.I.3.d)dd), BGH a. a. O., Rn. 72-81) – einen erheblichen Eingriff in die anwaltliche Berufsausübungsfreiheit der Beschwerdeführer – sowie aller Rechtsanwältinnen und Rechtsanwälte – darstellt. Das Urteil des Bundesgerichtshofes beruht damit auf einer grundsätzlich unrichtigen Anschauung von der Bedeutung des Grundrechts der Beschwerdeführer auf freie Ausübung ihres Anwaltsberufes und einer unrichtigen Einschätzung des Gewichts dieses Grundrechts (vgl. BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 18. April 2018 – 2 BvR 883/17, Rn. 24 m. w. N.).

Nach ständiger Rechtsprechung des Bundesverfassungsgerichts kommt es bei Risikobeurteilungen stets auf das Verhältnis zwischen Eintrittswahrscheinlichkeit und Ausmaß eines Schadens an (siehe nur BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 18. Februar 2010 – 2 BvR 2502/08, Rn. 12 m. w. N.). Dabei gilt, dass „die Wahrscheinlichkeit des Eintritts eines Schadensereignisses, die (…) hingenommen werden darf, so gering wie möglich sein muss, und zwar um so geringer, je schwerwiegender die Schadensart und die Schadensfolgen, die auf dem Spiel stehen, sein können“ (BVerfGE 49, 89 <138>).

In Anbetracht des erheblichen Schadensausmaßes in Gestalt einer zentralen Kompromittierung sämtlicher über das beA erfolgender Anwaltskommunikation, muss die Wahrscheinlichkeit dieses Schadensereignisses mithin „so gering wie möglich“ sein. Mit diesem vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Maßstab zur Beurteilung von Risiken im Recht ist die vom Bundesgerichtshof selbstentwickelte Formel der „Sicherheit im Rechtssinne“, die gerade nicht auf eine größtmögliche Sicherheit ausgerichtet ist und ausdrücklich außer Acht lässt, ob die Wahrscheinlichkeit eines Schadensereignisses gemindert werden kann, nicht vereinbar, vgl.:

> „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“.
>
> BGH a. a. O., Rn 106.

Der Bundesgerichtshof hat sich insofern der verfassungsrechtlich gebotenen Prüfung, dass bei Einrichtung des beAs mit einer Ende-zu-Ende-Verschlüsselung die Wahrscheinlichkeit einer zentralen Kompromittierung der über das System ausgetauschten Nachrichten deutlich gemindert wäre, vollständig entzogen.

D) UNZULÄNGLICHE ANWENDUNG DES VERFASSUNGSRECHTLICHEN VERHÄLTNISMÄßIGKEITSGRUNDSATZES

Der Bundesgerichtshof hat zudem den verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit nur unzulänglich auf die Frage der verfassungsrechtlich gebotenen Sicherheit des beAs angewandt. Die Anwendung des Verhältnismäßigkeitsgrundsatzes in Bezug auf die einschlägigen Rechtsvorschriften zur Einrichtung und Sicherheit des beAs hat er einer nicht ausreichenden oberflächlichen verfassungsrechtlichen Prüfung unterzogen (siehe BGH a. a. O., Rn. 99).

Der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit verlangt, dass ein Grundrechtseingriff einem legitimen Zweck dient und als Mittel zu diesem Zweck geeignet, erforderlich und angemessen ist (st. Rspr., siehe nur BVerfGE 109, 279 <335 ff.>; 115, 320 <345>). Bei Eingriffen in die Berufsausübung, wie vorliegend, gebietet der Verhältnismäßigkeitsgrundsatz nach der gefestigten Rechtsprechung des Bundesverfassungsgerichts, dass „nicht ein anderes, gleich wirksames aber das Grundrecht nicht oder doch weniger fühlbar einschränkendes Mittel“ hätte gewählt werden können (BVerfGE 30, 292 <316>).

Eine Befassung damit, ob die Ende-zu-Ende-Verschlüsselung des beAs in diesem Sinne ein milderes Mittel darstellt, weil hierdurch die Sicherheit des Nachrichtenverkehrs und damit der grundrechtlich gebotene Schutz der anwaltlichen Vertraulichkeit besser verwirklicht werden kann, lässt die Urteilsbegründung indes gänzlich vermissen. Dabei hatten die Beschwerdeführer dies bereits – leider ebenfalls unerhört – im vorinstanzlichen Verfahren vorgetragen.

> Siehe Schriftsatz zum AGH Berlin vom 11. April 2019, S. 1-3.

Die Frage, ob die Einrichtung des beAs mit einer Ende-zu-Ende-Verschlüsselung ein milderes Mittel darstellt und somit die von der BRAK gewählte HSM-Konstruktion eine unangemessene Grundrechtsbeeinträchtigung darstellt, ist geradezu die verfassungsrechtliche Kernfrage des Rechtsstreits. Der Bundesgerichtshof wirft sie nicht einmal auf. Stattdessen lässt er dies ausdrücklich „dahingestellt“; nochmals:

> „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“.
>
> BGH a. a. O, Rn.106

Damit missachtet der Bundesgerichtshof in eklatanter Weise die Reichweite der von Artikel 12 Absatz 1 GG geschützten Berufsausübungsfreiheit der Beschwerdeführer, indem er die verfassungsrechtlich gebotene Verhältnismäßigkeitsprüfung unterlässt, ob die Einrichtung des beAs mit einer Ende-zu-Ende-Verschlüsselung ein milderes Mittel gewesen wäre. Damit verkürzt er in verfassungswidriger Weise den Grundrechtsschutz der Beschwerdeführer.

Zudem gilt nach der Rechtsprechung des Bundesverfassungsgerichts:

> „Je empfindlicher die Berufsausübenden in ihrer Berufsfreiheit beeinträchtigt werden, desto stärker müssen die Interessen des Gemeinwohls sein, denen diese Regelung zu dienen bestimmt ist".
>
> BVerfGE 30, 292 (316).

Auch dieser Maßstab findet sich in der Entscheidung des Bundesgerichtshofes an keiner Stelle wieder. Der Bundesgerichtshof hat es unterlassen, im Rahmen seiner ohnehin äußerst oberflächlichen Grundrechtsprüfung zu bewerten, wie intensiv die anwaltliche Berufsfreiheit der Beschwerdeführer durch die Pflicht zur Nutzung des nicht Ende-zu-Ende-verschlüsselten beAs beeinträchtigt wird. So findet sich in den Urteilsgründen auch keine weitere Auseinandersetzung damit, dass die von der BRAK gewählte HSM-Konstruktion ein zentrales Kompromittieren sämtlicher über das beA abgewickelter Korrespondenz ermöglicht und damit einen schwerwiegenden Eingriff in die grundrechtlich und verfassungsrechtlich unter besonderem Schutz stehende anwaltliche Vertraulichkeit darstellt.

Zusammengefasst hat der Bundesgerichtshof damit weder den mit der Pflicht zur Nutzung des nicht Ende-zu-Ende-verschlüsselten beAs einhergehenden Eingriff in die Grundrechte der Beschwerdeführer zutreffend gewichtet noch diesen auch nur ansatzweise einer Verhältnismäßigkeitsprüfung im Hinblick auf die Gebotenheit der Wahl des milderen Mittels – hier: der Ende-zu-Ende-Verschlüsselung – unterzogen.

e) Verfassungswidrige Auslegung der Rechtsvorschriften über die Sicherheit des beAs

Aus den vorstehend benannten Gründen hat der Bundesgerichtshof auch die Rechtsvorschriften über die Einrichtung des beAs als „sicheren Übermittlungsweg“ im Sinne des § 19 Absatz 1 Satz 1 RAVPV sowie zur Pflicht der BRAK nach § 20 Absatz 1 Satz 2 RAVPV „fortlaufend zu gewährleisten, dass die in § 19 Absatz 1 (RAVPV) genannten Personen und Stellen miteinander sicher elektronisch kommunizieren können“, nicht verfassungskonform ausgelegt.

Die zur Auslegung richterlich entwickelte Formel „sicher im Rechtssinne“ genügt wie aufgezeigt nicht den verfassungsrechtlichen Anforderungen der vom Bundesverfassungsgericht entwickelten Maßstäbe zur Beurteilung von Risiken im Recht und verkennt zudem das Gewicht des Grundrechts der Beschwerdeführer aus Artikel 12 Absatz 1 GG auf freie Ausübung ihrer anwaltlichen Tätigkeit, indem es seinen Wesensgehalt in Gestalt der anwaltlichen Verschwiegenheit als Grundlage jedes Mandatsverhältnisses nicht hinreichend gewürdigt hat (siehe oben B.II.2.a)-c)).

3. Verfassungswidrigkeit der Vorschriften zu den Sicherheitsanforderungen an das beA

Die Beschwerdeführer rügen des Weiteren die Verfassungswidrigkeit der Vorschriften zur Einrichtung und Nutzungspflicht sowie zu den Sicherheitsanforderungen des beAs; zum einen mittelbar, soweit sie dem Urteil des Bundesgerichtshof zugrunde liegen (siehe oben A.III) sowie auch unmittelbar, soweit bestimmte Vorschriften hierzu überwiegend noch in Kraft treten werden (siehe oben A.IV). Zur Vermeidung von Wiederholungen wird dies im Folgenden zusammengefasst dargelegt.

Gerügt wird insbesondere der Verstoß gegen den Vorbehalt des Gesetzes sowie die Unbestimmtheit der Regelungen und damit die Verletzung der Grundrechte der Beschwerdeführer, insbesondere ihrer Berufsfreiheit nach Artikel 12 Absatz 1 GG.

Das Grundrecht auf Berufsausübung kann gemäß Artikel 12 Absatz 1 Satz 2 GG „durch Gesetz oder aufgrund eines Gesetzes“ beschränkt werden. Nach Art. 80 Absatz 1 GG kann die Bundesregierung durch Gesetz ermächtigt werden, Rechtsverordnungen zu erlassen. Dabei müssen allerdings gemäß Artikel 80 Absatz 1 Satz 2 GG „Inhalt, Zweck und Ausmaß der erteilten Ermächtigung im Gesetz bestimmt werden“.

Der Grad der jeweils zu fordernden Bestimmtheit einer Regelung hängt nach der gefestigten Rechtsprechung des Bundesverfassungsgerichts insbesondere „von der Intensität der Auswirkungen der Regelung für die Betroffenen ab“ (siehe nur jüngst BVerfG, Beschluss des Ersten Senats vom 24. März 2021 – 1 BvR 2656/18, Rn. 260); hierbei gilt:

> „Je schwerwiegender die Auswirkungen sind, desto höhere Anforderungen werden an die Bestimmtheit der Ermächtigung zu stellen sein. Insoweit berührt sich das Bestimmtheitsgebot mit dem Verfassungsgrundsatz des Vorbehalts des Gesetzes, der fordert, dass der Gesetzgeber die entscheidenden Grundlagen des zu regelnden Rechtsbereichs, die den Freiheits- und Gleichheitsbereich des Bürgers wesentlich betreffen, selbst festlegt und dies nicht dem Handeln der Verwaltung überlässt (BVerfGE 56, 1 <13>; vgl. BVerfGE 141, 143 <170 Rn. 59>; 147, 253 <309 f. Rn. 116>; 150, 1 <99 ff. Rn. 199 ff.> m.w.N.). Damit soll gewährleistet werden, dass Entscheidungen von besonderer Tragweite aus einem Verfahren hervorgehen, das der Öffentlichkeit Gelegenheit bietet, ihre Auffassungen auszubilden und zu vertreten, und das die Volksvertretung dazu anhält, Notwendigkeit und Ausmaß von Grundrechtseingriffen in öffentlicher Debatte zu klären. Geboten ist ein Verfahren, das sich durch Transparenz auszeichnet und das die Beteiligung der parlamentarischen Opposition gewährleistet (BVerfGE 150, 1 <96 f. Rn. 192> m.w.N.). Das Grundgesetz kennt allerdings keinen Gewaltenmonismus in Form eines umfassenden Parlamentsvorbehalts. Die in Art. 20 Abs. 2 Satz 2 GG normierte organisatorische und funktionelle Trennung und Gliederung der Gewalten zielt auch darauf ab, dass staatliche Entscheidungen möglichst richtig, das heißt von den Organen getroffen werden, die dafür nach ihrer

> Organisation, Zusammensetzung, Funktion und Verfahrensweise über die besten Voraussetzungen verfügen. Vor diesem Hintergrund kann auch die Komplexität der zu regelnden Sachverhalte den Umfang der Regelungspflicht des Gesetzgebers begrenzen (BVerfGE 150, 1 <99 Rn. 197> m.w.N.). Sollen Regelungen ergehen, die Freiheits- und Gleichheitsrechte der Betroffenen wesentlich betreffen, ist die Einbindung des Verordnungsgebers in die Regelungsaufgabe nicht schlechthin ausgeschlossen (vgl. BVerfGE 147, 310 <311 f. Rn. 120>). Die wesentlichen Fragen sind dann aber, sofern nicht funktionale Grenzen der Gesetzgebung entgegenstehen, entweder unmittelbar durch den Gesetzgeber oder durch entsprechend bestimmte Regelung von Inhalt, Zweck und Ausmaß der Verordnungsermächtigung in einem formellen Gesetz zu klären".
>
> BVerfG, Beschluss des Ersten Senats vom 24. März 2021 – 1 BvR 2656/18, Rn. 260.

Dem genügen die vorliegend gerügten Rechtsvorschriften (siehe oben A.III. und A.IV.) nicht.

a) Fehlende gesetzliche Vorgaben zur Sicherheit des beAs in der BRAO

§ 31a BRAO enthält keine hinreichend konkreten gesetzlichen Vorgaben zu den Sicherheitsanforderungen des beAs. Stattdessen verweist § 31c Nr. 3 BRAO lediglich pauschal darauf, dass die „Einzelheiten" unter anderem zur „Einrichtung", zur „Datenübermittlung" sowie zur „technischen Ausgestaltung" des beAs in einer Rechtsverordnung geregelt werden sollen.

Damit hat sich der Gesetzgeber einer Festlegung auch nur von gebotenen Mindestanforderungen an die Sicherheit des beAs vollständig entzogen. Die Sicherheit des beAs ist indes in erheblichem Maße grundrechtswesentlich, wie bereits ausführlich erläutert (siehe oben B.II.1.-2.). Der Gesetzgeber hätte zumindest grundlegende Mindestbedingungen festlegen müssen, die bei der Einrichtung des beAs durch die BRAK zu berücksichtigen sind.

Dies wäre auch möglich gewesen und wurde vom Gesetzgeber bereits in Bezug auf De-Mail – wenngleich ebenfalls in unzulänglicher Weise, indem eine Ende-zu-Ende-Verschlüsselung nicht verpflichtend vorgesehen wurde – in § 5 Absatz 3 des De-Mail-Gesetzes vom 28. April 2011 (BGBl. I S. 666), das zuletzt durch Artikel 14 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626) geändert worden ist, konkret geregelt:

> „Der Postfach- und Versanddienst hat die Vertraulichkeit, die Integrität und die Authentizität der Nachrichten zu gewährleisten. Hierzu gewährleistet der akkreditierte Diensteanbieter, dass
> 1. die Kommunikation von einem akkreditierten Diensteanbieter zu jedem anderen akkreditierten Diensteanbieter über einen verschlüsselten gegenseitig authentisierten Kanal erfolgt (Transportverschlüsselung) und
> 2. der Inhalt einer De-Mail-Nachricht vom akkreditierten Diensteanbieter des Senders zum akkreditierten Diensteanbieter des Empfängers verschlüsselt übertragen wird.
> Der Einsatz einer durchgängigen Verschlüsselung zwischen Sender und Empfänger (Ende-zu-Ende-Verschlüsselung) bleibt hiervon unberührt".

Der Gesetzgeber hätte mithin ohne Weiteres in Bezug auf das beA regeln können – und in Anbetracht des verfassungsrechtlichen Grundsatzes des Vorbehaltes des Gesetzes sowie des Bestimmtheitsgrundsatzes – konkret regeln müssen, mit welcher Form der Verschlüsselung – wie dargelegt, aus verfassungsrechtlichen Gründen: einer Ende-zu-Ende-Verschlüsselung, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaber befinden – das beA einzurichten ist.

Diese gesetzgeberische Pflicht folgt insbesondere auch aus dem rechtsstaatlich vorausgesetzten Institut einer freien Advokatur (Artikel 20 Absatz 3 GG), die nur gewährleistet ist, wenn die anwaltliche Vertraulichkeit gewährleistet ist. Den Gesetzgeber trifft hier insofern auch eine Schutzpflicht, die freie Ausübung des Anwaltsberufes im Rechtsstaat zu wahren.

B) Fehlende gesetzliche Vorgaben zur Sicherheit des beAs im Prozessrecht

Das Vorstehende trifft gleichermaßen auf die in den verschiedenen Prozessordnungen vorgesehenen Vorschriften zu (siehe oben A.IV.), die lediglich deklarieren, dass es sich bei dem beA um einen „sicheren Übermittlungsweg" handele; pars pro toto sei hier nur der § 130a Absätze 3 und 4 ZPO nochmals wiedergegeben:

> „Das elektronische Dokument muss mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.
> (4) Sichere Übermittlungswege sind
> 1. der Postfach- und Versanddienst eines De-Mail-Kontos, wenn der Ab-sender bei Versand der Nachricht sicher im Sinne des § 4 Absatz 1Satz 2 des De-Mail-Gesetzes angemeldet ist und er sich die sichere Anmeldung gemäß § 5Absatz 5 des De-Mail-Gesetzes bestätigen lässt,
> 2. der Übermittlungsweg zwischen dem besonderen elektronischen Anwaltspostfach nach § 31a der Bundesrechtsanwaltsordnung oder einem entsprechenden, auf gesetzlicher Grundlageerrichteten elektronischen Postfach und der elektronischen Poststelle des Gerichts (…)".

Das beA – ebenso wie De-Mail – wird hier vom Gesetzgeber einfach als „sicherer Übermittlungsweg" deklariert, ohne dass die Voraussetzungen bestimmt werden, nach denen sich beurteilt, ob es sich tatsächlich um einen „sicheren Übermittlungsweg" handelt. Wie dargelegt, schweigt die BRAO hierzu vollständig.

Insofern findet sich die inhaltsleere Zirkelschlüssigkeit der vom Bundesgerichtshof verwendete Formel „sicher im Rechtssinne" hier auf gesetzgeberischer Ebene als „sicher im Sinne des Gesetzes" wieder. In beiden Fällen bleibt unklar, unter welchen Gegebenheiten eine Sicherheit tatsächlich vorliegt. Das Recht verweist hier auf sich selbst, ohne eine Antwort zu liefern.

In Anbetracht dessen, dass § 31a Absatz 6 BRAO sowie die verschiedenen bezeichneten prozessrechtlichen Vorschriften (siehe oben A.IV.) – pars pro toto etwa: § 130d ZPO – eine grundsätzlich ausnahmslose Pflicht zur Nutzung des beAs vorsehen, verstärkt sich der Mangel klarer gesetzlicher Vorgaben zur Sicherheit des beAs noch weiter zu einer erheblichen, wesentlichen Beeinträchtigung des Grundrechts auf freie anwaltliche Berufsausübung.

c) Unbestimmtheit der Vorschriften zur Sicherheit des beAs in der RAVPV

Schließlich genügen auch die in den §§ 19 und 20 RAVPV zu findenden Regelungen zur Sicherheit des beAs (siehe oben A.III.) nicht den Anforderungen des rechtsstaatlichen Bestimmtheitsgebotes.

§ 19 Absatz 1 Satz 1 RAVPV spricht insoweit ebenfalls nur vom beA als „sicherem Übermittlungsweg“ und geht damit nicht über die Unbestimmtheit der Regelungen in den Prozessvorschriften wie etwa § 130a ZPO hinaus.

§ 20 Absatz 1 RAVPV nimmt zwar Bezug auf den OSCI-Protokollstandard sowie den „Stand der Technik“ und sieht ebenfalls vor, dass die BRAK zu gewährleisten habe, dass die beA-Nutzer „miteinander sicher elektronisch kommunizieren können“, lässt aber letztlich ebenfalls offen, unter welchen Gegebenheiten dies der Fall ist.

Dass auch dies noch zu unbestimmt ist, zeigt nicht zuletzt die vom Bundesgerichtshof vorgenommene Auslegung der §§ 19 und 20 RAVPV (BGH a. a. O., Rn- 85-95), die zu dem Ergebnis gelangt, dass sich u. a. auch nicht aus dem OSCI-Protokollstandard eine Pflicht zur Ende-zu-Ende-Verschlüsselung ableiten lasse.

C. Hinweise zum Verfahren

I. Anhängige Anhörungsrüge

Die Bevollmächtigten weisen darauf hin, dass gegen das hier gegenständliche Urteil des Bundesgerichtshofes vom 22. März 2021 (AnwZ <Brfg> 2/20) eine Anhörungsrüge erhoben wurde, über die noch nicht entschieden wurde.

II. Korrespondenz

Weiter bitten die Bevollmächtigten höflich darum, sämtliche weitere Korrespondenz über den Bevollmächtigten Rechtsanwalt Christoph R. Müller zu führen; seine Kontaktdaten lauten:

Rechtsanwalt Christoph R. Müller
Riemannstr. 29b
04107 Leipzig
Telefon: +49 341 68 67 88 07
Fax: +49 341 68 67 88 06

Dr. Delhey
Rechtsanwalt

Müller
Rechtsanwalt