mueller legal ::: RA Christoph R. Müller ::: Arno-Nitzsche-Str. 19 ::: 04277 Leipzig

An den
Bundesgerichtshof in Anwaltssachen
Herrenstraße 45 a

76133 Karlsruhe

**vorab per Fax**
**0721 159-1509**

**Christoph R. Müller**
Rechtsanwalt

Arno-Nitzsche-Str. 19 / Haus A
04277 Leipzig

Tel.: +49 (0) 341 | 68 67 88 07
Fax: +49 (0) 341 | 68 67 88 06

www.mueller-legal.de
kanzlei@mueller-legal.de

Leipzig, 18.03.2020

Ihr Zeichen: AnwZ(Brfg) 2/20

Unser Zeichen: **00381-ml** (bei Korrespondenz bitte angeben)

In dem anwaltsgerichtlichen Rechtsstreit

**R. u.a. gegen BRAK**

bedanke ich mich für die gewährte Fristverlängerung und begründe die Berufung gegen das Urteil des Anwaltsgerichtshofs Berlin vom 14.11.2019 zum Az I AGH 6/18 wie folgt:

Das Urteil des erkennenden Senats des Anwaltsgerichtshofs Berlin (im Folgenden: Senat) ist rechtlich weder in seiner Begründung noch im Ergebnis haltbar. Der Senat hat den Argumenten der Kläger kein Gehör schenkt, vielmehr stützt sich die Entscheidung im Wesentlichen allein auf ein bloßes Negieren des klägerischen Vortrags.

Zudem hat der Senat in seiner Entscheidung zum einen die in Streit stehende Risikosituation in tatsächlicher Hinsicht unzureichend gewürdigt und zum anderen die Frage des Bestehens einer „Sicherheit im Rechtssinne“ unzutreffend beurteilt.

Zur Vermeidung von Wiederholungen wird zunächst auf den bisherigen und umfassenden Vortrag der Kläger im Ausgangsverfahren verwiesen; er wird ausdrücklich vollumfänglich zum Bestandteil des weiteren Klägervorbringens im Rahmen des hiesigen Berufungsverfahrens erklärt.

**I.**

**Unzureichende rechtliche Würdigung der Risikolage durch die Vorinstanz**

Die aus Sicht der Kläger wesentliche, entscheidungserhebliche Tatsache, dass die Konstruktion des beA ohne Ende-zu-Ende-Verschlüsselung ein Ausspähen sämtlicher anwaltlicher Kommunikation mittels eines einzigen Angriffs („*Single Point of Failure*“) ermöglicht, wurde vom Senat in seiner Sachverhaltsdarstellung vollständig weggelassen. Dadurch entzog er sich von vorneherein der gebotenen argumentativen Auseinandersetzung hiermit.

**1.**

**Bewusste Sachverhaltsverkürzung:**
**Unterschlagung des wesentlichen Sicherheitsrisikos des beA**

Der Senat hat den Sachverhalt verkürzt dargestellt. Er ließ den von den Klägern mehrfach und ausdrücklich herausgestellten Umstand unerwähnt, wonach es gemäß des unstreitigen, von der Beklagten selbst in Auftrag gegebenen Gutachtens der secunet Security Networks AG vom 18.06.2018 (im Folgenden: Secunet-Gutachten; Anlage K26) möglich ist, mit einem einzigen Angriff sämtliche anwaltliche und gerichtliche Korrespondenz heimlich auszuspähen.

Dies, obgleich nicht nur das Secunet-Gutachten in den Prozess eingebracht wurde, sondern die Kläger die einschlägige Passage sogar wie folgt wörtlich zitierten. Wegen der elementaren Bedeutung wird sie nachstehend nochmals im Wortlaut wiedergegeben (Kläger-Schriftsatz vom 12.11.2018, S. 11 f.):

> „*Elementar geht es um die Sicherheit der verschlüsselten Arbeitsschlüssel (Master-Key-Sets) für die verschiedenen Zwecke des HSM 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.***
>
> […]
>
> *Der Missbrauch dieser Schlüssel kann auf zwei Arten geschehen:* ***die Key Custodians des Auftraggebers und ein Helfer beim Betreiber des beA führen den ver-***

***schlüsselten Nachrichtenbestand und die Schlüssel zusammen und sind dann in der Lage, die Nachrichten zu entschlüsseln***. *Oder es wurde unberechtigt beim Betreiber des beA nach der Erzeugung der Schlüssel vor der Übergabe an den Auftraggeber an einer Stelle eine Kopie erstellt.* ***Dann kann das Personal des Betreibers alleine die Nachrichten entschlüsseln***.

*Vor diesem Hintergrund besteht zudem die Möglichkeit, dass der* ***Auftraggeber im Rahmen von Beschlagnahmen von Postfächern gezwungen werden könnte, Nachrichten offenzulegen***. *Damit sind rechtliche Fragen verbunden, die im Rahmen dieses Gutachtens nicht beantwortet werden können. Daher wurde diese Möglichkeit auch nicht in die Bewertung der Ausnutzbarkeit einbezogen.*

*Die Verwahrung der Schlüssel außerhalb der HSM dient der Inbetriebnahme neuer HSM. Diese Praxis ist nicht unüblich und findet z.B. im Bankwesen oft Anwendung. Damit sie 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.*

[…]

***Der Angriff erlaubt die umfassende Aufdeckung des Inhalts aller in beA-Postfächern gespeicherten Nachrichten. Die Bedrohung wird daher als hoch eingeschätzt***“.

Secunet-Gutachten, S. 85 f., Hervorhebungen durch den Unterzeichner

Auffälligerweise wurde dies von der Beklagten bis zuletzt und selbst in ihrer Stellungnahme zum Antrag auf Tatbestandsberichtigung vom 17.12.2019 nicht bestritten.

Demgegenüber führte der Senat in seinem Beschluss vom 03.02.2020 zur Ablehnung des auf entsprechende Ergänzung gerichteten Tatbestandsberichtigungsantrages der Kläger aus:

„*Auch der weitere Passus ist nicht in den Urteilstatbestand aufzunehmen. Mangels Entscheidungserheblichkeit hat der Senat auch hier keinen Anlass,* ***einen überholten Sachstand*** **[sic!]** *zu rekapitulieren. Die Darlegung einer sachverständigen (Dritt-)Bewertung eines* ***früheren Zustands*** [sic!] *widerspräche schon dem*

> *Wesen des Urteilstatbestands, die tatsächlichen und verfahrensbezogenen Grundlagen der Entscheidung zur Erhöhung ihres Verständnisses darzustellen*“.
>
> AGH, Beschluss vom 20. Februar 2020 – I AGH 6/18, S. 5., Hervorhebungen durch den Unterzeichner

Folglich ging der Senat irrig davon aus, dass die **maßgebliche Schwäche des beA-Systems** – nämlich dass mit einem einzigen Angriff sämtliche Nachrichten heimlich mitgelesen werden können – **zum Entscheidungszeitpunkt nicht mehr existiert habe**.

Auf welche Tatsachen der Senat dies stützen will, ist nicht nachvollziehbar. Als gerichtsbekannt können sie nicht unterstellt werden.

So wurde von der Beklagten bis zuletzt nicht bestritten, dass das Angriffsrisiko nicht mehr bestehe. Ein derartiger Vortrag der Beklagten findet denn auch im Urteil – insoweit zutreffend – bei der Wiedergabe des streitigen Beklagtenvorbringens keine Erwähnung.

**2.**

**Weiterbestehen des Risikos eines heimlichen Ausspähens sämtlicher beA-Kommunikation („Single Poinf of Failure“)**

Vielmehr nahm die Beklagte nach eigenem öffentlichen Bekunden laut ihrer Presseerklärung Nr. 23 vom 20.08.2018 das beA wieder in Betrieb, ohne den Mangel behoben zu haben, weil dieser im Secunet-Gutachten – höchst fragwürdig – als lediglich „*betriebsbehindernd*“ eingeordnet wurde und die in diese Kategorie fallenden „*Schwachstellen*“ – ebenfalls höchst zweifelhaft – erst „*im laufenden Betrieb*“ behoben werden sollten.

> BRAK, Presseerklärung Nr. 23 vom 20. August 2018; abrufbar unter https://brak.de/fuer-journalisten/pressemitteilungen-archiv/2018/presseerklaerung-23-2018/

Ob dies inzwischen geschehen ist, wurde von der Beklagten bislang nach Kenntnis der Kläger weder öffentlich noch im Ausgangsverfahren vorgetragen und unter Beweis gestellt. So findet sich bis heute auch keine Presseerklärung der Beklagten dazu, ob bzw. inwieweit inzwischen während des laufenden Betriebes weitere Schwachstellen behoben wurden.

Dessen ungeachtet haben die Kläger schon im Ausgangsverfahren stets deutlich gemacht, dass der von Secunet vorgeschlagene Lösungsansatz – sollte er denn verwirklicht

werden –, jedenfalls nicht ausreicht, um das System hinreichend sicher zu gestalten. Denn der Lösungsvorschlag sieht keine Ende-zu-Ende-Verschlüsselung vor, sondern – im Gegenteil –, dass die Schlüssel nicht wie bei einer Ende-zu-Ende-Verschlüsselung von den Kommunikationspartnern, sondern in einem sog. „*Hardware Security Module*“ (HSM) erzeugt werden (Secunet-Gutachten, S. 87).

## II.

## beA nicht „*im Rechtssinne sicher*“

Das – durch die unzureichende Sachverhaltserfassung vorgezeichnete – Ergebnis der rechtlichen Würdigung des Senats, das beA sei „*im Rechtssinne sicher*“ (AGH Berlin, Urt. v. 14.11.2019 – I AGH 6/18, S. 10) ist unzutreffend.

### 1.

### Außerachtlassung des maßgeblichen Risikos eines zentralen Ausspähens der gesamten anwaltlichen Kommunikation über das beA

Wie dargelegt, hat der Senat im Rahmen seiner rechtlichen Beurteilung der Sicherheit des beA den wesentlichen Aspekt, dass mit einem einzigen erfolgreichen Angriff die gesamte beA-Kommunikation ausgespäht werden kann, vollständig außer Acht gelassen.

Stattdessen beschränkte der AGH seine rechtliche Prüfung auf die unstreitig bereits behobenen Schwachstellen, zu denen jedoch nicht der wesentliche, von den Klägern zentral angegriffene Mangel zählt. So befasste sich der AGH nur mit den im Sinne des Secunet-Gutachtens „*betriebsverhindernden*“, nicht jedoch mit den „*betriebsbehindernden*“ **Schwachstellen** (AGH Berlin, Urteil vom 14.11.2019, S. 12). Das oben zitierte Sicherheitsrisiko des zentralen Ausspähens der beA-Kommunikation wurde indes im Secunet-Gutachten als betriebsbehindernd qualifiziert (Secunet-Gutachten, S. 87) und sein weiteres Bestehen von der Beklagten nicht bestritten.

Schon aus diesem Grunde ist die rechtliche Würdigung des AGH wegen der Außerachtlassung des eigentlich entscheidungserheblichen Sicherheitsrisikos vollkommen unzureichend und kann das Ergebnis nicht stützen.

**2.**

**Hinwegsetzen über den Willen des Gesetzgebers, des Verordnungsgebers und des Bundesverfassungsgerichts**

Eklatant rechtsfehlerhaft ist das Urteil des AGH zudem, soweit sich der Senat über den ausdrücklichen Willen des Gesetzgebers, des Verordnungsgebers und des Bundesverfassungsgerichts hinwegsetzt.

So führt der Senat zum dokumentierten Willen des Verordnungsgebers der RAVPV lapidar aus (AGH Berlin, Urteil vom 14.11.2019, S. 7 f.):

> „*Nach Auffassung des Senats ist die Wortwahl* [Anm.: „Ende-zu-Ende-Verschlüsselung] *vielmehr* ***Ausfluss dessen, dass die Beklagte – ersichtlich zur Erhöhung der Akzeptanz, und im Ergebnis irreleitend* [sic!] *– über Jahre kommuniziert hat****, die von ihr gewählte Architektur enthalte eine Ende-zu-Ende-Verschlüsselung. Dass dieser Terminus Eingang in die Begründung zur RAVPV gefunden hat, dürfte mithin nicht dem Umstand geschuldet sein, dass im Bundesministerium unterschiedliche Sicherheitsarchitekturen durchdacht und ausschließlich kryptografische Lösungen für sicher befunden wurden. Die Erwähnung der Ende-zu-Ende-Verschlüsselung steht nach Auffassung des Senats vielmehr damit im Zusammenhang, dass die mit der Ausarbeitung befassten Beamten* ***die Terminologie der Beklagten übernommen und angenommen haben, das von dieser geplante besondere elektronische Anwaltspostfach verwende dieses Verschlüsselungs- und Übermittlungskonzept***“.
>
> AGH Berlin, Urteil vom 14.11.2019, S. 7 f., Hervorhebungen durch den Unterzeichner

Damit sagt der Senat nichts anderes, als dass die mit dem beA über Jahre hinweg befassten Ministerialbeamten lediglich den irreführenden Äußerungen der Beklagten erlegen seien, dass das beA eine Ende-zu-Ende-Verschlüsselung aufweise und eine solche eigentlich selbst gar nicht für erforderlich erachten würden.

Im Ergebnis belohnt der Senat damit die Beklagte für die Verbreitung der unwahren Behauptung, dass das beA über eine Ende-zu-Ende-Verschlüsselung verfüge.

Dabei muss sich doch vielmehr die Gegenfrage aufdrängen, warum die Beklagte denn über eben diesen Umstand getäuscht hat? Die Antwort liegt auf der Hand: um das nicht sichere beA sicher erscheinen zu lassen! – Mit ihrer Täuschung über die tatsächlich bestehende Sicherheit des beA hat die Beklagte letztlich selbst zu erkennen gegeben, dass

auch sie ganz offensichtlich nur ein beA mit Ende-zu-Ende-Verschlüsselung für hinreichend sicher gehalten hat – sonst wäre die Irreführung nicht nötig gewesen und ist ihr Verhalten anders auch nicht nachvollziehbar. Der Beklagten muss bewusst gewesen sein, dass sie der Anwaltschaft das beA nur „*verkaufen*“ kann, wenn sie dieses als „*sicher*“ anpreisen kann und dass hierfür die Ausstattung mit einer Ende-zu-Ende-Verschlüsselung „*conditio sine qua non*“ ist.

Im Übrigen sollte gerichtsbekannt sein, dass sich das Justizministzterium – wie in Gesetzgebungsverfahren üblich – über Jahre hinweg in einem engen, stetigen Austausch mit Vertretern der Beklagten befunden hat. Ein jahrelanges „*Irren*“ der zuständigen Ministerialbeamten über den wohl wichtigsten sicherheitstechnischen Aspekt des beA – seine Ende-zu-Ende-Verschlüsselung – erscheint dabei fern jeder Lebenswirklichkeit.

Weiter kann auch die Ansicht des Senats nicht überzeugen, dass die einschlägigen Ausführungen in der Begründung zur RAVPV bezüglich der Notwendigkeit einer Ende-zu-Ende-Verschlüsselung den BRAO-Vorschriften zeitlich nachfolgten und somit allein deswegen im Rahmen der Auslegung schon per se nicht verwertbar seien. Denn selbstverständlich ist auch ein später geäußerter gesetzgeberischer Wille zu berücksichtigen. Insbesondere liegen auch keine Anhaltspunkte dafür vor, dass der Gesetzgeber seinen Willen geändert hätte.

Vielmehr führte auch bereits der **Bundesrat** im Verlaufe des Gesetzgebungsverfahrens in seiner Stellungnahme zum Entwurf des § 174 Absatz 3 ZPO aus:

> *„Die vorgeschlagene Streichung der Bezugnahme auf ‚sichere Übermittlungswege‘ im Sinne des § 130a Absatz 4 ZPO-E führt auch nicht etwa zur Zulassung ‚unsicherer‘ Übertragungswege, da die* ***Anforderung, die Übermittlung „gegen unbefugte Kenntnisnahme Dritter zu schützen“****, bestehen bliebe und diese beim Einsatz der EGVP-Infrastruktur durch die automatisierte* ***(Ende-zu-Ende-)Verschlüsselung*** *der Daten über das sogenannte OSCI-Transportprotokoll gewährleistet wird“.*
>
> *Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 06. März 2013, BT-Drs. 17/12634, S. 46 f.; Hervorhebung durch den Unterzeichner*

Und schließlich ist auch das Bundesverfassungsgericht davon ausgegangen, dass das beA über eine Ende-zu-Ende-Verschlüsselung verfügt, hat dies in seiner Sachverhaltsdarstellung ausdrücklich betont und sogar gerügt, dass sich der Beschwerdeführer nicht hinrei-

chend mit diesem – vom Bundesverfassungsgericht ganz offensichtlich für besonders wesentlich erachteten – Sicherheitsaspekt auseinandergesetzt habe (BVerfG, Beschluss vom 20. Dezember 2017 – 1 BvR 2233/17, Rn. 5:

> *„Das beA verwendet zur sicheren Übermittlung eine so genannte Ende-zu-Ende-Verschlüsselung (vgl. § 20 Abs. 1 RAVPV).* […]
>
> „[…] *jedenfalls aber fehlt es an einer Auseinandersetzung mit den konkret getroffenen Sicherheitsvorkehrungen wie etwa der Ende-zu-Ende-Verschlüsselung“.*

Der Senat hat sich nach alledem folglich bei seiner Herleitung, was in Bezug auf das beA als „*sicher im Rechtssinne*“ (des Senats) gelten solle sowohl über den Willen des Gesetzgebers und des Verordnungsgebers als auch des Bundesverfassungsgerichts hinweggesetzt. Damit hat er die Grenzen richterlicher Normauslegung bei weitem deutlich überschritten.

**3.**

**„*Im Rechtssinne sicher*“ nicht gleichbedeutend mit „*irgendwie sicher*“: Verhältnismäßigkeitsprinzip verlangt Wahl der sichersten Lösung als mildestes Mittel**

Die Urteilsbegründung des Senats erweckt den Eindruck, „*im Rechtssinne sicher*“ bedeute lediglich, dass das beA nur „*irgendwie sicher*“ sein müsste:

> „***Im Rechtesinne sicher*** *ist* ***nicht zwingend ausschließlich das „sicherste“ Verfahren****. Unter wissenschaftlich gebotener Zugrundelegung eines relativen Sicherheitsbegriffs kann es vielmehr einen „****Sicherheitskorridor****“ geben, so dass ggf. unterschiedliche Sicherheitsarchitekturen als sicher im Rechtssinne angesehen werden können. Dabei können technische Lösungen auch dann als „sicher“ gelten, wenn sie zwar anderen Architekturen* ***unterlegen, aber, noch in den gewissermaßen unteren Bereich dieses gedachten Sicherheitskorridors einzustufen*** *wären.*
>
> AGH Berlin, Urteil vom 14.11.2019, S. 9, Hervorhebungen durch den Unterzeichner

Zwar kann insoweit zugestimmt werden, dass es regelmäßig mehrere technische Lösungen geben mag, die eine hinreichende Sicherheit gewährleisten. Nicht nachvollziehbar ist aber, warum es gerechtfertigt sein sollte, eine **minderwertige Lösung** zu wählen, die weniger sicher ist als eine andere.

Dies widerspricht diametral dem grundrechtlichen Verhältnismäßigkeitsmaßstab, der einen Grundrechtseingriff nur insoweit erlaubt, als die staatliche Maßnahme das mildeste geeignete Mittel darstellt (vgl. BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07, Rn. 224 f.).

Kommen verschiedene geeignete Sicherheitsmaßnahmen in Betracht, muss stets diejenige gewählt werden, die den mildesten Eingriff in Grundrechte verspricht, mithin also vice versa den weitgehendsten Grundrechtsschutz gewährleistet, sodass es sich folglich im Ergebnis stets um die sicherste technische Lösung handeln muss. Diese sicherste technische Lösung ist die von den Klägern begehrte Ende-zu-Ende-Verschlüsselung. Sie ist der von der Beklagten gewählten HSM-Lösung unstreitig überlegen.

**4.**

**Verfassungsrechtliche Pflicht zur Gewährleistung eines besonders hohen Maßes an Sicherheit**

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 Berücksichtigung der Besonderheiten** […] ein **besonders hohes Maß an Sicherheit gewährleistet***“ (BVerfG, Urteil des Ersten Senats vom 02.03.2010 – 1 BvR 256/08 -, Rn. 224; Hervorhebungen durch den Unterzeichner).

In Anbetracht dessen, dass über das beA besonders schutzwürdige, der anwaltlichen Verschwiegenheit unterliegende, teils hochsensible Mandantengeheimnisse auszutauschen sind, muss in Bezug auf das beA in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts ein besonders hohes Maß an Sicherheit gewährleistet werden. Und dieses besteht nur bei Einrichtung einer Ende-zu-Ende-Verschlüsselung.

Eine **einfache** und eine **beglaubigte** Abschrift anbei.

Christoph R. Müller
Rechtsanwalt