Hochschule des Bundes
für öffentliche Verwaltung

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)434 D

POSTANSCHRIFT HS BUND, POSTFACH 40527, 10063 BERLIN

Deutscher Bundestag
- Ausschuss für Inneres u. Heimat -

via E-Mail

Prof. Dr. Jan-Hendrik Dietrich
HAUSANSCHRIFT Habersaathstr. 51, 10115 Berlin
POSTANSCHRIFT Postfach 40527, 10063 Berlin
TEL 030 – 22 00 89 – 86341
EMAIL jan-hendrik.dietrich@fhbund-muc.de

DATUM Berlin, 26.01.2020

BETREFF **Schriftliche Stellungnahme zur Sachverständigenanhörung vor dem Ausschuss für Inneres und Heimat des Deutschen Bundestages am 27.01.2020**

über

den Antrag der Abgeordneten Jimmy Schulz, Stephan Thomae, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP

Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken

BT-Drs. 19/5764

Zu den im o.g. Antrag aufgeworfenen Rechtsfragen nehme ich vor der mündlichen Anhörung aus verfassungs- und verwaltungsrechtlicher Sicht folgendermaßen Stellung:

I. „Recht auf Verschlüsselung“?

Ein „Recht auf Verschlüsselung“ kennt die deutsche Rechtsordnung nicht. Ein entsprechendes Grundrecht ist weder ausdrücklich im Grundgesetz geregelt noch der Rechtsprechung des BVerfG zu entnehmen. Einfachgesetzlich ist es bisher nicht hin-

terlegt. Dafür besteht auch kein Bedarf. Denn „Verschlüsselung“ ist nichts anderes als ein **schutzbereichsrelevantes Verhalten im Rahmen der Gewährleistung bekannter Grundrechte**.[1] Soweit gesetzliche Pflichten bestehen, Inhalte von elektronischer Kommunikation „verschlüsselt“ zu übertragen (Vgl. etwa § 5 Abs. 3 S. 2 De-Mail-Gesetz), bei Datenübermittlungen Vorkehrungen zum Schutz „gegen den unbefugten Zugriff Dritter“ (Vgl. z.B. § 21a S. 1 BZRG) zu treffen oder elektronische Überwachungsinstrumente „nach dem Stand der Technik gegen unbefugte Nutzung zu schützen (Vgl. § 49 Abs. 2 S. 2 BKAG), wird lediglich das grundrechtliche Schutzniveau konkretisiert.

1. „Verschlüsselung“ in der abwehrrechtlichen Dimension der Grundrechte

Grundrechte fungieren zu allererst als Abwehrrechte von Bürgerinnen und Bürgern gegenüber staatlichen Eingriffen.[2] „Verschlüsselung“ kann in diesem Zusammenhang ein Verhalten darstellen, das vom Schutzbereich eines Grundrechts erfasst ist. So kann Verschlüsselung etwa vom **Schutz des Fernmeldegeheimnisses i.S.v. Art. 10 Abs. 1 GG** umfasst sein. Das Fernmeldegeheimnis schützt die Vertraulichkeit der räumlich distanzierten Kommunikation. Die Verwendung von Verschlüsselungstechniken soll diesen Schutz stärken. Ganz vergleichbar ist die Verwendung eines Briefumschlags zur Wahrung des Briefgeheimnisses.[3] Insofern stellt „Verschlüsselung“ ein geschütztes Verhalten im Schutzbereich von Art. 10 Abs. 1 GG dar. Schutzbereichsverstärkend kann sich hierbei auswirken, dass es auch Gegenstand der Meinungsäußerungsfreiheit i.S.v. Art. 5 Abs. 1 S. 1 Hs. 1 GG sein kann, eine Meinung „codiert“ zu äußern.[4] Der Grundrechtsträger ist bei der Wahl der Form der Meinungsäußerung frei.

---

[1] Siehe ausführlich dazu *Gerhards*, (Grund-) Recht auf Verschlüsselung?, 2010, S. 123 ff.

[2] Vgl. BVerfGE 7, 198 (204); 50, 290 (337); 68, 193 (205)

[3] Vgl. *Voßhoff/Büttgen*, ZRP 2014, 232 (232).

[4] Vgl. *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 202 ff.; in diese Richtung wohl auch *Gusy*, nach dessen Auffassung die Nutzung von Verschlüsselungstechniken allgemein dem Schutzbereich von Art. 5 Abs. 1 S. 1 GG unterfallen soll. Siehe *Gusy*, in: v. Mangoldt/Klein/Starck, GG, Bd. 1, 7. Aufl. 2018, Art. 10 Rn. 66.

Die Nutzung von Verschlüsselungstechniken kann zudem dem Schutz des **allgemeinen Persönlichkeitsrechts i.S.v. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG** unterfallen. Das vom BVerfG aus dem allgemeinen Persönlichkeitsrecht abgeleitete **Recht auf informationelle Selbstbestimmung** vermittelt dem Grundrechtsträger das Recht, über die Verwendung seiner personenbezogenen Daten grundsätzlich selbst zu entscheiden. Dies umfasst zweifellos das Recht, solche Daten zu verschlüsseln. Darüber hinaus hat das BVerfG in seiner Entscheidung zur „Online-Durchsuchung" dem allgemeinen Persönlichkeitsrecht den Teilgehalt eines **Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme** entnommen.[5] Geschützt ist dabei das Interesse des Nutzers, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben.[6] Die Vertraulichkeits- und Integritätserwartung lässt sich insbesondere über Verschlüsselungsmechanismen erreichen. Sie bilden die entscheidende technische Hürde gegen Ausspähung, Überwachung oder Manipulation. Mit Blick auf die zunehmende Digitalisierung des Alltags und faktisch bestehenden Grenzen eines staatlich vermittelten Schutzes vor Bedrohungen im „World Wide Web" muss der Einzelne berechtigt sein, die Vertraulichkeit und Integrität seiner informationstechnischen Systeme selbst in die Hand zu nehmen.[7] Der Einsatz von Verschlüsselung unterfällt demgemäß dem Schutzbereich von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

Schließlich kann die Nutzung von Verschlüsselung von der **grundrechtlichen Gewährleistung wirtschaftlicher Betätigung** nach Art. 12 Abs. 1 GG und Art. 14 Abs. 1 S. 1 GG umfasst sein. Die Berufsfreiheit gem. Art. 12 GG schützt u.a. die Berufs*ausübungs*freiheit. Vom Schutzbereich erfasst alles, was eine berufliche Tätigkeit ausmacht (insb. Form, Mittel, Umfang und Inhalt der Betätigung).[8] Bei bestimmten Berufsgruppen ist ein besonderes Vertrauensverhältnis besonders charakteristisch für die berufliche Tätigkeit. Angesprochen sind sog. Berufsgeheimnisträger, wie etwa

---

[5] BVerfGE 120, 274 (313 ff.).

[6] BVerfGE 120, 274 (314).

[7] In diesem Sinne *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 183.

[8] Siehe *Manssen*, in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Fn. 4), Art. 12 Rn. 67; *Mann*, in: Sachs (Hrsg.), GG, 8. Aufl. 2018, Art. 12 Rn. 79.

Ärzte, Geistliche oder Strafverteidiger. Das diese Berufe kennzeichnende Vertrauensverhältnis wird gesetzlich besonders geschützt (Vgl. z.B. § 53 Abs. 1 StPO, § 62 BKAG, § 203 Abs. 1 StGB).[9] Die Wahrung des Berufsgeheimnisses zählt damit untrennbar zur beruflichen Betätigung. Jedes Verhalten, das der Gewährleistung des typischen Vertrauensverhältnisses dient, unterfällt insofern dem Schutzbereich von Art. 12 GG.[10] So liegt es im Fall der Verwendung von Verschlüsselungstechniken. Zudem kann der Schutzbereich der Eigentumsfreiheit i.S.v. Art. 14 Abs. 1 GG eröffnet sein. Dies ist jedenfalls anzunehmen, soweit es um den Schutz betriebsbezogener Daten geht, die bereits zu einem Vermögenswert geworden sind.[11] Namentlich Betriebs- und Geschäftsgeheimnisse können ohne Verschlüsselungsvorkehrungen nicht vor unbefugter fremder Kenntnisnahme bewahrt werden.[12]

Der Einsatz von Verschlüsselungstechniken wird nach alledem von verschiedenen Grundrechten geschützt. Der grundrechtliche Schutz wird allerdings nicht schrankenlos gewährleistet. Der Staat kann „Verschlüsselung“ in Konkretisierung jeweils einschlägiger grundrechtlicher Gesetzesvorbehalte regulieren. Als solche **Grundrechtseingriffe** kommen verschiedene Maßnahmen in Betracht. Der denkbar schwerste Eingriff wäre ein **grundsätzliches Verbot von Verschlüsselungstechniken**, wie es zur Zeit in den USA diskutiert[13] und in manchen Staaten bereits praktiziert wird[14]. Unterhalb der Verbotsschwelle sind **mildere gesetzliche Beschränkungen** denkbar. Hierzu würde etwa zählen, Diensteanbieter zur Wahrung von staatlichen Sicherheitsinteressen zum **Einbau von sog. „Backdoors“** oder zur **Hinterlegung von Schlüsseln** zu verpflichten. Schließlich könnte der Gesetzgeber für Diensteanbieter, bei denen Verschlüsselungsoptionen gewählt werden können, eine

---

[9] Zur Schutzbedürftigkeit von Berufsgeheimnisträgern siehe jüngst BVerfGE 141, 220 (Rn. 255) sowie *Löffelmann*, GSZ 2019, 190 (193).

[10] Siehe näher *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 253 ff.

[11] Vgl. *Jarass/Pieroth*, GG, 15. Aufl. 2018, Art. 14 Rn. 17.

[12] Vgl. *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 233 ff.

[13] Näher *Geller*, POLITICO v. 27.06.2019, https://www.politico.com/story/2019/06/27/trump-officials-weigh-encryption-crackdown-1385306 (Stand: 20.01.2020).

[14] So z.B. in Saudi-Arabien. In anderen Staaten steht der Einsatz von Verschlüsselungstechniken unter Genehmigungsvorbehalt (z.B. im Iran, in China oder Russland). Nachweise bei *Schulze*, APuZ 46-47/2017, 23 (25 f.); *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 117 ff.

gesetzliche Pflicht zur Herausgabe von Schlüsseln oder Passwörtern an Sicherheitsbehörden vorsehen, wenn im Einzelfall eine bestimmte Gefahren- oder Verdachtslage besteht und ein Gericht die Herausgabe anordnet. Auf die Zulässigkeit solcher Beschränkungsmaßnahmen wird unten eingegangen (siehe unten III.).

2. „Verschlüsselung" und grundrechtliche Schutzpflichten

Die Grundrechte vermitteln nicht nur abwehrrechtliche Schutzansprüche des Einzelnen. Sie verkörpern in ihrer Gesamtheit eine **objektive Werteordnung**.[15] In diesem Sinne wirken sie sich auf die Gestaltung und Anwendung des einfachen Rechts durch alle drei Gewalten aus, indem sie objektiv-rechtlich **staatliche Schutzpflichten** begründen[16], d.h. sie verlangen vom Staat ein positives Tun, die grundrechtlich verbrieften Rechtsgüter des Einzelnen vor Eingriffen Dritter zu schützen.[17] In Bezug auf den Einsatz von Verschlüsselungstechniken ist fraglich, ob den Staat eine grundrechtliche Schutzpflicht trifft, Diensteanbieter gesetzlich hierzu zu verpflichten (dazu sogleich unter II.).

II. Gesetzliche Verpflichtung zum Einsatz von „Ende-zu-Ende"-Verschlüsselung

Im o.g. Antrag wird die Bunderegierung aufgefordert,

> „Telekommunikations- und Telemedienanbieter zu verpflichten, ihre Kommunikationsdienste nach einer Übergangsfrist für zukünftige technische Systeme als Standard abhörsicher (Ende-zu-Ende verschlüsselt) anzubieten".

Es stellt sich die Frage, ob der deutsche Gesetzgeber hierzu im Wege grundrechtlicher Schutzpflichten verpflichtet ist. Eine Schutzpflicht, die gesetzgeberische Handlungsaufträge vermittelt, ist grundsätzlich in Bezug auf alle Grundrechte denkbar.[18]

---

[15] Siehe nur BVerfGE 7, 198 (205).

[16] Vgl. BVerfGE 39, 1 (41 f.); 53, 30 (57); 56, 54 (73); 88, 203 (232, 251); 115, 118 (152).

[17] Siehe *Groß*, JZ 1999, 236 (331).

[18] Siehe *Ronellenfitsch*, DuD 2018, 110 (111); *Roßnagel*, ZRP 1997, 26 (28), *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 321; *Schliesky/Hoffmann/Luch/Schulz/Borchers*, Schutzpflichten und Drittwirkung im Internet, 2014, S. 48.

Eine gesetzliche Verpflichtung von Diensteanbietern zum Einsatz von Ende-zu-Ende-Verschlüsselungen könnte sich aus der Schutzpflichtendimension des Fernmeldegeheimnisses i.S.v. Art. 10 Abs. 1 GG ergeben.[19] Diesbezüglich hat das BVerfG ausdrücklich festgestellt, dass Art. 10 Abs. 1 GG (auch) einen Auftrag an den Staat begründet, **„Schutz insoweit vorzusehen, als private Dritte sich Zugriff auf die Kommunikation verschaffen“**.[20]

Hieraus folgt zunächst, dass eine akute Gefährdungslage hinsichtlich der Vertraulichkeit der räumlich distanzierten Kommunikation bestehen muss.[21] Die drohende – oder sogar schon eingetretene – Rechtsgutverletzung müsste dabei von dritter Seite herrühren und auf den Mangel einer Verschlüsselung zurückzuführen sein. Dem soll am Beispiel der E-Mail-kommunikation nachgegangen werden: es spricht einiges dafür, dass von den Milliarden E-Mails, die jährlich in Deutschland verschickt werden, immer noch ein gewisser Anteil nicht verschlüsselt wird. Im Jahr 2015 wurde in nur 16% aller Fälle eine Verschlüsselungssoftware verwendet.[22] Eine Gefährdungslage hinsichtlich des Rechtsguts aus Art. 10 Abs. 1 GG ist demnach nicht auszuschließen, denn ohne Verschlüsselungstechnik ist die E-Mail-Kommunikation gegen Hacking-Angriffe oder andere Formen des unbefugten Zugriffs nur unzureichend geschützt. Insoweit ist eine aus Art. 10 Abs. 1 GG resultierende Schutzpflicht anzunehmen.

Es stellt sich allerdings die Frage, ob die Schutzpflicht so weit reicht, dem Gesetzgeber die Einführung einer verpflichtenden Ende-zu-Ende-Verschlüsselung aufzuerlegen. Denn dem Staat kommt bei der Erfüllung der Schutzpflichten ein sehr **weiter Einschätzungs-, Wertungs- und Gestaltungsspielraum** zu.[23] Dieser Spielraum wird lediglich durch das sog. **Untermaßverbot** beschränkt.[24] Eine Handlungspflicht

---

[19] Daneben sind auch Schutzpflichten aus dem allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG denkbar, die in dieser Betrachtung unberücksichtigt bleiben.

[20] BVerfG NJW 2002, 3619 (3620); NJW 2007, 3055 (3055).

[21] Siehe zur Schutzpflichtendogmatik *Möstl*, Die staatliche Garantie für öffentliche Sicherheit und Ordnung, 2002, S. 93 ff.; *Schliesky/Hoffmann/Luch/Schulz/Borchers*, Schutzpflichten (Fn. 18), S. 47 ff.

[22] *Schulze*, APuZ 46-47/2017, 23 (23); *Voßhoff/Büttgen*, ZRP 2014, 232 (232).

[23] BVerfGE 77, 170 (214 f.); 88, 203 (262).

[24] In der Rechtsprechung des BVerfG ist dies bisher kaum konturiert worden. Siehe BVerfGE 88, 203 (254). Näher dazu *Möstl*, Garantie für öffentliche Sicherheit und Ordnung, S. 103 ff.

des Staates erwächst allein dann, wenn das Untermaßverbot verletzt ist.[25] Davon kann hier keine Rede sein. Zur Gewährleistung des Schutzes der Vertraulichkeit der Distanzkommunikation hat der Gesetzgeber mittlerweile zahlreiche Regelungen getroffen. Im Mittelpunkt steht die einfachgesetzliche Verpflichtung der Diensteanbieter auf das Fernmeldegeheimnis durch § 88 TKG sowie daraus abzuleitende technische Konsequenzen i.S.v. § 109 Abs. 1 TKG. Eine Verletzung des Fernmeldegeheimnisses ist nach § 206 StGB strafbewehrt. Hinzu kommen weitere strafrechtliche Vorschriften, die mittelbar den Schutz der Vertraulichkeit der Kommunikation bezwecken (z.B. §§ 202a, 202b StGB). Im Mai 2011 ist zudem das De-Mail-Gesetz[26] in Kraft getreten, das De-Mail-Diensteanbieter auf die Nutzung von Signatur- und Verschlüsselungstechniken verpflichtet.[27] Schutzverstärkend wirken darüber hinaus Regelungen der sog. eIDAS-Verordnung[28] sowie der DS-GVO[29]. Art. 32 DS-GVO verpflichtet etwa Unternehmen in Verbindung mit Art. 33, 34 DS-GVO zur Verschlüsselung von E-Mails, die personenbezogene Daten enthalten, da bei Verstößen gegen Sicherheitsverpflichtungen bei der Datenverarbeitung Geldbußen in Millionenhöhe drohen.[30] Zu den gesetzgeberischen Anstrengungen treten zahlreiche administrative Initiativen wie die Empfehlungen und Services des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Die Kombination der geschilderten Maßnahmen kann unmöglich eine Wirkung abgesprochen werden. Vor allem werden Bürgerinnen und Bürger in die Lage versetzt, **wirkungsvollen Selbstschutz** dort zu betreiben, wo – infolge der Internationalität des Internets – ohnehin nur eingeschränkt staatliche Zugriffsmöglichkeiten beste-

---

[25] *Schliesky/Hoffmann/Luch/Schulz/Borchers*, Schutzpflichten (Fn. 18), S. 51.

[26] De-Mail-Gesetz vom 28. April 2011 (BGBl. I S. 666), zuletzt geändert durch Artikel 14 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626).

[27] Siehe dazu *Roßnagel*, NJW 2011, 1473 (1473 ff.)

[28] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. L 257 vom 28.8.2014, S. 73-114.

[29] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119 vom 4.5.2016, S. 1-88.

[30] Vgl. *Hladjk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 32 Rn. 14.

hen[31]. Eine **Verengung der Erfüllung der staatlichen Schutzpflicht** auf lediglich ein einziges Mittel, ist demnach **nicht vertretbar**.[32] Eine gesetzliche Verpflichtung von Diensteanbietern zum Einsatz von Ende-zu-Ende-Verschlüsselungen lässt sich insofern nicht aus der objektiv-rechtlichen Dimension von Art. 10 Abs. 1 GG ableiten.[33]

III. Zulässigkeit gesetzlicher Verschlüsselungsverbote oder -beschränkungen

Mit dem gegenständlichen Antrag wird die Bundesregierung u.a. aufgefordert, „sich gegen gesetzliche Beschränkungen oder Verbote kryptographischer Sicherungssysteme auszusprechen“ und „den Einsatz von sogenannten Backdoors zu verurteilen“.

Hinter Verschlüsselungsverboten oder -beschränkungen steht in der Regel der Zweck, die sicherheitsbehördliche Arbeit nicht zu be- oder verhindern. Strafverfolgungsbehörden und Nachrichtendienste warnen vor einem **„Going Dark-Problem“**: die verbreitete Nutzung von Verschlüsselungstechnik führe dazu, dass klassische Telekommunikationsüberwachungsinstrumente zunehmend an Grenzen stießen.[34] Neu sind solche Überlegungen keineswegs. Die Anfänge der sog. **„Kryptokontroverse“** reichen bis in die 1990er Jahre zurück.[35] Seitdem hat sich die Lage aber weiter verschärft. Im Bereich der Kinderpornographie etwa stellte EUROPOL fest:

> „The use of end-to-end encrypted platforms for sharing media, coupled with the use of largely anonymous payment systems, is facilitating an escalation in the live streaming of child abuse. Offenders target regions where there are high levels of poverty, limited domestic child protection measures and easy access to children.[36]“

---

[31] Vgl. dazu *Hoffmann-Riem*, JZ 2008, 1009 (1011).

[32] In diesem Sinne wohl auch *Schliesky/Hoffmann/Luch/Schulz/Borchers*, Schutzpflichten (Fn. 18), S. 104.

[33] Auch in Bezug auf Schutzpflichten anderer Grundrechte ergibt sich kein anderes Ergebnis.

[34] Näher *Schulze*, APuZ 46-47/2017, 23 (24 ff.).

[35] Siehe ausführlich *Bizer*, in: Hammer (Hrsg.), Sicherungsinfrastrukturen – Gestaltungsvorschläge für Technik, Organisation und Recht, S. 179 (179 ff.).

[36] EUROPOL, Internet Organised Crime Threat Assessment 2016, S. 10.

Auch im jüngsten „Internet Organised Crime Threat Assessment 2019“ warnte die Behörde eindringlich vor versiegenden Informationsquellen der Strafverfolgungsbehörden:

> „Encryption, while recognised as an essential element of our digitised society, also facilitates significant opportunities for criminals. Investigative techniques, such as lawful interception, are becoming increasingly ineffective (or even impossible) as criminals exploit encrypted communication services, applications and devices. Similarly, criminals can deny forensic investigators access to critical evidence by encrypting their data. The criminal abuse of encryption technologies, whether it be anonymisation via VPNs or Tor, encrypted communications or the obfuscation of digital evidence (especially in cases of CSEM), was a significant threat highlighted by respondents to this year's IOCTA survey.[37]“

Es liegt auf der Hand, dass es der deutsche Staat nicht akzeptieren kann, wenn der Vollzug geltender Gesetze infolge missbräuchlicher Verwendung von Verschlüsselungstechnik derart erschwert oder unmöglich gemacht wird. Vielmehr ist er verfassungsrechtlich verpflichtet, die **exekutive Einlösung der Staatsaufgabe „Sicherheit“** auch im Internet zu effektuieren. Einhergehend mit der Digitalisierung des Alltags müssen daher die Sicherheitsbehörden in die Lage versetzt werden, ihrem gesetzlichen Auftrag „trotz Verschlüsselung“ nachzukommen. In dieser Hinsicht motivierte gesetzliche Regelungen zur Einschränkung von Verschlüsselungen würden in die Schutzbereiche mehrerer Grundrechte (s.o.) eingreifen und bedürften einer verfassungsmäßigen Rechtfertigung.

Der schwerste denkbare Grundrechtseingriff bestünde in einem **generellen Verbot jeglichen Einsatzes von Verschlüsselungstechniken**. Eine entsprechende gesetzliche Regelung wäre indes **unzweifelhaft verfassungswidrig**. Unabhängig davon, dass einiges dafür spricht, dass eine absolute Verbotsnorm sogar den Wesensgehalt der Grundrechte antasten würde[38], würde sie sich jedenfalls als unverhältnismäßig erweisen. Denn es fehlte ihr schon an der Geeignetheit, die Erfüllung des staatlichen Sicherheitsauftrags zu fördern. Verschlüsselungssoftware wäre trotz eines Verbotes in Deutschland weiterhin anderenorts auf der Welt verfügbar. Ob sie im Einzelfall

---

[37] EUROPOL, Internet Organised Crime Threat Assessment 2019, S. 56 f.

[38] Näher *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 139 ff.

eingesetzt wird, ließe sich kaum sinnvoll überprüfen.[39] Verstößen gegen ein absolutes Verschlüsselungsverbot stünden zudem keine wirksamen Sanktionsinstrumente entgegen.

Demzufolge kommen allein gesetzliche Beschränkungen unterhalb der Schwelle eines generellen Verschlüsselungsverbots in Betracht. Eine solche Beschränkung bestünde in einer gesetzlichen Verpflichtung von Herstellern und/oder Diensteanbietern zum **Einbau von sog. „Backdoors"**. Damit sind planmäßige Sicherheitslücken in Software oder Geräten angesprochen, die in der Regel aufwendig versteckt werden müssen.[40] Aus verfassungsrechtlicher Sicht bestehen **Zweifel an der Verhältnismäßigkeit** einer gesetzlichen Verpflichtung. Bei Abwägung der schutzwürdigen verfassungsrechtlichen Positionen zeigt sich, dass einem Eingriff von großer Streubreite kaum nennenswerte Sicherheitsgewinne gegenüberstehen. Im Gegenteil: über das (notwendige) Gesetz, das zur Einführung der Hintertür anhält, würde die Existenz einer Sicherheitslücke öffentlich bekannt. Für Hackergruppierungen aus der ganzen Welt böte sich damit ein lohnendes Ziel, eine „Backdoor" aufzuspüren und auf dem internationalen Markt für „Zeroday-Exploits"[41] gewinnbringend an solche zu veräußern, die noch weniger Gutes im Schilde führen.[42] Zudem erscheint im Hinblick auf die Transnationalität des Internets fraglich, inwieweit eine gesetzliche Verpflichtung überhaupt wirksam vollzogen werden könnte.

Der Einsatz von Verschlüsselungstechnik ließe sich schließlich im Wege gesetzlicher **Pflichten zur Schlüsselherausgabe** einzelfallbezogen einschränken. Der damit verbundene Grundrechtseingriff muss verfassungsmäßig gerechtfertigt werden können. Entscheidend ist hierbei, dass sich die Herausgabepflicht an den richtigen Adressaten richtet und im übrigen verfahrensmäßige Sicherungen bestehen, die den Eingriff unter Verhältnismäßigkeitsgesichtspunkten einhegen. Denkbar erscheint zunächst, im Falle offener Ermittlungen von Strafverfolgungsbehörden eine gesetzliche

---

[39] Vgl. *Schulze*, APuZ 46-47/2017, 23 (25).

[40] Siehe näher *Schulze*, APuZ 46-47/2017, 23 (24 f.).

[41] Hierzu ausführlich *Brunst*, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, V § 7 Rn. 99.

[42] So wohl auch *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 273; *Blechschmitt*, MMR 2018, 361 (365).

Herausgabepflicht an Beschuldigte selbst zu adressieren. Die Beschuldigten würden gesetzlich auf diese Weise zu einem aktiven Tun angehalten werden. Gerade dies ist aber mit dem verfassungsrechtlich hinterlegten **„nemo-tenetur"-Grundsatz[43] nicht zu vereinbaren**, wonach niemand gezwungen werden kann, sich selbst zu belasten. Ein Zwang zur Selbstbezichtigung würde die Würde des Menschen berühren, dessen Aussage als Mittel gegen ihn selbst verwendet wird.[44] Eine **gesetzliche Herausgabepflicht** von Beschuldigten wäre demzufolge **verfassungswidrig**.

Möglich ist dagegen, die **Herausgabe von Schlüsseln und Passwörtern von privaten Dritten** (z.B. Systemadministratoren oder Diensteanbietern) zu verlangen. Verfassungsrechtlich bestehen hiergegen grundsätzlich keine Bedenken, solange das Zusammenspiel aus tatbestandlichen Eingriffsschwellen für behördliche Maßnahmen (z.B. Anhaltspunkte eines Verdachts für schwere Straftaten) und verfahrensmäßigen Sicherungen (z.B. ein Richtervorbehalt) der Intensität des Grundrechtseingriffs gerecht wird. Teilweise sind Herausgabepflichten für Diensteanbieter bereits gesetzlich geregelt worden. § 8 Abs. 3 der Telekommunikations-Überwachungsverordnung (TKÜV)[45] verpflichtet Anbieter von Telekommunikationsdiensten, Schlüssel aufzuheben und den Sicherheitsbehörden bereitzustellen, wenn die Telekommunikation netzseitig – durch den Dienstanbieter selbst – verschlüsselt wird. Eine teilnehmerautonome Verschlüsselung wird von der Norm allerdings nicht erfasst, ebenso wenig die Internet-Telefonie.[46] Hinzu kommt, dass nach einer jüngsten Entscheidung des EuGH E-Mail-Dienste (wie etwa GMail, GMX), die keinen Internetzugang vermitteln, keinen „elektronischen Kommunikationsdienst" im europarechtlichen Sinne darstellen[47]. Infolgedessen können sie auch nicht im Wege des Telekommunikationsgesetzes (TKG)[48] und der TKÜV verpflichtet werden. Einen

---

[43] Grundlegend zum „nemo tenetur se ipsum accusare"-Prinzip BGHSt 38, 214 (214 ff.).

[44] BVerfGE 38, 105 (114 f.); 56, 37 (42).

[45] Telekommunikations-Überwachungsverordnung i. d. Fassung der Bekanntmachung vom 11. Juli 2017 (BGBl. I S. 2316), zuletzt geändert durch Art. 27 d. Gesetzes v. 20.11.2019 (BGBl. I S. 1724).

[46] Vgl. *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 302.

[47] EuGH NVwZ 2019, 1118 (1120).

[48] Telekommunikationsgesetz vom 22.06. 2004 (BGBl. I S. 1190), zuletzt geändert d, Art. 1 des G. vom 5.11.2019 (BGBl. I S. 2005).

Ausweg soll eine Änderung des § 15a Telemediengesetz (TMG) versprechen. Nach § 15a TMG in der Fassung des Referentenentwurfs[49] sollen Anbieter zur Auskunft über Bestandsdaten verpflichtet werden, „mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird“. Angesprochen sind damit z.B. Passwörter von E-Mailkonten oder von Cloud-Diensten. Tatsächlich kollidiert diese Regelung mit bestehenden Verpflichtungen aus der DS-GVO, denn die Anbieter sind grundsätzlich gehalten, Passwörter nicht im Klartext zu speichern. Sie verfügen lediglich über Hashwerte, die aber wiederum den Sicherheitsbehörden nichts nützen. Insofern hätte § 15a TMG n.F. wohl lediglich geringe praktische Relevanz.

IV. Behördliche Meldepflicht und Ankauf von IT-Sicherheitslücken

Im gegenständlichen Antrag wird die Bunderegierung aufgefordert,

> „alle staatlichen Behörden zu verpflichten, IT-Sicherheitslücken unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden“ sowie
>
> „(…) eine staatliche Beteiligung an digitalen Grau- und Schwarzmärkten für Sicherheitslücken abzulehnen“.

Beide Forderungen sind in einer Gesamtschau in den Blick zu nehmen. Eine allgemeine behördliche Meldepflicht ist zunächst vor dem Hintergrund von § 7 BSIG zu sehen. Danach ist das BSI befugt, zur **Erfüllung seiner gesetzlichen Aufgaben vor Sicherheitslücken und Schadprogrammen warnen**. Dabei steht dem BSU ein Ermessen zu, ob und in welchem Umfang es warnt. In eine Abwägung sind einerseits die Interessen der IT-Anwender einzustellen.[50] Ihnen würde durch die behördliche Warnung die Möglichkeit evtl. eröffnet, eigene Schutzmaßnahmen zu ergreifen. Andererseits muss das BSI berücksichtigen, ob durch die Veröffentlichung einer Schutzlücke schon deshalb ein Schaden entsteht, weil diese nicht so schnell geschlossen werden kann und gerade deshalb ein Angriffsziel darstellt. Möglicherweise kann eine Warnung auch unterbleiben, wenn ein Hersteller die Sicherheitslücke be-

[49] Siehe https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_ BekaempfungHatespeech. pdf?blob=publicationFile&v=1 (Stand: 22.01.2020).

[50] Zum Folgenden ausführlich *Buchberger*, GSZ 2019, 183 (187 f.).

reits erkannt hat und an Abhilfe arbeitet. Schließlich kann der Adressatenkreis der Warnung nach § 7 Abs. 1 S. 4 BSIG insbesondere beschränkt werden, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern.[51]

Eine **allgemeine behördliche Meldepflicht von Sicherheitslücken** würde das BSI darin unterstützen, seiner Warnfunktion besser nachkommen zu können. Gleichwohl darf nicht übersehen werden, dass Strafverfolgungsbehörden und Nachrichtendienste u.U. ein Interesse daran haben können, dass Sicherheitslücken nicht sofort geschlossen werden, um sie für eigene Zwecke – etwa zur Durchführung einer Quellen-Telekommunikationsüberwachung oder einer sog. Online-Durchsuchung – zu nutzen.[52] Der Bedarf an einer Ausnutzung von Sicherheitslücken steigt: wie gezeigt stoßen klassische Überwachungsinstrumente infolge zunehmender Verbreitung von Verschlüsselungstechniken zunehmend an ihre Grenzen. Gleichzeitig erweisen sich gesetzliche Beschränkungen von Verschlüsselungen als unzulässig oder kaum durchsetzbar (s.o.). Die Sicherheitsbehörden müssen demgemäß in die Lage versetzt werden, ihrem gesetzlichen Auftrag **auf anderem Wege** nachzukommen. Dazu gehört auch, im Einzelfall Sicherheitslücken auf dem freien Markt zu erwerben, wenn anders der Schutz überragend wichtiger Rechtsgüter nicht sichergestellt werden kann.

Es geht damit um eine **(Schutz-) Pflichtenkollision**. Den Sicherheitsbehörden obliegt der Schutz der Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht sowie der von ihm zu gewährleistenden Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit.[53] Auf der anderen Seite stehen grundrechtlich geschützte Rechtspositionen des einzelnen IT-Anwenders. Diese Pflichtenkollision lässt sich nicht mit einer einseitigen allgemeinen behördlichen Meldepflicht für Sicherheitslücken lösen. Auch das grundsätzliche Verbot eines behördlichen Ankaufs von Sicherheitslücken ist kontraproduktiv. Vielmehr bedarf es **flexibler gesetzlicher**

---

[51] Siehe *Buchberger*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2018, BSIG § 7 Rn. 7.

[52] Zum „Wettlauf um Zeroday-Exploits“ siehe *Brunst*, in: Dietrich/Eiffler (Hrsg.), HdbRdN (Fn. 41), V § 7 Rn. 97 ff.

[53] BVerfGE 120, 274 (319).

Konfliktschlichtungsformeln in den Gesetzen der Sicherheitsbehörden.[54] Danach würde etwa die jeweilige Behörde selbst zur Abwägung ermächtigt, ob eine Weitergabe von Informationen an das BSI erfolgen sollte. Es versteht sich von selbst, dass sich das eingeräumte Ermessen umso mehr reduziert, je gefährlicher sich eine Sicherheitslücke auswirken kann. So wäre etwa bei einer Gefährdung der IT-Sicherheit sog. Kritischer Infrastrukturen (z.B. Atomkraftwerke) das behördliche Ermessen auf null reduziert. Vorbildcharakter für eine gesetzliche Regelung könnte § 7 Abs. 4a des Artikel-10-Gesetzes (G10) entfalten. Danach *darf* der Bundesnachrichtendienst (BND) personenbezogene Daten aus der Telekommunikationsüberwachung an das BSI übermitteln, „wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Daten erforderlich sind zur Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes oder zur Sammlung und Auswertung von Informationen über Sicherheitsrisiken auch für andere Stellen und Dritte“.

(Prof. Dr. Jan-Hendrik Dietrich)

[54] So wohl auch *Derin/Golla*, NJW 2019, 1111 (1115).