BfDI
Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

RA Dr. Spengler
Eing.: 12. Okt. 2020

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Bundesverfassungsgericht
Erster Senat
- Der Vorsitzende -
Postfach 17 71
76006 Karlsruhe

Bundesverfassungsgericht
Eing. 01. 10. 20 8-9
Doppel
Anl.
Ed.
Doppel

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-5000
FAX (0228) 997799-5550
E-MAIL referat32@bfdi.bund.de
INTERNET www.bfdi.bund.de
DATUM Bonn, 28.09.2020
GESCHÄFTSZ. 32-642/054#1470

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Verfassungsbeschwerde gegen § 15b und § 15c des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung**
HIER Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
BEZUG Ihr Schreiben vom 17.04.2020 (Az.: 1 BvR 1552/19)

Sehr geehrter Herr Vorsitzender,

für Ihr Schreiben vom 17. April 2020, hier zugestellt am 14. Mai 2020, in dem Sie mir Gelegenheit zur Stellungnahme im o.g. Verfassungsbeschwerdeverfahren einräumen, danke ich Ihnen. Gerne nehme ich die Gelegenheit wahr und übersende Ihnen anbei meine Stellungnahme wie erbeten in 20-facher Ausfertigung.

Mit freundlichen Grüßen

Ulrich Kelber

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

BfDI Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 28.09.2020

Stellungnahme

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

im Verfassungsbeschwerdeverfahren – 1 BvR 1552/19 –
gegen § 15b und § 15c des Hessischen Gesetzes
über die öffentliche Sicherheit und Ordnung (HSOG)
in der Fassung des Gesetzes zur Neuausrichtung
des Verfassungsschutzes in Hessen vom 25. Juni 2018 (GVBL S. 302)

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Die mit der Verfassungsbeschwerde angegriffenen Rechtsvorschriften – § 15b und § 15c HSOG – genügen meiner Ansicht nach nicht dem verfassungsrechtlichen Gebot, informationstechnische Systeme gegen Dritte zu schützen.

1. Verfassungsrechtliche Notwendigkeit staatlicher Maßnahmen zum Schutz von IT-Systemen

Die Frage der verfassungsrechtlichen Notwendigkeit staatlicher Maßnahmen zum Schutz informationstechnischer Systeme (weiter: IT-Systeme) ist anhand des Maßstabes grundrechtlicher Schutzpflichten und des Gebotes der Folgerichtigkeit zu beurteilen.

Nach der Rechtsprechung des Bundesverfassungsgerichts begründet Art. 10 Abs. 1 GG neben einem Abwehrrecht gegen die Kenntnisnahme des Inhalts und der näheren Umstände der Telekommunikation durch den Staat auch einen Auftrag an den Staat, Schutz auch insoweit vorzusehen, als private Dritte sich Zugriff auf die Kommunikation verschaffen (BVerfGE 106, 28 [37]). Auch aus dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG kann eine Schutzpflicht des Staates resultieren (BVerfGE 54, 148 [153]; 79, 256 [268]; 96, 56 [64]). Der Staat ist „grundrechtlich gehalten, den Einzelnen vor Persönlichkeitsgefährdungen durch Dritte zu schützen" (BVerfGE 99, 185 [194 f.]). Konsequenterweise wird in der juristischen Literatur aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ebenfalls eine Schutzpflicht des Staates für die IT-Sicherheit abgeleitet (vgl. Derin/Golla, NJW 2019, 1111 [1114] m.w.N.). Dass der Staat zur Gewährleistung von Freiheit und Sicherheit auch im Cyber-Raum verpflichtet ist, dürfte unstreitig sein (vgl. z.B. Unterrichtung durch die Bundesregierung zur Cyber-Sicherheitsstrategie für Deutschland 2016, BT-Drucks. 18/10395, S. 4).

Verfassungsrechtlich ist der Gesetzgeber besonders verpflichtet, die mit dem Einsatz der Quellen-Telekommunikationsüberwachung und Online-Durchsuchung verbundenen Risiken für die Freiheiten der betroffenen Bürger im Korridor zwischen Übermaß- und Untermaßverbot zu schützen. „Die Vorkehrungen, die der Gesetzgeber trifft, müssen für einen angemessenen und wirksamen Schutz ausreichend sein und zudem auf sorgfältigen Tatsachenermittlungen und vertretbaren Einschätzungen beruhen" (BVerfGE 88, 203 [254]). Im Hinblick auf das Untermaßverbot muss die Ausgestaltung des Schutzes

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn FAX +49 (0)228-997799-5550 INTERNET www.bfdi.bund.de

durch die Rechtsordnung Mindestanforderungen entsprechen (BVerfGE 88, 203 [255]), wobei der Inhalt der Schutzpflicht von der Art, der Nähe und dem Ausmaß möglicher Gefahren, der Art und dem Rang des verfassungsrechtlich geschützten Rechtsguts sowie von den schon vorhandenen Regelungen abhängt (BVerfGE 49, 89 [142]).

Unter dem Gesichtspunkt der Folgerichtigkeit ist der Gesetzgeber zur konsequenten Weiterverfolgung eines einmal gewählten Regelungskonzepts verpflichtet (BVerfGE 121, 317 [362]). Das Rechtsstaatsprinzip verlangt im Interesse der Vermeidung von Widersprüchen in der Rechtsordnung abgestimmte Regelungen. Dies gilt nicht nur für das Verhältnis zwischen den Regelungen desselben Gesetzgebers, sondern z.B. auch für Regelungen verschiedener Gesetzgeber auf Bundes- und Landesebene (BVerfGE 98, 106 [118 f.]; P. Kirchhof, in: Maunz/Dürig, Grundgesetz-Kommentar, Werkstand: 90. EL Februar 2020, Art. 3 Abs. 1, Rn. 408; Bethge, in: Maunz/Schmidt-Bleibtreu/Klein/Bethge, Bundesverfassungsgerichtsgesetz, Werkstand: 58. EL Januar 2020, § 91 BVerfGG, Rn. 67).

1.1. IT-Sicherheitslücken

IT-Sicherheitslücken begründen ein enormes Gefährdungspotenzial für die Vertraulichkeit der Kommunikation und für die Privatsphäre der Bürger in Gestalt möglicher Ausspähung durch Dritte. Dies gilt in besonderem Maße für jene Sicherheitslücken, die dem Hersteller des jeweiligen IT-Systems bzw. der jeweiligen Software nicht bekannt sind (weiter: Zero-Day-Exploits).

1.1.1. Staatliches Schutzkonzept

Der daraus resultierenden Schutzpflicht wird nicht Genüge getan, da ein in sich abgestimmtes Schutzkonzept fehlt. Mehr noch: Gesetzlich ist nicht festgelegt, ob die zuständigen Behörden die Informationen über derartige Sicherheitslücken für Maßnahmen der Quellen-Telekommunikationsüberwachung und Online-Durchsuchung ausnutzen und geheim halten dürfen. Insoweit nimmt der Staat „sehenden Auges" äußerst schwerwiegende Gefahren für die o.g. Rechtsgüter sowie für das allgemeine Wohl hin.

Sofern der Staat Befugnisse schafft, mit denen die Behörden Sicherheitslücken ausnutzen dürfen, setzt er sich zu seinem eigenen Schutzkonzept

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

zur IT-Sicherheit in Widerspruch, das im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) zum Ausdruck kommt. Neben der Beratung der Bundesverwaltung und der Information der Öffentlichkeit ist es Aufgabe des BSI, die Gewährleistung von Cybersicherheit in Deutschland zu unterstützen. Wenn der Gesetzgeber den Aufgaben des BSI neben der Abwehr von Gefahren für die Sicherheit in der Informationstechnik des Bundes eine zunehmende Bedeutung attestiert, das BSI als eine nationale „Informationssicherheitsbehörde" qualifiziert (vgl. BT-Drucks. 18/4096, S. 23) und zur Erfüllung seiner Aufgaben mit weitreichenden Befugnissen ausstattet (vgl. insbesondere § 5 BSIG), entspricht es dem Gebot der Folgerichtigkeit, das gewählte Konzept auch konsequent weiterzuverfolgen (vgl. BVerfGE 121, 317 [362]). Offenkundig wird der Widerspruch im Hinblick auf die Benachrichtigungspflicht des BSI gegenüber den Beteiligten des Kommunikationsvorgangs gemäß § 5 Abs. 4 BSIG. Widersprüchlich ist es ferner, wenn das BSI zur Erfüllung seiner Aufgaben gemäß § 7 BSIG die Öffentlichkeit und betroffene Kreise vor Sicherheitslücken und Schadprogrammen warnen kann, andere (Sicherheits-) Behörden dieselben Sicherheitsrisiken jedoch geheim halten dürfen. In der von der Bundesregierung formulierten Cyber-Sicherheitsstrategie für Deutschland 2016 hieß es zu Recht: „Staat, Wirtschaft, Wissenschaft und Gesellschaft tragen für die Sicherheit des Cyber-Raums eine gemeinsame Verantwortung. Sie müssen daher auch aufeinander abgestimmte Antworten auf die jeweils aktuellen Herausforderungen geben" (BT-Drucks. 18/10395, S. 4). Demgegenüber zieht es der Gesetzgeber jedoch in systemwidriger Weise vor, die rechte Hand nicht wissen zu lassen, was die linke tut.

Generell ist nicht ersichtlich, wie der Gesetzgeber den Gefahren, die mit der gesetzlich nicht ausgeschlossenen Ausnutzung von Sicherheitslücken verbunden sind, mit einem einheitlichen Konzept im Hinblick auf alle Behörden zu begegnen gedenkt.

1.1.2. Empirische Datengrundlage

Die Geeignetheit und Erforderlichkeit von Quellen-Telekommunikationsüberwachung und Online-Durchsuchung hängen in hohem Maße von der praktischen Relevanz und Wirksamkeit dieser Ermittlungsmaßnahmen ab. Ich rege gegenüber den betroffenen Behörden an, zunächst empirische Daten darüber vorzulegen, wie sich der Einsatz von Quellen-Tele-

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

kommunikationsüberwachung und Online-Durchsuchung in der bisherigen Vollzugspraxis – gegebenenfalls anderer Sicherheitsbehörden – auf die Aufklärungsquote ausgewirkt haben.

Ich rege an, die Sicherheitsbehörden ebenfalls zu bitten, empirisch darzulegen, in welchem Umfang Sicherheitslücken genutzt werden (müssen).

1.1.3. Subsidiarität der Ausnutzung von Sicherheitslücken

Sieht ein Gesetz vor, dass die Sicherheitsbehörden Sicherheitslücken ausnutzen dürfen, so muss es die Einzelheiten regeln. Unter anderem ist zu regeln, in welchem Umfang Sicherheitsbehörden gegebenenfalls Informationen über Sicherheitslücken „bevorraten" dürfen. Alternativ kann vorgesehen werden, dass das Vorhalten entsprechender Informationen nicht von der Pflicht entbindet, die Informationen mit den von der Lücke betroffenen Hard- und Softwareanbietern oder dem BSI zu teilen.

1.2. Gesetzliche Vorgaben an die Überwachungssoftware

Zum Schutz von IT-Systemen gegenüber Dritten gehört auch die Beschaffenheit der eingesetzten Überwachungssoftware. Die für die verfassungsrechtliche Beurteilung maßgebliche Eingriffsintensität sowie das Gefährdungspotenzial für die Vertraulichkeit der Kommunikation und die Privatsphäre des Einzelnen hängen in hohem Maße davon ab, wie die Überwachungssoftware ausgestaltet ist. Maßgebend sind vor allem die Herkunft der Software, die Ausgestaltung von Nachladefunktionen und der Ort der Speicherung der durch die Software erfassten Daten. Schon die Wesentlichkeitstheorie des BVerfG, nach der der Gesetzgeber im Bereich der Grundrechtsausübung alle wesentlichen Entscheidungen selbst zu treffen hat (vgl. BVerfGE 116, 24 [58]), verlangt gesetzliche Vorgaben – ggf. verbunden mit einer Verordnungsermächtigung – bezüglich der Beschaffenheit der Überwachungssoftware.

In dieselbe Richtung weist auch das Gebot der Folgerichtigkeit. So müssen beispielsweise Messgeräte vor ihrem Inverkehrbringen den in § 6 Abs. 2 Mess- und Eichgesetz (MessEG) festgelegten und in einer Rechtsverordnung (Mess- und Eichverordnung – MessEV) konkretisierten Anforderungen genügen (§ 6 Abs. 1 MessEG). Wenn schon die Anforderungen an Messgeräte, die z.B. zur amtlichen Überwachung des öffentlichen Verkehrs eingesetzt werden (vgl. § 1 Abs. 1 Nr. 12 Buchst. a MessEV), gesetzlich festgelegt sind, ist kein sachlicher Grund ersichtlich, warum dies bei

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn FAX +49 (0)228-997799-5550 INTERNET www.bfdi.bund.de

der zum Zweck der Quellen-Telekommunikationsüberwachung und Online-Durchsuchung eingesetzten Software nicht auch der Fall ist. Denn der Gesetzgeber sieht dies bei weit weniger gefahrträchtigen Messgeräten als erforderlich an (vgl. in diese Richtung auch Gazeas, Stellungnahme zur Anhörung des Innenausschusses am 7. Juni 2018 zum Gesetzesentwurf der Landesregierung – 6. Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen (LT-Drs. 17/2351), Landtag NRW 17/662, 19 f.).

Aufgrund der bedrohlichen Cyber-Sicherheitslage ist es geboten, den Umgang der staatlichen Behörden mit IT-Sicherheitslücken gesetzlich zu regeln.

2. Einfachgesetzliche Rechtslage

Den oben aufgezeigten Schutzpflichten trägt die aktuelle einfachgesetzliche Rechtslage nicht ausreichend Rechnung.

2.1. § 15b und § 15c HSOG

Weder § 15b noch § 15c HSOG hindern die Polizeibehörden daran, bestehende Sicherheitslücken – darunter auch die Zero-Day-Exploits – zu nutzen.

Vorgaben hinsichtlich der Beschaffenheit der „technischen Mittel" sind in § 15b und § 15c HSOG nur rudimentär geregelt. Die Entscheidung über wesentliche Aspekte wie Herkunft der Software, Ausgestaltung von Nachladefunktionen und Ort der Datenspeicherung überlassen die angegriffenen Vorschriften der Exekutive. Ein abgestimmtes Schutzkonzept im Zusammenhang mit dem Umgang mit IT-Sicherheitslücken ist nicht ersichtlich.

2.2. § 64 Abs. 1 BDSG

§ 64 Abs. 1 Satz 1 BDSG, der Art. 29 der RL (EU) 2016/680 umsetzt, verpflichtet den Verantwortlichen und den Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen, die erforderlichen technischen und organisatorischen Maßnahmen zu treffen,

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Gemäß § 64 Abs. 1 Satz 1 Nr. 1 BDSG sollen die zu ergreifenden Maßnahmen u.a. dazu führen, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden.

- Die Vorgaben des § 64 Abs. 1 BDSG sind auch beim Einsatz einer Überwachungs-Software im Rahmen von Quellen-Telekommunikationsüberwachung und Online-Durchsuchungen zu berücksichtigen. In der Aufsichtspraxis des BfDI werden auf diese Norm – in Verbindung mit spezialgesetzlichen Vorgaben wie z.B. § 52 Abs. 2 Satz 2 BKAG – vor allem folgende Anforderungen gestützt: Es muss klar geregelt sein, wer zum Zugriff auf die Überwachungssoftware und zu deren Steuerung befugt ist. Dementsprechend dürfen der Zugang und die Steuerung nur einem festgelegten Kreis der berechtigten Personen möglich sein.
- Bei der Übertragung der ausgeleiteten Datenströme müssen deren Vertraulichkeit und Integrität gewährleistet sein. Insbesondere ist sicherzustellen, dass die Datenströme nur den berechtigten Personenkreis erreichen.
- Erforderlich ist ein Löschkonzept, das ein nachhaltiges Löschen der Überwachungssoftware nach Beendigung der Maßnahme ermöglicht.
- Die Überwachungssoftware darf über keine Funktionen verfügen, die für die Durchführung der jeweiligen gesetzlich zulässigen Maßnahme nicht erforderlich sind.
- Der Quellcode – flankiert durch eine entsprechende Dokumentation – muss zum Zweck der Überprüfung einsehbar sein.
- Bei der Beschaffung der Überwachungssoftware sollte auf Eigenentwicklung gesetzt werden.

Die Aufsichtspraxis des BfDI zeigt, dass die Erfüllung der o.g. Anforderungen den verantwortlichen Stellen möglich ist.

Aufgrund der spezifischen Gefahren der Quellen-TKÜ und Online-Durchsuchung sind jedoch verarbeitungsspezifische Regelungen notwendig, die den damit verbundenen Risiken und der hohen Intensität potenzieller Grundrechtsbeeinträchtigungen auch durch Dritte bereichsspezifisch Rechnung tragen.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de