Hessische Staatskanzlei

HESSEN

Hessische Staatskanzlei · Postfach 31 47 · 65021 Wiesbaden

Bundesverfassungsgericht
- Erster Senat -
Schlossbezirk 3
76131 Karlsruhe

Per Fax vorab!

Aktenzeichen RUV 05/0931 -
Bearbeiterin Herr Prof. Dr. Günther
Durchwahl/Fax 3738161323806
E-Mail herbert.guenther@stk.hessen.de
Ihr Zeichen
Ihre Nachricht
Datum 27. Oktober 2020

In dem Verfahren über die Verfassungsbeschwerden

1. des Herrn Helge H e r g e t,
   Goerdelerstraße 112a, 63071 Offenbach,

2. des Herrn Gregory E n g e l s,
   Parkstraße 61, 63067 Offenbach,

3. der Piratenpartei Deutschland Landesverband Hessen,
   vertreten durch den Vorstand,
   Pflugstraße 9a, 10115 Berlin

- Bevollmächtigter: Rechtsanwalt Dr. Peter Spengler,
Schleiermacherstraße 2, 64283 Darmstadt -

- **1 BvR 1552/19** -

äußere ich mich für die Hessische Landesregierung:

I.

Mit ihrer Verfassungsbeschwerde vom 3. Juli 2019 wenden sich die Beschwerdeführer gegen zwei Bestimmungen des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (im Folgenden: HSOG), die den Polizeibehörden des Landes den verdeckten Zugriff auf informationstechnische Systeme zur Telekommunikationsüberwachung (§ 15b HSOG, „Quellen-TKÜ“) und zur Durchsicht der auf den Endgeräten vor-

65183 Wiesbaden
Georg-August-Zinn-Straße 1
Telefon (06 11) 32 0
Telefax (06 11) 32 37 08
E-Mail: poststelle@stk.hessen.de
Internet: www.hessen.de

handenen Daten (§ 15c HSOG, „Online-Durchsuchung") gestatten und in ihrer derzeit geltenden Fassung - so § 15b HSOG - oder als Neuregelung - so § 15c HSOG am 4. Juli 2018 in Kraft getreten sind. Die Verfassungswidrigkeit dieser Bestimmungen leiten die Beschwerdeführer daraus her, dass der Gesetzgeber verpflichtet gewesen sei, es jedoch unterlassen habe, mit der Schaffung dieser Befugnisse „zugleich angemessene Vorkehrungen gegen die durch den Einsatz von Staatstrojanern geförderten Fehlentwicklungen zu treffen, insbesondere strikte Pflichten der ermächtigten Behörden für den Umgang mit digitalen Sicherheitslücken und Schwachstellen gesetzlich zu verankern" (Beschwerdeschrift - im Folgenden: BS - S. 21).

1. Die angegriffenen Vorschriften haben folgenden Wortlaut:

„§ 15b

Telekommunikationsüberwachung an informationstechnischen Systemen

(1) Unter den Voraussetzungen des § 15a Abs. 1 kann die Überwachung und Aufzeichnung der Telekommunikation ohne Wissen der betroffenen Person in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn

1. *durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und*
2. *der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.*

(2) 1Es ist technisch sicherzustellen, dass

1. *an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und*
2. *die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.*

[2]Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. [3]Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) [1]§ 15 Abs. 4 Satz 4 bis 6 gilt entsprechend. [2]§ 15 Abs. 5 Satz 1 bis 9 gilt entsprechend mit der Maßgabe, dass das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, in der Anordnung möglichst genau zu bezeichnen ist. [3]§ 15 Abs. 9 Satz 1 bis 7 gilt entsprechend.

§ 15c

Verdeckter Eingriff in informationstechnische Systeme

(1) Die Polizeibehörden können ohne Wissen der betroffenen Person mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn dies zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, unerlässlich ist.

(2) [1]Eine Maßnahme nach Abs. 1 darf sich nur gegen eine Person richten, die nach den §§ 6 oder 7 verantwortlich ist, und nur in die von dieser Person genutzten informationstechnischen Systeme eingreifen. [2]Eine Maßnahme nach Abs. 1 ist auch gegen eine in § 15 Abs. 2 Satz 1 Nr. 2 oder 3 genannte Person zulässig, soweit dies zur Verhütung terroristischer Straftaten unerlässlich ist. [3]In informationstechnische Systeme anderer Personen darf die Maßnahme nur eingreifen, wenn Tatsachen die Annahme rechtfertigen, dass eine in Satz 1 oder 2 genannte Person dort ermittlungsrelevante Informationen speichert, und dies unerlässlich ist. [4]Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(3) [1]§ 15b Abs. 2 gilt entsprechend. [2]§ 15 Abs. 4 Satz 4 bis 6 gilt entsprechend mit der Maßgabe, dass, soweit möglich, technisch sicherzustellen ist, dass Da-

ten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. [3]§ 15 Abs. 5 Satz 1 bis 9 gilt entsprechend mit der Maßgabe, dass das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, in der Anordnung möglichst genau zu bezeichnen ist. [4]§ 15 Abs. 9 Satz 1 bis 7 gilt entsprechend für Erkenntnisse, die nach Abs. 1 und 2 erlangt worden sind."

> Die Nummerierung der Sätze ist hier und in der folgenden Wiedergabe des Gesetzestexts zur besseren Auffind- und Zitierbarkeit eingefügt worden.

Beide Vorschriften sind - § 15b in seiner gegenwärtigen Fassung und § 15c insgesamt - als Art. 3 („Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung") Nr. 2e. und Nr. 2f. Teil des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen vom 25. Juni 2018, das im Gesetz- und Verordnungsblatt des Landes Hessen vom 3. Juli 2018 (GVBl. S. 302, hier S. 319) verkündet worden und nach Art. 5 dieses Gesetzes am Tag nach der Verkündung, also am 4. Juli 2018 in Kraft getreten ist. Von den nachfolgenden Gesetzesänderungen

> Art. 2 des Gesetzes zur Änderung des Hessischen Brand- und Katastrophenschutzgesetzes und des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung v. 23.08.2018 (GVBl. S. 374) und Art. 10 des Gesetzes zur Verbesserung der politischen Teilhabe von ausländischen Einwohnerinnen und Einwohnern an der Kommunalpolitik sowie zur Änderung kommunal- und wahlrechtlicher Vorschriften v. 07.05.2020 (GVBl. S. 318)

sind sie nicht betroffen.

In seiner ursprünglichen Fassung findet sich § 15b HSOG erstmals in Art. 1 Nr. 8 des am 23. Dezember 2009 (Art. 8) in Kraft getretenen Gesetzes zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze vom 14. Dezember 2009 (GVBl. I S. 635). Zuvor hatte sich das Hessische Gesetz über die öffentliche Sicherheit und Ordnung in seiner bis heute letztmals bekanntgemachten Neufassung vom 14. Januar 2005 (GVBl. I S. 14) darauf beschränkt, in § 15a als „Datenerhebung durch Telekommunikationsüberwachung" Auskunftsbefugnisse gegenüber Telekommunikationsdienstleistern zu begründen und den Einsatz technischer Mittel zur Ermittlung des Stand-

ortes, der Geräte- und der Kartennummer von Mobilfunkendgeräten zuzulassen. Bevor § 15b HSOG durch das oben zitierte Gesetz vom 25. Juni 2018 seine gegenwärtige Fassung erhielt, hatte die Vorschrift aufgrund ihrer unmittelbar vorangegangenen Änderung durch Art. 18 Nr. 9a. des Gesetzes vom 3. Mai 2018 (GVBl. S. 82, 149) folgenden Wortlaut:

„§ 15b

Telekommunikationsüberwachung an informationstechnischen Systemen

(1) Wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist, kann die Überwachung und Aufzeichnung der Telekommunikation ohne Wissen der betroffenen Person in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn

1. *durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und*
2. *der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.*

(2) [1]Es ist technisch sicherzustellen, dass

1. *an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und*
2. *die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.*

[2]Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.

(3) [1]Die Maßnahme darf sich nur gegen eine Person richten, die nach den §§ 6 oder 7 verantwortlich ist. [2]Sie darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(4) § 15 Abs. 4 Satz 2 bis 5 und Abs. 5 gilt entsprechend mit der Maßgabe, dass das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, in der Anordnung möglichst genau zu bezeichnen ist."

Das nunmehr angegriffene Gesetz vom 25. Juni 2018, das in § 15b HSOG die Zulässigkeitsvoraussetzungen der Quellen-TKÜ neu formuliert und mit § 15c HSOG die Online-Durchsuchung neu eingeführt hat, beschränkt sich (GVBl. 2018 S. 302, 324) in seinem Art. 3 Nr. 2e. somit auf die folgenden Änderungen von § 15b:

„a) In Abs. 1 werden die Wörter „Wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist," durch die Angabe „Unter den Voraussetzungen des § 15a Abs. 1" ersetzt.

b) Dem Abs. 2 wird folgender Satz angefügt:

„Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen."

c) Abs. 3 wird aufgehoben.

d) Der bisherige Abs. 4 wird Abs. 3 und wie folgt gefasst:

„(3) § 15 Abs. 4 Satz 4 bis 8 gilt entsprechend. § 15 Abs. 5 Satz 1 bis 9 gilt entsprechend mit der Maßgabe, dass das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, in der Anordnung möglichst genau zu bezeichnen ist. § 15 Abs. 9 Satz 1 bis 7 gilt entsprechend.""

§ 15a Abs. 1 HSOG, auf den § 15b Abs. 1 HSOG nunmehr Bezug nimmt, hat durch Art. 3 Nr. 2d. Buchst. a) desselben Gesetzes (GVBl. 2018 S. 302, 323) die folgende Fassung erhalten:

„§ 15a

(1) [1]Die Polizeibehörden können von einem Dienstanbieter, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, verlangen, dass er die Kenntnisnahme durch Überwachung und Aufzeichnung des Inhalts der Te-

lekommunikation ermöglicht und die näheren Umstände der Telekommunikation einschließlich des Standorts aktiv geschalteter nicht ortsfester Telekommunikationsanlagen ermittelt, wenn dies zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, unerlässlich ist. [2]Die Maßnahme darf sich gegen eine Person richten,

1. *die nach den §§ 6 oder 7 verantwortlich ist,*
2. *bei der die Voraussetzungen des § 9 vorliegen,*
3. *bei der bestimmte Tatsachen die Annahme rechtfertigen, dass*
   a) *sie für eine Person nach Nr. 1 bestimmte oder von dieser herrührende Mitteilungen entgegennimmt oder weitergibt oder*
   b) *eine Person nach Nr. 1 deren Kommunikationsanschluss oder Endgerät benutzen wird, soweit die Maßnahme zur Verhütung terroristischer Straftaten unerlässlich ist, oder*
4. *die in § 15 Abs. 2 Satz 1 Nr. 2 oder 3 genannt ist, soweit die Maßnahme zur Verhütung terroristischer Straftaten unerlässlich ist.*

[3]Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden. [4]§ 15 Abs. 4 Satz 4 bis 8 gilt entsprechend.

[(2) ... (7)]."

Der zu § 15b Abs. 3 gewordene frühere Abs. 4 (Art. 3 Nr. 2a. Buchst. d) des Gesetzes) verweist auf § 15 Abs. 4 Satz 4 bis 8, Abs. 5 Satz 1 bis 9 und Abs. 9 Satz 1 bis 7 HSOG, den das Gesetz in Art. 3 Nr. 2c. Buchst. b) neu gefasst oder - so im Fall von § 15 Abs. 9 (Art. 3 Nr. 2c. Buchst. e)) - neu eingefügt hat. Mit Hilfe dieser Verweisungen werden die materiellen Anforderungen an die Zulässigkeit informationstechnischer Eingriffe neu bestimmt, es werden Verfahrensregeln für die Einleitung derartiger Maßnahmen zur Sicherstellung des richterlichen Genehmigungsvorbehalts festgelegt und Bestimmungen über die Auswertung und Löschung ihrer Ergebnisse getroffen; auf Einzelheiten wird, soweit erforderlich, noch einzugehen sein. Dass der in § 15b Abs. 1 in Bezug genommene § 15a

Abs. 1 in seinem Satz 4 gleichfalls § 15 Abs. 4 Satz 4 bis 8 für entsprechend anwendbar erklärt, ist als Verdoppelung dieses Rechtsanwendungsbefehls unschädlich.

§ 15c HSOG enthält ähnliche Bezugnahmen für den verdeckten Eingriff in informationstechnische Systeme: § 15c Abs. 2 HSOG erweitert mit dem Verweis auf den gleichfalls neuen (Art. 3 Nr. 2c. Buchst. b)) § 15 Abs. 2 Satz 1 Nr. 2 und 3 HSOG den Kreis der in Betracht kommenden Zielpersonen über die Verhaltens- (§ 6 HSOG) und Zustandsstörer (§ 7 HSOG) hinaus. Der oben (S. 2) wörtlich wiedergegebene § 15b Abs. 2 sowie § 15 Abs. 4 Satz 4 bis 6, Abs. 5 Satz 1 bis 9 und Abs. 9 Satz 1 bis 7 gelten entsprechend (§ 15c Abs. 3).

2. Die zunehmende Verbreitung verschlüsselter Kommunikation macht die Auswertung und Verarbeitung der durch die Telekommunikationsüberwachung erlangten Informationen und schon deren Gewinnung immer schwieriger und teilweise sogar unmöglich; denn häufig läuft die Überwachung des Fernmeldeverkehrs deshalb ins Leere, weil die überwachten Nutzer verschlüsselte Kommunikationswege nutzen.

> Vgl. dazu allgemein die Begründung des Regierungsentwurfs für ein Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt v. 13.08.2008 BT-Drs. 16/10121 S. 28-32 zu §§ 20k und 20l BKAG sowie die Beschlussempfehlung und den Bericht vom 20.06.2017 BT-Drs. 18/12785 S. 48f. zu § 100a StPO

Mit § 15b HSOG ist der hessische Gesetzgeber daher in Anlehnung an § 20l des Bundeskriminalamtgesetzes (im Folgenden: BKAG) in seiner damals geltenden Fassung

> Gesetz v. 25.12.2008 BGBl. I S. 3083 und dazu die Begründung des (hessischen) Gesetzentwurfs v. 30.06.2009 LT-Drs. 18/861 S. 14

schon frühzeitig den Entwicklungen der Informationstechnik gefolgt und hat, ohne gleichzeitig den Zugriff auf weitere inhaltliche Informationen des informationstechnischen Systems zu gestatten, eine laufende Telekommunikationsüberwa-

chung mit technischen Mitteln dort zugelassen, wo dies mit Hilfe der herkömmlichen Überwachungstechnik nicht mehr möglich war.

> Bereits hier ist zu betonen, dass § 15b Abs. 1 HSOG seit jeher „technische Maßnahmen" fordert, die sicherstellen, „dass *ausschließlich* laufende Telekommunikation überwacht und aufgezeichnet wird" (Hervorhebung nur hier). Das schließt, wie die Anlehnung an § 20l BKAG a.F. zeigt, die gänzliche Ausforschung des Zielsystems aus und beschränkt die Überwachung auf „Daten aus einem laufenden Kommunikationsvorgang" (BVerfGE 120, 220, 309); zu dieser bewussten Begrenzung von § 20l BKAG s. die Begründung des Regierungsentwurfs BT-Drs. 16/10121 S. 31 zu § 20l Abs. 2

Vor allem Täter des internationalen Terrorismus sind aufgrund ihrer häufig länderübergreifenden Vernetzung und ihres konspirativen Vorgehens darauf angewiesen, über Mobilfunkgeräte und andere Kommunikationsmittel und -wege zu kommunizieren. Die Quellen-TKÜ kann gerade deshalb von großer Relevanz sein, weil sie eine Überwachung der immer öfter verschlüsselten digitalen Kommunikation ermöglicht. Der Zugriff auf informationstechnische Systeme schließt insoweit eine technisch-sicherheitskritische Lücke.

Für Maßnahmen nach §§ 15b und 15c HSOG muss auf dem Endgerät eine Software installiert werden, die die gespeicherten Daten oder die Kommunikation vor der Verschlüsselung aufzeichnet und gegebenenfalls ausleitet. Die technische Umsetzung der Maßnahmen gestaltet sich dabei äußerst schwierig, da direkt auf das zu überwachende Endgerät zugegriffen werden muss, ohne dass der Nutzer Kenntnis davon erlangt. Die Installation der notwendigen Software erfolgt direkt am Endgerät oder wird mittels Fernübertragung aufgespielt. Dafür ist es unabdingbar zu wissen, um was für ein Endgerät es sich handelt, welche Software installiert ist und welche Sicherheitsvorkehrungen (z.B. Virenscanner) benutzt werden. Sind diese Informationen nicht vorhanden, besteht die Gefahr, dass die polizeiliche Maßnahme durch das Endgerät selbst oder durch den Nutzer erkannt, der Erfolg der Maßnahme verhindert und die Tatsache der polizeilichen Beobachtung möglicherweise erstmals offenkundig wird. Die Quellen-TKÜ sowie die Online-Durchsuchung erfordern deshalb ein hohes Maß an Personal

verschiedener Organisationseinheiten sowie eine langwierige, intensive Vorbereitung.

> Einen Überblick über die technischen und praktischen Anforderungen gibt die als **Anlage** beigefügt, von Bund und Ländern vereinbarte Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung (Stand 05. Oktober 2018).

So werden vor dem Hintergrund der technisch überaus komplexen und schwierigen Umsetzung der Maßnahmen und des nicht zu vernachlässigenden Entdeckungsrisikos jeweils vor einem Einsatz insbesondere die Gegebenheiten und die tatsächlichen Erfordernisse einer tiefgreifenden Bewertung und Prüfung unterzogen. Die ohnehin wenigen Produkte des freien Marktes (kommerzielle Produkte) und die Eigenentwicklungen des Bundeskriminalamtes wären beispielsweise nach einer Enttarnung durch das inzwischen IT-technisch versierte polizeiliche Gegenüber nicht mehr in weiteren Ermittlungsverfahren oder für präventive Maßnahmen einsetzbar. Zudem muss jede einzusetzende Software vor der Nutzung den „einheitlichen Gesamtabnahmeprozess (eGAP)" des Bundeskriminalamtes durchlaufen, der sie hinsichtlich der rechtlichen Vorgaben (Datenschutz, IT-Sicherheit und Rechtskonformität) sowie der grundsätzlichen funktionalen Einsatzfähigkeit testet und bewertet

Um im Vorfeld jeder Maßnahme ermitteln zu können, welche Kommunikationsmittel und Kommunikationswege (z.B. Mobilfunk, Festnetz, WLAN) die Zielperson nutzt, ist es in der Regel erforderlich, zuerst polizeiliche Maßnahmen gemäß § 15a HSOG (klassische TKÜ-Maßnahmen, WLAN-Aufklärungsmaßnahmen) durchzuführen, auszuwerten und den Datenstrom zu analysieren. Sämtliche für die Zielperson zugänglichen WLAN-Router müssen ausgewertet und die MAC-Adressen und IPs der Nutzer zugeordnet werden. Nur so ist es möglich, die eingesetzten Kommunikationsmittel zu bestimmen und die für die weiteren Maßnahmen erforderlichen systemtechnischen Hard- und Softwareinformationen zu erhalten. Auswertung und Analyse dieser Vorbereitungsmaßnahmen können bis zur eigentlichen technischen Umsetzung der Quellen-TKÜ und Online-Durchsuchung mehrere Wochen in Anspruch nehmen. Anschließend muss eine

Debug-Umgebung mit den gleichen Hard- und Softwareparametern aufgebaut werden, um die einzusetzende Software unter möglichst realen Bedingungen zu testen.

Werden zwischenzeitlich die Kommunikationsmittel gewechselt oder wird das Kommunikationsverhalten verändert, werden die bis dahin durchgeführten polizeilichen Ermittlungen, Vorbereitungsmaßnahmen und die aus der technischen Analyse gewonnenen Informationen gegenstandslos und müssen erneut erhoben werden. Auch wenn eine Maßnahme richterlich genehmigt ist, ist nicht gewährleistet, dass die Software erfolgreich auf dem Endgerät eingebracht werden kann. So hatte das Polizeipräsidium Westhessen im Jahre 2018 zwar einen Beschluss zur Umsetzung einer Quellen-TKÜ aufgrund von § 100a StPO erwirkt und wegen fehlender Personalressourcen das Bundeskriminalamt zur Durchführung der Maßnahme um Amtshilfe ersucht. Sie blieb jedoch erfolgslos, da es nicht gelang, die Software auf dem zu überwachenden Endgerät zu installieren.

Aufgrund ihrer hohen rechtlichen und technischen Hürden und wegen der Vorrangigkeit vergleichbarer repressiver Maßnahmen aufgrund der Strafprozessordnung sind die präventive Quellen-TKÜ und die Online-Durchsuchung in Hessen bislang noch nicht zur Anwendung gekommen. Das Land hat bisher auch davon abgesehen, die erforderliche Software zu entwickeln oder zu erwerben.

> Für den Bund sind die entsprechenden Fallzahlen zumindest nicht öffentlich zugänglich, vgl. dazu grundsätzlich die Antwort der Bundesregierung v. 21.06.2018 BT-Drs. 19/2907 S. 3f. zu Fragen 1.-3. sowie die durchgängig abschlägigen Antworten z.B. v. 24.05. 2018 BT-Drs. 19/2306 S. 3 zu Fragen 1.-4., v. 16.08.2019 BT-Drs. 19/12465 S. 18 zu Frage 11., v. 23.08.2019 BT-Drs. 19/12636 S. 3 zu Frage 2.b., v. 06.02.2020 BT-Drs. 19/17055 S. 14f. zu Fragen 7. und 8., v. 22.06.2020 BT-Drs. 19/20245 S. 5 und 6 zu Fragen 1.-11.
> Nach eigenen Angaben hat das BKA in eigener Zuständigkeit im Zeitraum vom 25.05.2018 bis zum 30.04.2019 „sieben Anschlüsse/Kennungen/Benutzerkonten" aufgrund von § 51 BKAG (Quellen-TKÜ) überwacht, Maßnahmen nach § 49 BKAG (Online-Durchsuchung) dagegen nicht durchgeführt (Bericht des BKA aufgrund von § 88 BKAG BT-Drs. 19/15570 S. 4). Die aktuelle Übersicht des Bundesamtes für Justiz über Maßnahmen nach § 110a StPO für das Jahr 2018 ist im vorliegenden Zusammenhang wenig aussagekräftig, da sie den Sonderfall des Eingriffs mit

technischen Mitteln (§ 100a Abs. 1 Satz 2 StPO) nicht eigens und Maßnahmen nach § 100b StPO gar nicht berücksichtigt.

II.

1. Die Beschwerdeführer zu 1. und 2. sind in beträchtlichem Umfang für die Piratenpartei Deutschland politisch aktiv, unterhalten - so der Beschwerdeführer zu 2. - in diesem Rahmen auch intensive Beziehungen ins Ausland, kommunizieren hierbei und privat mit eigener Hardware über das Internet und betreiben oder administrieren unterschiedliche Internetauftritte. Der Beschwerdeführer zu 3. ist der Gebietsverband der Piratenpartei Deutschland auf Landesebene in Hessen. Wie er gleichfalls eingehend darlegt, bedient er sich bei seiner politischen Arbeit in großem Umfang der Kommunikation im Internet, unterhält eine eigene Domain und betreibt unterschiedliche Internetforen, die zum Teil seinen Mitgliedern, im Übrigen aber auch der Öffentlichkeit zur Verfügung stehen. Dabei sind die von ihm genutzten Programme bei nahezu vollständigem Fehlen eigener Hardware auf Servern eines Hosting-Unternehmens installiert; wegen der Einzelheiten mag auf BS S. 12-17 verwiesen werden.

2. In der Annahme, es sei „die Befugnis der Polizeibehörden, verdeckte Eingriffe in informationstechnische Systeme zum Zweck der Telekommunikationsüberwachung vorzunehmen (Quellen-TKÜ), erheblich ausgeweitet worden", und unter Hinweis auf die erstmalige Zulassung von Online-Durchsuchungen durch § 15c HSOG geht es den Beschwerdeführern um eine „Nachschärfung der verfassungsrechtlichen Maßstäbe für die Durchführung verdeckter Eingriffe in informationstechnische Systeme" (BS S. 4): Der Gesetzgeber müsse „jedenfalls grundlegende Fragen des Umgangs mit digitalen Schwachstellen selbst regeln, wenn er Stellen der Exekutive zur heimlichen Infiltration informationstechnischer Systeme ermächtigt", und habe zudem „eine wirksame Kontrolle der grundrechts- und sicherheitsrelevanten Eigenschaften des ‚Hessentrojaners' gesetzlich sicherzustellen" (BS S. 5).

Allgemein beanstanden sie eine strukturelle Schwächung der IT-Sicherheit, die mit den Eingriffsbefugnissen nach §§ 15b und 15c HSOG verbunden sei (BS S. 17), und halten dem Gesetzgeber insoweit ein „unechtes Unterlassen" (BS S. 32, 40) vor. Da sie sich gegen informationstechnische Maßnahmen aufgrund ihrer Heimlichkeit nicht zur Wehr setzen könnten und die ohnehin lückenhafte Pflicht zur nachträglichen Benachrichtigung (§ 29 HSOG) keinen hinreichenden Ausgleich biete, sehen sie sich unmittelbar, darüber hinaus auch selbst und gegenwärtig betroffen. So sei es für sie angesichts der Intensität ihrer Internetkommunikation mit bekannten wie mit unbekannten Personen und aufgrund der Streubreite der zugelassenen informationstechnischen Eingriffe hinreichend wahrscheinlich, von ihnen erfasst zu werden, ohne selbst zu den Zielpersonen zu zählen (BS S. 35-38). Im Fall des Beschwerdeführers zu 2. komme hinzu, dass er befürchten müsse, wie schon in der Vergangenheit (dazu BS S. 13-14) das Interesse von Geheimdiensten auf sich zu ziehen und zum Zielobjekt ihrer Überwachungsaktivitäten zu werden. Der Beschwerdeführer zu 3. sei zudem deshalb selbst und gegenwärtig betroffen, weil er befürchtet, Dritte könnten die von ihm genutzten Systeme heimlich infiltrieren und für die Verarbeitung von Informationen etwa im Zusammenhang mit Anschlagsplanungen oder einem Cyberangriff auf Infrastruktureinrichtungen missbrauchen.

„Bei der gebotenen Gesamtbetrachtung der von dem hessischen Gesetzgeber getroffenen Regelung" gefährde sie die Vertraulichkeit und Integrität der von den Beschwerdeführern genutzten informationstechnischen Systeme, und zwar „insbesondere hinsichtlich eines Schwachstellenmanagements, aber auch näherer Anforderungen an die Herkunft, Beschaffenheit, Funktionsweise und Anwendungskontrolle der zur Infiltration der Zielsysteme einzusetzenden technischen Mittel" (BS S. 30). Hierzu verweisen sie auf die Implikationen, die mit der Beschaffung und Nutzung von eingriffstauglicher Schadsoftware verbunden seien: Deren Einsatz setze in den Zielsystemen Schwachstellen voraus, die gefunden und, um sie für Ermittlungszwecke nutzen zu können, offengehalten werden müssten. Auf welchem Wege sich die Polizeibehörden die Kenntnis solcher Schwachstellen verschaffen dürfen, habe der Gesetzgeber indessen ebenso wenig geregelt wie den Umgang mit ihnen.

Abgesehen davon auch, dass vielfach die aus dem Einsatz von Schadsoftware folgenden Probleme für die Sicherheit der betroffenen Systeme nicht einzuschätzen seien, habe der Gesetzgeber es unterlassen, den mit deren Identifizierung und Nutzung verbundenen Zielkonflikt zu bewältigen. Die Beschwerdeführer erblicken ihn namentlich darin, dass es im Interesse der Behörden selbst, aber auch der Betreiber kritischer Infrastrukturen, der Wirtschaft, der Software- und der Hardwareanbieter liege, erkannte Schwachstellen so schnell wie möglich zu schließen, während die Sicherheitsbehörden ihre präventiven und repressiven Befugnisse nur unter Offenhaltung solcher Sicherheitslücken nutzen könnten.

Zur Begründung ihrer Verfassungsbeschwerde kommen die Beschwerdeführer auf ihre Beschreibung dieses Zielkonflikts und die Notwendigkeit seiner Auflösung zurück. Unter Berufung auf das Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 (BVerfGE 120, 274) verweisen sie auf das Interesse der Behörden, von ihnen benutzte Schwachstellen offen zu halten, auf der einen Seite und demgegenüber auf die Notwendigkeit, die Sicherheit informationstechnischer Systeme zu gewährleisten, sowie auf das Vertrauen der Bevölkerung darauf, dass sich der Staat eben darum auch bemühe. Wenn der Gesetzgeber dennoch verdeckte Eingriffe in diese Systeme gestatte, sei es seine Aufgabe, im Sinne einer für die Grundrechtsverwirklichung wesentlichen Entscheidung auch für die Auflösung dieser Konflikte Sorge zu tragen, ohne derartige Entscheidungen der Exekutive zu überlassen. Die zwingend gebotenen Regelungen habe er jedoch nicht getroffen und damit nicht nur den objektiven Schutzgehalt des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme missachtet. Vielmehr habe er zugleich diejenige den Beschwerdeführern gegenüber bestehende Schutzpflicht verletzt, die aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hergeleitet werden müsse, zumal ihnen ihrerseits ein zuverlässiger Eigenschutz vor Eingriffen des Staates und beliebiger Dritter nicht möglich sei. In welcher Weise der Landesgesetzgeber diese Regelungslücke schließe, bleibe ihm überlassen. Unabhängig davon begründe sein Versäumnis jedenfalls die Nichtigkeit der Eingriffsermächtigungen.

Verfassungswidrig seien diese aber auch deshalb, weil die Eingriffe nicht auf unvermeidbare und unverhältnismäßige Beeinträchtigungen beschränkt blieben. Je nach eingesetzter Infiltrationstechnik könnten sie vielmehr Folgeschäden an den betroffenen Systemen verursachen, die auch durch die begrenzenden Bestimmungen des § 15b Abs. 2 und § 15c Abs. 3 Satz 1 HSOG nicht verhindert würden. Die Veränderungen, die an dem Zielsystem vorgenommen werden dürfen, müssten zwar für die Datenerhebung unerlässlich sein, müssten, soweit technisch möglich, nach Beendigung der Maßnahme automatisiert auch wieder rückgängig gemacht werden, das für den Eingriff genutzte Mittel müsse nach dem Stand der Technik ferner gegen unbefugte Nutzung, kopierte Daten müssten gegen Veränderungen und unbefugte Kenntnisnahme oder Löschung geschützt werden. Es fehle indessen ein Regelwerk, das die hier vorausgesetzten technischen Standards konkretisiere. Dieser Mangel habe zur Folge, dass nicht nur die gesetzlichen Vorgaben nicht vollziehbar, sondern auch gerichtliche Kontrollen unmöglich seien. Angesichts der großen Streubreite der Beeinträchtigungen, die die Nutzung fehlerhafter oder ungeschützter Software zur Folge haben könne, seien die Beschwerdeführer auch insoweit in ihrem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verletzt.

Im Wesentlichen mit dieser Begründung beantragen sie zu erkennen:

> § 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 25.06.2018, GVBl. Nr. 13 vom 03.07.2018, S. 302, sind nichtig.

III.

Die Verfassungsbeschwerde wird keinen Erfolg haben können.

Es erscheint bereits zweifelhaft, zumindest aber klärungsbedürftig, ob es den Beschwerdeführern im Hinblick auf die Subsidiarität der Verfassungsbeschwerde nicht zuzumuten war und ist, anstelle des Bundesverfassungsgerichts zunächst die Verwaltungsgerichte anzurufen, um dort die von ihnen angenommene Unzulässigkeit der beanstandeten Eingriffe mit einer vorbeugenden Unterlassungsklage geltend zu machen (dazu unter 1.). Jedenfalls dürfte die Verfassungsbeschwerde insoweit wegen Verfristung unzulässig sein, als sie dem hessischen Gesetzgeber die Vernachlässigung grundrechtlicher Schutzpflichten im Zusammenhang mit der Zulassung der Quellen-TKÜ durch § 15b HSOG vorwirft. Diese Maßnahme ist bereits durch das Gesetz vom 14. Dezember 2009 zugelassen worden, so dass die seither laufende Jahresfrist des § 93 Abs. 3 BVerfGG versäumt ist (dazu unter 2.). Die Behauptung gesetzgeberischer Versäumnisse als Grund für die Verfassungswidrigkeit der beiden angegriffenen Vorschriften hätte angesichts der vom Bundesverfassungsgericht grundsätzlich bestätigten Zulässigkeit heimlicher Eingriffe in informationstechnische Systeme schließlich die substantiierte Auseinandersetzung mit der Rechtsprechung des Bundesverfassungsgerichts, mit den Ausprägungen des Verhältnismäßigkeitsgebotes in § 4 Abs. 2 und 3 HSOG, mit der Sicherstellungspflicht nach § 15b Abs. 2 und § 15c Abs. 3 Satz 1 HSOG und mit dem bereits vorhandenen informationstechnischen Regelwerk erwarten lassen. Abgesehen davon, dass der Vortrag der Beschwerdeführer insoweit nicht den Begründungsanforderungen der §§ 92 und 23 Abs., 1 Satz 2 BVerfGG für eine Verfassungsbeschwerde entspricht, erweist sie sie sich aber auch in der Sache als unbegründet (dazu unter 3.)

Dabei mag davon ausgegangen werden, dass die Verfassungsbeschwerde vom 3. Juli 2019 gegen die §§ 15b und 15c HSOG jedenfalls die mit dem Inkrafttreten des angegriffenen Gesetzes am 4. Juli 2018 ausgelöste Jahresfrist des § 93 Abs. 3 BVerfGG gewahrt hat und deshalb spätestens am Tage ihrer Fertigstellung am Mittwoch, dem 3. Juli 2019, bei dem Bundesverfassungsgericht eingegangen ist.

> Zur Fristberechnung s. etwa BVerfGE 18, 1, 11; 102, 254, 295; Beschl. v. 10.04.2007 2 BvR 2228/05 juris Rdn. 2, v. 03.05.2007 1 BvR 1847/05 juris Rdn. 2-3 und v. 06.05.2009 1 BvR 3153/07 juris Rdn. 8-10

Ob das der Fall war, kann hier nicht beurteilt, soll aber angenommen werden.

Die Beschwerdebefugnis der Beschwerdeführer ergibt sich aus ihrer Rüge, der Landesgesetzgeber habe es unterlassen, die Eingriffsermächtigungen der §§ 15b und 15c HSOG mit einem flankierenden insbesondere technischen Regelwerk über den Umgang mit Sicherheitslücken und über die Normierung der für die Eingriffe benutzten Software auszustatten. Damit behaupten sie die Verletzung ihres Grundrechts auf Gewährleistung und Vertraulichkeit informationstechnisches Systeme insoweit, als es sie als Ausprägung des allgemeinen Persönlichkeitsrechts vor dem verfassungsrechtlich nicht legitimierten staatlichen Zugriff auf die von ihnen genutzten informationstechnischen Systeme

BVerfGE 120, 274, 302, 313-315; 141, 220, 304 Rdn. 210

und zugleich die Integrität des Systems vor Schäden schützt, die außer Verhältnis zu den mit dem Eingriff verfolgten Zwecken stehen.

BVerfGE 120, 274, 325f.

Mit dem weiteren Hinweis, der Gesetzgeber habe pflichtwidrig keine Regelungen über die Beschaffung der Infiltrationssoftware getroffen, lässt sich die Beschwerdebefugnis dagegen nicht begründen. Für das Gefährdungspotential, zu dessen expliziter Minimierung der Gesetzgeber verpflichtet sein soll, rührt nicht aus der Herkunft, sondern aus der Beschaffenheit der Infiltrationssoftware. Sie könnte nur wegen ihrer Unzulänglichkeit die Integrität betroffener Systeme und damit die Grundrechte der Beschwerdeführer berühren, und derartigen Schäden haben die Behörden vor dem Einsatz durch eine umfassende Prüfung vorzubeugen. Nicht der Beschaffungsvorgang, sondern ein Einsatz nach unzulänglicher Prüfung kann daher grundrechtsrelevant sein.

Die gegenwärtige und unmittelbare Selbstbetroffenheit der Beschwerdeführer folgt aus der Heimlichkeit des informationstechnischen Eingriffs, von dem sie voraussetzungsgemäß zunächst keine Kenntnis erhalten und gegen den sie sich daher nicht vorbeugend zur Wehr setzen können.

dazu etwa BVerfGE 133, 277, 311f. Rdn. 83-84 m.w.Hinw.; 141, 220, 261 Rdn. 82; 150, 309, 324 Rdn. 35; Senatsbeschl. v. 27.05.2020 1 BvR 1873/13, 1 BvR 2618/13 juris Rdn. 73-75

sowie aus der nicht näher quantifizierbaren Aussicht, bereits durch den bloßen elektronischen Kontakt mit potentiellen polizeilichen Zielpersonen von einem ungeregelten Umgang mit Sicherheitslücken und von Schäden durch die Infiltrationssoftware betroffen zu werden. Die entsprechende für die Beschwerdebefugnis hinreichende Wahrscheinlichkeit ergibt sich hinlänglich aus der praktisch-politischen Tätigkeit der Beschwerdeführer,

vgl. nur BVerfGE 141, 220, 262 Rdn. 83-84 und allgemeiner bereits BVerfGE 133, 277, 312f. Rdn. 86-87

und zwar unabhängig davon, ob sie hierbei eigene oder, wie der Beschwerdeführer zu 3., fremde Endgeräte einsetzen.

BVerfGE 141, 220, 304 Rdn. 210

Als Gebietsverband einer politischen Partei dürfte dessen Beschwerdefähigkeit außer Frage stehen.

So für die Zulässigkeit der Verfassungsbeschwerde des Kreisverbandes einer politischen Partei BVerfG, Beschl. v. 11.07.2014 2 BvR 1006/14 juris Rdn. 8 und für die Beteiligtenfähigkeit i.S.v. § 61 Nr. 2 VwGO BVerwG, Beschl. v. 10.08.2010 6 B 16/10 juris Rdn. 6 und Urt. v. 28.11.2018 6 C 2/17 juris Rdn. 12-19

1. Die Verfassungsbeschwerde könnte jedoch aus Subsidiaritätsgründen unzulässig sein, weil die Beschwerdeführer vor der Anrufung des Bundesverfassungsgerichts nicht den fachgerichtlichen Rechtsweg beschritten haben. Wie nicht auszuschließen ist, dürfte es ihnen möglich und zumutbar sein, mit der nunmehr vorgetragenen Begründung die Verwaltungsgerichte anzurufen. Dort hätten sie eine vorbeugende Unterlassungsklage erheben können mit dem Antrag, das Land zu verurteilen, solche auf §§ 15b und 15c HSOG gestützte Eingriffe zu unterlassen, von denen sie betroffen würden oder betroffen werden könnten.

Aus der Subsidiarität der Verfassungsbeschwerde folgt grundsätzlich die Obliegenheit eines Beschwerdeführers, vor der Anrufung des Bundesverfassungsgerichts sämtliche ihm zur Verfügung stehenden prozessualen Möglichkeiten zu nutzen, um eine Grundrechtsverletzung zu verhindern oder zu beheben. Eine Verfassungsbeschwerde ist daher unzulässig, wenn er sich in zumutbarer Weise um fachgerichtlichen Rechtsschutz hätten bemühen können. Dieser Grundsatz gilt mit seinen noch zu behandelnden Einschränkungen auch für die unmittelbar gegen ein Gesetz gerichtete Verfassungsbeschwerde.

> st. Rspr., zuletzt etwa BVerfGE 120, 274, 300; 123, 148, 172f.; 138, 261, 271f. Rdn. 21-24; 143, 246, 321f. Rdn. 208-211; 150, 309, 326f. Rdn. 41-51

a) Die Beschwerdeführer bezweifeln die Zulässigkeit weder der Quellen-TKÜ noch der Online-Durchsuchung, halten die §§ 15b und 15c HSOG aber deshalb für verfassungswidrig, weil der Landesgesetzgeber es versäumt habe, diese Eingriffsermächtigungen um ein Regelwerk zu vervollständigen, das den Polizeibehörden verbindliche Vorgaben insbesondere für die Beschaffung und Qualität der für ihre Eingriffe erforderlichen Software sowie für den Umgang mit den für die Eingriffe genutzten Sicherheitslücken macht. Für sie stellen sich die Befugnisnormen auf der einen und die vermissten Begleitregelungen auf der anderen Seite als ein einheitlicher Normenkomplex dar, den der Gesetzgeber, wenn er schon Eingriffe in informationstechnische Systeme gestatte, durch ein insbesondere technisches Regelwerk vollständig auszugestalten habe. Sie rügen also nicht ein eigenständiges gesetzgeberisches Unterlassen, das die Geltung der Eingriffsbefugnisse möglicherweise unberührt ließe, sondern sehen deren Verfassungsmäßigkeit in Abhängigkeit von einem hier kurzerhand als technisch bezeichneten flankierenden und vom Gesetzgeber geschuldeten umfassenden, die Eingriffe in informationstechnische Systeme gleichsam kodifizierenden Normenkomplex. Gerade und allein wegen seiner Unvollständigkeit verletze es ihr Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme und habe deshalb die Verfassungswidrigkeit und Nichtigkeit der davon umfassten Eingriffsermächtigungen zur Folge.

Es erscheint nicht ausgeschlossen, dass sie mit dieser Begründung eine vorbeugende Unterlassungsklage gegen das Land erheben könnten, um Maßnahmen zu verhindern, die gegen sie gerichtet sind oder von denen sie unvermeidbar betroffen werden könnten.

b) Eine solche Klage wäre statthaft. Sie setzt „ein besonderes schützenswertes Interesse gerade an der Inanspruchnahme vorbeugenden Rechtsschutzes" voraus, das das Bundesverwaltungsgericht dann annimmt, wenn „der Verweis auf den nachrangigen Rechtsschutz - einschließlich des einstweiligen Rechtsschutzes - mit für den Kläger unzumutbaren Nachteilen verbunden wäre".

> BVerwG, Urt. v. 22.10.2014 6 C 7/13 juris Rdn. 17 m.w. Nachw., v. 13.12.2017 6 A 6/16 juris Rdn. 15 und 6 A 7/16 juris Rdn. 17

Für die Beschwerdeführer ergibt sich dieses Interesse zwanglos aus der unerkennbaren Heimlichkeit der Maßnahmen unabhängig davon, ob sie nach deren Abschluss möglicherweise benachrichtigt werden und deren Unzulässigkeit anschließend feststellen lassen könnten,

> In diesem Sinne allgemein BVerwG, Urt. v. 22.10.2014 6 C 7/13 juris Rdn. 18 und v. 13.12.2017 6 A 6/16 und 6 A 7/16, jeweils juris Rdn. 16

und zwar schon deshalb, weil die Kontrolle bereits durchgeführter Maßnahmen sie vor solchen künftigen Eingriffen nicht schützen kann, denen es, wie die Beschwerdeführer meinen, an einer verfassungskonformen Rechtsgrundlage fehlt und die deshalb schlechthin zu unterbleiben haben.

Freilich macht das Bundesverwaltungsgericht - ersichtlich mit dem Ziel, den zulässigen Individualrechtsschutz gegen eine unzulässige abstrakte Normenkontrolle abzugrenzen - in zwei jüngeren Entscheidungen die Statthaftigkeit davon abhängig, ob das Handeln, das mit der vorbeugenden Unterlassungsklage abgewehrt werden soll, sich auch „hinreichend konkret abzeichnet, insbesondere die für eine Rechtmäßigkeitsprüfung erforderliche Bestimmtheit aufweist".

> Urt. v. 13.12.2017 6 A 6/16 und 6 A 17/16, jeweils juris Rdn. 12

Daran dürfte es im Fall der Beschwerdeführer nicht fehlen.

Die gegenständliche Bestimmtheit der abzuwehrenden Maßnahmen ergibt sich ohne weiteres aus dem Gesetz; das mit §§ 15b und 15c HSOG die polizeilichen Zugriffe beschreibt, die die Beschwerdeführer für verfassungswidrig halten. Dass sie nicht angeben können, wann in ihrem Fall mit solchen Maßnahmen zu rechnen ist, sich das polizeiliche Handeln also nicht „hinreichend konkret abzeichnet", liegt in der Natur der Sache. Wirksam sind die informationstechnischen Eingriffe nur, wen sie die Zielperson überraschen, sich also gerade nicht abzeichnen. Darüber hinaus müsste ein Kläger, um der Forderung des Bundesverwaltungsgerichts gerecht zu werden, zumindest vortragen, dass er als Zielperson Gegenstand polizeilichen Interesses geworden ist, weil die Voraussetzungen präventiver Maßnahmen aus polizeilicher Sicht in seiner Person erfüllt sein können. Zur vorsorglichen Abwehr der Quellen-TKÜ hätte ein Kläger also anzugeben, dass er nicht nur zu dem in § 15b Abs. 1 i. V. m. § 15a Abs. 1 Satz 2 HSOG aufgeführten Personenkreis gehört, sondern der Eingriff auch zum Schutz der in § 15a Abs. 1 Satz 1 HSOG genannten Rechtsgüter unerlässlich sein könnte. Die Online-Durchsuchung ließe sich gleichfalls nur mit eben dieser Behauptung verhindern (§ 15c Abs. 1 HSOG), die nach Maßgabe der Anforderungen aus § 15c Abs. 2 Satz 1 bis 3 HSOG noch ergänzt werden müsste. Eine derartige Klagebegründung wäre indessen den Beschwerdeführern schwerlich zuzumuten.

vgl. BVerfGE 125, 260, 305; 130, 151, 176f.

Zwar könnten sie sich stattdessen darauf berufen, dass Eingriffe in informationstechnische Systeme auch zulässig sind und mit ihnen deshalb gerechnet werden muss, wenn andere Personen und deshalb möglicherweise auch sie unvermeidbar betroffen werden (§ 15b Abs. 1 i. V. m. § 15a Abs. 1 Satz 3 und § 15c Abs. 2 Satz 4 HSOG). Selbst damit wäre indessen nicht zu belegen, dass die abzuwehrende Maßnahme sich „hinreichend konkret abzeichnet". Sollten die Verwaltungsgerichte dennoch an diesem Statthaftigkeitserfordernis festhalten, erwiese sich die grundsätzliche Zulässigkeit der vorbeugenden Unterlassungsklage - vermutlich entgegen der Rechtsschutzgewährleistung durch Art. 19 Abs. 4 GG - zumindest dann als weitgehend gegenstandslos, wenn sie gegen Eingriffe der hier behandel-

ten Art gerichtet ist. Vorzugswürdig erscheint es daher, dass das Bundesverwaltungsgericht im Fall der automatischen Kennzeichenerfassung allein die „bloße Eventualität" eines behördlichen Handelns, „dem nur bei künftigem Hinzutreten außergewöhnlicher Umstände Eingriffsqualität gegenüber dem Anspruchsteller zuwüchse", als Anspruchsvoraussetzung nicht genügen lassen.

Urt. v. 22.10.2014 6 C 7/13 juris Rdn. 31

Die Rechtsprechung wird deshalb diese „bloße Eventualität" eines Eingriffs für den Fall des polizeilichen Eindringens in informationstechnische Systeme noch zu konturieren haben. Dass sie im Fall der Beschwerdeführer angesichts ihrer über den privaten Bereich deutlich hinausgehenden politischen Aktivitäten auch ohne das „Hinzutreten außergewöhnlicher Umstände" überschritten und deren vorbeugende Unterlassungsklage deshalb statthaft sein könnte, ist zumindest nicht von der Hand zu weisen. Vielmehr schließt deren politische Betätigung die konkreter nicht einschätzbare Möglichkeit von elektronischen, durch polizeiliche Eingriffe betroffenen Kontakten mit potentiellen Zielpersonen ein.

vgl. nur BVerfGE 133, 277, 313 Rdn. 87; 141, 20, 262 Rdn. 84

Der Umstand, dass es in Hessen bislang zu derartigen Maßnahmen nicht gekommen ist, dürfte dagegen keine Rolle spielen. Vielmehr wird berücksichtigt werden müssen, dass das Bundesverfassungsgericht die unmittelbare und gegenwärtige Selbstbetroffenheit als Zulässigkeitsvoraussetzung der Verfassungsbeschwerde gegen eine Norm bereits dann anzunehmen pflegt, wenn der Beschwerdeführer keine Kenntnis von dem darauf gestützten Vollzugsakt erhält, von diesem aber wegen dessen großer Streubreite mit einiger Wahrscheinlichkeit berührt wird und in der polizeilichen Praxis von einer nachträglichen Benachrichtigung aufgrund weitreichender Ausnahmetatbestände auch langfristig abgesehen werden kann.

BVerfGE 130, 151, 176; 133, 277, 312f. Rdn. 86-87; vgl. ähnlich auch BVerfGE 141, 220, 261f. Rdn. 82-84; 150, 309, 324 Rdn. 35; Senatsbeschl. v.. 27.05.2020 1 BvR 1873/13, 1 BvR 2618/13 juris Rdn. 73-75

Die Anforderungen an die Statthaftigkeit einer vorbeugenden Unterlassungsklage gegen einen befürchteten Normvollzug dürften indes unter dem Gesichtspunkt der sachgerechten Funktionsabgrenzung zwischen Fach- und Verfassungsgerichtsbarkeit schwerlich anspruchsvoller sein als der Betroffenheitsmaßstab einer gegen dieselbe Norm gerichteten Verfassungsbeschwerde.

Das gleichfalls notwendige besondere schützenswerte Interesse der Beschwerdeführer an der Gewährung vorbeugenden Rechtsschutzes ergibt sich daraus, dass ihnen der nachträgliche Rechtsschutz, auf den sie stattdessen verwiesen wären, nicht zugemutet werden kann.

> Vgl. BVerwG, Urt. v. 13.12.2017 6 A 6/16 und 6 A 7/16, jeweils juris Rdn. 15-16

Die Möglichkeit der nachträglichen Feststellungsklage könnte dem Aufklärungs- und Rehabilitierungsbedarf Betroffener schon deshalb nicht genügen, weil eine Benachrichtigung keinesfalls gewährleistet werden, sondern entfallen kann, wenn sie die Ermittlung, Aufdeckung und Verfolgung von Straftaten gefährden würde (§ 29 Abs. 1 HSOG i. V. m. § 51 Abs. 2 Nr. 1 Buchst. a) und § 40 Abs. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes [im Folgenden: HDSIG] vom 3. Mai 2018 GVBl. S. 82).

c) Die Klagebefugnis der Beschwerdeführer entfiele nur, wenn deren subjektive Rechte durch die in §§ 15b und 15c HSOG zugelassenen Eingriffe keinesfalls verletzt sein könnten. Das wird sich schwerlich annehmen lassen. Da sowohl die Quellen-TKÜ wie die Online-Durchsuchung selbst dann durchgeführt und die Beschwerdeführer von ihnen berührt werden dürfen, wenn sie zwar nicht zu deren Zielpersonen gehören, sich die Maßnahmen aber unvermeidbar auf sie auswirken können (§ 15b Abs. 1 i.V.m. § 15a Abs. 1 Satz 3, § 15c Abs. 2 Satz 4 HSOG), lässt sich als Eingriffsfolge deren faktische Betroffenheit in ihrem Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme und darüber hinaus in ihrer durch Art. 10 GG geschützten Kommunikationsfreiheit nicht ausschließen.

Der Erfolg einer vorbeugenden Unterlassungsklage kann somit davon abhängen, ob es den denkbaren, nicht einmal gegen die Beschwerdeführer selbst gerichteten Eingriffen in die informationstechnischen Systeme Dritter aus den von ihnen vorgebrachten Gründen tatsächlich an einer verfassungskonformen Rechtsgrundlage fehlt. Sollten die Fachgerichte sich davon nicht überzeugen können und die Klage deshalb abweisen, wäre gegen die in der Regel letztinstanzliche Entscheidung die Verfassungsbeschwerde zulässig. Andernfalls müssten sie das Verfahren aussetzen und die Verfassungsfrage je nach dem angewendeten Prüfmaßstab zur konkreten Normenkontrolle dem Bundesverfassungsgericht oder dem Hessischen Staatsgerichtshof vorlegen. Zudem käme dann eine einstweilige Anordnung des Verwaltungsgerichts im Sinne des Klagebegehrens in Betracht.

vgl. BVerfGE 145, 20, 55 Rdn. 86

d) Zulässigkeit und Begründetheit eines Rechtsbehelfs sind nach alledem letztlich ungeklärt und deshalb offen. Den fachgerichtlichen Rechtsweg müssen die Beschwerdeführer dennoch beschreiten,

so z.B. BVerfGE 145, 20, 54 Rdn. 85 m.w.Nachw.

nur offensichtlich sinn- und aussichtslose Rechtsbehelfe werden ihnen nicht zugemutet.

BVerfGE 123, 148, 172f. m.w.Nachw.; 138, 261, 271f. Rdn. 23

Für einen absehbar sicheren Misserfolg der hier in Betracht kommenden vorbeugenden Unterlassungsklage gibt der Fall jedoch keine hinreichenden Anhaltspunkte. Aus der zitierten Rechtsprechung des Bundesverwaltungsgerichts lassen sich für die Unzulässigkeit einer vorbeugenden Unterlassungsklage gegen mögliche Eingriffe in informationstechnische Systeme keine unmissverständlichen und vor allem auch den Anforderungen des Art. 19 Abs. 4 GG genügenden Ergebnisse herleiten.

Mit Recht betont BVerfGE120, 274, 300 im Zusammenhang mit der Subsidiarität der Verfassungsbeschwerde, es dürften „im fachgerichtlichen Ver-

> fahren [...] die Anforderungen an das Rechtsschutzinteresse im Sinne eines effektiven Grundrechtsschutzes nicht überspannt werden".

und wenn die Beschwerdeführer mit der dem Bundesverfassungsgericht vorgetragenen Begründung die §§ 15b und 15c HSOG für verfassungswidrig halten, kann es für sie nicht unzumutbar sein, aus denselben Gründen zunächst die Verwaltungsgerichte anzurufen.

e) Freilich kann die unmittelbare Anrufung des Bundesverfassungsgerichts zulässig und die an sich zumutbare Erschöpfung des fachgerichtlichen Rechtswegs entbehrlich sein, wenn ein Fall ausschließlich verfassungsrechtliche Fragen aufwirft, die letztverbindlich ohnehin allein das Bundesverfassungsgericht beantwortet, sofern dieses von einer Klärung der verfassungsrechtlich relevanten Sach- und Rechtsfragen durch die Fachgerichte keine Verbesserung seiner Entscheidungsgrundlagen zu erwarten hat.

> BVerfGE 122, 63, 80f.; 138, 261, 272 Rdn. 23 u. 24; 143, 246, 322 Rdn. 211; 150, 309, 327 Rdn. 44; Senatsbeschl. v. 19.05.2020 1 BvR 2835/17 juris Rdn. 78-79, und v. 27.05.2020 1 BvR 1873/13, 1 BvR 2618/13 juris Rdn. 77-78; Beschl. v. 29.11.2000 1 BvR 630/93 juris Rdn. 25, v. 27.12.2005 1 BvR 1725/05 juris Rdn. 19 und v. 31.02.2006 1 BvR 1184/04 juris Rdn. 64

Unter der Voraussetzung, dass die von den Beschwerdeführern angenommene Regelungslücke den Bestand der angegriffenen Eingriffsermächtigungen überhaupt in Frage zu stellen vermag, dürfte vor allem entscheidend sein, wie das Bundesverfassungsgericht den mit der Verfassungsbeschwerde zur Sprache gebrachten technisch-fachlichen Vorklärungsbedarf bewertet. Dabei geht es nicht um die individuellen Verhältnisse der Beschwerdeführer, deren Klärung den Fachgerichten überlassen werden könnte, sondern im Rahmen der Entscheidungserheblichkeit um die Ermittlung und Bewertung des angeblichen Regelungsdefizits sowie der Notwendigkeit und Möglichkeit seiner Behebung. Dass das Bundesverfassungsgericht auch mit Hilfe sachkundiger Dritter hierzu in der Lage ist, steht indessen außer Frage.

Wenngleich die Verfassungsbeschwerde somit außer verfassungsrechtlichen auch eine Reihe tatsächlicher Probleme aufwirft, kommt die Möglichkeit in Betracht, die Beschwerdeführer nicht zunächst auf den fachgerichtlichen Rechtsweg zu verweisen, sondern ihnen den unmittelbaren Zugang zum Bundesverfassungsgericht zu eröffnen.

2. Soweit die Verfassungsbeschwerde sich gegen § 15b HSOG richtet, ist sie jedoch wegen Versäumung der Beschwerdefrist aus § 93 Abs. 3 BVerfGG unzulässig.

Die hessischen Polizeibehörden sind zur Telekommunikationsüberwachung an informationstechnischen Systemen erstmals durch § 15b des Gesetzes zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze vom 14. Dezember 2009 (GVBl. I S 635) ermächtigt worden, das im Gesetz- und Verordnungsblatt vom 22. Dezember 2009 verkündet worden und nach seinem Art. 8 am folgenden Tage in Kraft getreten ist. Das nunmehr angegriffene Gesetz vom 25. Juni 2018 hat die Eingriffsvoraussetzungen zwar erweitert, hat den tragenden Grund der Verfassungsbeschwerde, die behauptete Verletzung staatlicher Schutzpflichten für die Integrität informationstechnischer Systeme, jedoch nicht berührt. Die ursprüngliche Eingriffsschwelle der „gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person" wurde dahin modifiziert, dass der Eingriff „zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz des Menschen berührt, unerlässlich" sein muss. Ferner hat es den Kreis der in Betracht kommenden Zielpersonen erweitert: Durfte sich die Maßnahme ursprünglich „nur gegen eine Person richten, die nach den §§ 6 oder 7 verantwortlich ist. Sie darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden".

> § 15b Abs. 4 HSOG i.d.F. v. Art. 1 Nr. 8 des Gesetzes v. 14.12.2009 (GVBl. I S. 635), der durch Art. 18 Nr. 9a des Gesetzes v. 03.05.2018 (GVBl. S. 82, 149) ohne inhaltliche Änderung zu § 15b Abs. 3 geworden war.

ist diese Bestimmung nunmehr durch die Bezugnahme auf die ihrerseits neu gefassten „Voraussetzungen des § 15a Abs. 1" ersetzt worden. Damit werden Eingriffe gegen alle Personen zugelassen, die in § 15a Abs. 1 Satz 2 und 3 HSOG auch über den Personenkreis der §§ 6 und 7 HSOG hinaus aufgeführt werden.

Diese Änderungen haben den Anwendungsbereich des Gesetzes in einer Weise ausgedehnt, die über die Vorgängerfassung des § 15b HSOG hinausgeht. Gleichwohl haben sie die Jahresfrist des § 93 Abs. 3 BVerfGG für die vorliegende Verfassungsbeschwerde nicht neu ausgelöst; denn die Beschwerdeführer sehen sich nicht etwa durch die beschriebenen Änderungen oder überhaupt durch die Eingriffsermächtigung des § 15b HSOG, sondern dadurch beschwert, dass es ihr an solchen Bestimmungen fehle, die die in welcher Form auch immer zugelassene Telekommunikationsüberwachung durch Regeln insbesondere über den Umgang mit Sicherheitslücken der angegriffenen Systeme, über die Beschaffung und Beschaffenheit der nötigen Schadsoftware und schließlich über deren Verwendung ergänzen und konkretisieren müsse. In der Sache geht es ihnen damit nicht um die Eingriffsbefugnisse als solche, die sie augenscheinlich hinzunehmen bereit sind. Vielmehr vermissen sie ein eigenständiges gesetzgeberisches Begleitkonzept und rügen nicht eine gänzliche Untätigkeit des Gesetzgebers,

> Dafür müssten sie sich auf einen ausdrücklichen Auftrag des Grundgesetzes berufen, der Inhalt und Umfang der Gesetzgebungspflicht im Wesentlichen umgrenzt (BVerfGE 6, 257, 264; 23, 242, 249; 56, 54, 70f.; 129, 124, 176; 139, 321, 346 Rdn. 82; Beschl. v. 23.08.1999 1 BvR 2164/98 juris Rdn. 11), und einen solchen Verfassungsauftrag behaupten sie nicht einmal. Hat der Gesetzgeber dagegen wie hier eine angeblich unvollständige und allein aus diesem Grund für verfassungswidrig gehaltene Regelung getroffen, muss die Verfassungsbeschwerde die Norm selbst angreifen (BVerfGE 29, 268, 273; 56, 54, 71; Beschl. v. 14.12.2008 2 BvR 2338/07 u.a. juris Rdn. 3, und ähnlich Beschl. v. 02.05.2018 1 BvR 3250/14 juris Rdn. 8).

sondern ausdrücklich nur die Unvollständigkeit seiner Regelungen - wenn er schon Eingriffe in informationstechnische Systeme zulasse und, was sie substantiiert nicht bezweifeln, auch zulassen dürfe, müsse er gleichzeitig auch deren

informationstechnisches Umfeld ordnen. Diesem Regelwerk messen sie im Hinblick auf die staatliche Schutzpflicht für die Vertraulichkeit und Integrität informationstechnischer Systeme derartige Bedeutung bei, dass es wesentlicher Bestandteil der Eingriffsermächtigung selbst sein müsse und diese nur als umfassender Regelungskomplex verfassungsmäßig sein könne.

In der Tat gibt es derartige eigens auf die Quellen-TKÜ und die Online-Durchsuchung bezogene spezialgesetzliche Bestimmungen mit der für erforderlich gehaltenen Regelungstiefe weder in Hessen noch, soweit erkennbar, im Bund oder in anderen Bundesländern. Sollte ihr Fehlen überhaupt eine verfassungsrechtlich relevante Beschwer begründen können, dann wäre sie unabhängig von der Größe des betroffenen Personenkreises und von der Höhe der Eingriffsschwelle umstandslos mit der grundsätzlichen Ermächtigung zur Telekommunikationsüberwachung verbunden. In Hessen bestünde sie deshalb seit dem Jahre 2009. Bereits in seinem Urteil vom 27. Februar 2008

> BVerfGE 120, 274, 325, 326 im Anschluss an Hansen/Pfitzmann, Online-Durchsuchung, DRiZ 2007, 225, 228

hat das Bundesverfassungsgericht darauf hingewiesen, dass schon der bloße Zugriff auf einen Rechner dort Schäden verursachen könne, und den von den Beschwerdeführern in diesem Zusammenhang ins Feld geführten „Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme" angesprochen. Bedürfte es, um ihn aufzulösen, besonderer Regeln, hätte das Gericht sie fraglos auch gefordert. Daher konnte der Landesgesetzgeber bei der erstmaligen Zulassung der Online-TKÜ durch § 15b HSOG ohne weiteres an jene Entscheidung anknüpfen,

> so die Begründung v. 30.06.2009 zu § 15b des Gesetzentwurfs LT-Drs. 18/861 S. 14

ohne die damit verbundenen im weiteren Sinne technischen Fragen auch nur ansprechen zu müssen. An der Qualität dieses in der Verfassungsbeschwerde zutreffend so bezeichneten „unechten Unterlassens" hat sich im Zusammenhang

mit § 15b HSOG bis heute nichts geändert. Vielmehr hätte der Gesetzgeber die dort vermisste Regelung, um ihren verfassungsrechtlichen Ansprüchen zu genügen, bereits im Jahre 2009 treffen müssen. Damit ist die Beschwerdefrist

> zu ihrer Geltung in Fällen, in denen nicht ein gänzliches Unterlassen des Gesetzgebers, sondern die Unvollständigkeit seiner Regelung gerügt wird, s. BVerfGE 13, 284, 287; 56, 54, 71; Beschl. v. 25.08.1998 1 BvR 2487/94 juris Rdn. 4 und v. 04.12.1998 2 BvR 2126/96 juris Rdn. 15

für den Angriff auf § 15b HSOG seit langem abgelaufen und nicht etwa von den Änderungen des Gesetzes vom 25. Juni 2018 neu ausgelöst worden.

Sie kann insbesondere nicht deshalb neu begonnen haben, weil der Gesetzgeber die Zulässigkeit der Quellen-TKÜ bei Gelegenheit der Novellierung des hessischen Polizeirechts gebilligt, sie damit in seinen Willen aufgenommen

> Diesen Gesichtspunkt lässt das Bundesverfassungsgericht in ständiger Rechtsprechung grundsätzlich nicht gelten, vgl. nur BVerfGE 11, 255, 259f.; 17, 364, 369; 18, 1, 9; 43, 108, 116; 80, 137, 129, 208, 234; 149; 122, 63, 74; 129, 208, 234.

und zugleich an deren angeblicher Lückenhaftigkeit festgehalten haben mag. Die in der Rechtsprechung anzutreffenden Umstände, die die Frist für eine Verfassungsbeschwerde gegen älteres Recht neu auszulösen vermögen, erfassen die hier vorliegende Fallgestaltung nicht: Wenn es danach einer Änderung entweder der verfahrensgegenständlichen Norm selbst bedarf, die ihr - und sei es nur durch ihre Präzisierung -

> BVerfGE 11, 351, 359f.; 74, 69, 73; Beschl. v. 29.11.2000 1 BvR 630/93 juris Rdn 10

einen neuen oder erweiterten Inhalt gibt,

> BVerfGE 43, 108, 116; 122, 63, 74-78; 129, 208, 234

wenn eine Ausdehnung ihres Anwendungsbereichs

> BVerfGE 12, 10, 24, 122, 63, 74

oder ihre mit einem Bedeutungswandel verbundene grundlegenden Umgestaltung gefordert wird,

so z.B. BVerfGE 130, 151, 177

geht es um die prozessuale Bedeutung inhaltlicher Änderungen. Von ihnen ist zwar, wie dargestellt, im Falle von § 15b HSOG auszugehen. Mit deren Inkrafttreten am 4. Juli 2018 hätte die Beschwerdefrist indessen nur beginnen können, wenn die Änderung für die Beschwerdeführer eine neue Beschwer ausgelöst hätte.

zu diesem Erfordernis BVerfGE 11, 255, 259; 17, 364, 369; 78, 350, 356; 79, 1, 14; 122, 63, 78; 120, 274, 298; 141, 220, 263 Rdn. 85; Senatsbeschl. v. 19.05.2020 1 BvR 2835/17 juris Rdn. 83; Beschl. v. 21.03.1994 1 BvR 311/94 juris Rdn. 3, v. 29.11.2000 1 BvR 630/93 juris Rdn. 19, v. 03.01.2002 2 BvR 1827/01 juris Rdn. 2-3, v. 09.09.2003 2 BvR 508/03 juris Rdn. 10,12, und v. 07.10.2009 1 BvR 3479/08 juris Rdn. 9

Nichts Anderes ist gemeint, wenn das Bundesverfassungsgericht die Jahresfrist „prinzipiell nur für die geänderten Vorschriften" beginnen lässt

BVerfGE 129, 208, 234

und den Fristbeginn davon abhängig macht, ob die Änderung für den Beschwerdeführer eine Verschlechterung gegenüber der bisherigen Rechtslage mit sich gebracht

BVerfGE 26, 100, 109; 45, 104, 119f.; Beschl. v. 21.03.1994 1 BvR 311/94 juris Rdn. 3 und v. 04.12.1998 2 BvR 2126/96 juris Rdn. 18

oder eine ihn stärker als bisher belastende Wirkung entfaltet hat.

BVerfGE 78, 350, 356; 100, 313, 356; Beschl. v. 10.09.2009 1 BvR 2054/09 juris Rdn. 11 und v. 27.01.2011 1 BvR 3222/09 juris Rdn. 29

Diese Kriterien zusammenfassend lässt das Gericht die Jahresfrist trotz unveränderten Wortlauts dann neu beginnen, wenn „die Gesetzesänderung die Verfassungswidrigkeit der angegriffenen Norm erst begründet oder verstärkt",

BVerfGE 111, 382, 411; ebenso Beschl. v. 07.10.2009 1 BvR 3479/08 juris Rdn. 8, v. 12.11.2009 2 BvR 2034/04 juris Rdn. 34 und v. 22.02.2017 1 BvR 2875/16 juris Rdn. 7

und hält es für entscheidend, „dass gerade durch diese Änderung die Verfassungswidrigkeit begründet oder erhöht wird".

Beschl. v. 30.07.2003 1 BvR 646/02 juris Rdn. 18

Im Gegenschluss folgt daraus: Greift die Verfassungsbeschwerde die bereits aus der ursprünglichen Norm resultierende und später in ihrer Wirkung unverändert gebliebene Belastung als solche an, lösen nachfolgende Änderungen die Jahresfrist des § 93 Abs. 3 BVerfGG nicht erneut aus.

BVerfGE 80, 137, 149; 122, 63, 78

Für das Bundesverfassungsgericht kann daher selbst eine nach Ablauf der Beschwerdefrist noch intensivierte Beschwer die Frist dann nicht neu in Lauf setzen, „wenn unter Zugrundelegung der Begründung der Verfassungsbeschwerde auch schon die anfänglich geringere Beschwer verfassungswidrig gewesen sein soll" und die angeblich seit jeher verfassungswidrige Norm daher bereits nach ihrem Inkrafttreten hätte angegriffen werden können.

Beschl. v. 03.01.2002 2 BvR 1828/01 juris Rdn. 4, 6-7

So liegt es hier. Die Beschwerdeführer sehen sich, wie bereits betont und woran sie sich festhalten lassen müssen, nicht unmittelbar durch § 15b HSOG, sondern durch das Fehlen eines nach ihrer Ansicht mit der Eingriffsermächtigung notwendig zu verbindenden Begleitgesetzes beschwert, und eben diese Selbsteinschätzung ist der Prüfung ihrer Verfassungsbeschwerde zugrunde zu legen. Für eine so verstandene Beschwer sind die Änderungen von § 15b HSOG durch das Gesetz vom 25. Juni 2018 ohne Bedeutung. Weder haben sie die Beschwer vergrößert noch haben sie die Intensität des behaupteten Verfassungsverstoßes verstärkt. Mit der Begründung ihrer gegenwärtigen Verfassungsbeschwerde hätten sie daher bereits die Einführung von § 15b HSOG durch das Gesetz vom

14. Dezember 2009 angreifen können. Insoweit haben sie demnach die Jahresfrist des § 93 Abs. 3 BVerfGG versäumt.

3. Die Verfassungsbeschwerde wird schließlich auch deshalb erfolglos bleiben müssen, weil sie sich damit begnügt, die Unzulänglichkeit und Ergänzungsbedürftigkeit der hessischen Eingriffsermächtigungen zu behaupten, sich aber nicht substantiiert mit der Rechtsprechung des Bundesverfassungsgerichts und den Regeln auseinandersetzt, die der Entstehung jener angeblichen Defizite entgegenwirken können.

a) In seinen Urteilen vom 27. Februar 2008 und 20. August 2016 hat das Bundesverfassungsgericht die heimliche Infiltration informationstechnischer Systeme im Grundsatz für zulässig erklärt und diese Feststellung mit zahlreichen Einschränkungen für deren Voraussetzungen und Verfahren wie für die Behandlung der dabei gewonnenen Daten verbunden.

> BVerfGE 120, 274 und 141, 220, als strategische Kommunikationsüberwachung bestätigt durch Urt. v. 19.05.2020 1 BvR 2835/17 juris Rdn. 143-144

Im Grundsatz kann damit die Verfassungsmäßigkeit sowohl der Quellen-TKÜ wie der Online-Durchsuchung zu präventiven und repressiven Zwecken als geklärt gelten. Als mögliches Eingriffsobjekt dieser Maßnahmen dort, wo sie vom Schutzbereich anderer Grundrechte wie des Kommunikationsgeheimnisses (Art. 10 GG), der Unverletzlichkeit der Wohnung (Art. 13 GG) und des Grundrechts auf informationelle Selbstbestimmung nicht erfasst werden, und mit dem Ziel ihrer Begrenzung hat das Gericht das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme entwickelt. Es schützt nicht nur die Vertraulichkeit der dort erzeugten, verarbeiteten und gespeicherten Daten, sondern ebenso das Vertrauen des Betroffenen auf die Verfügbarkeit des Systems ausschließlich für berechtigte Nutzer und auf dessen Integrität gegenüber staatlichen Eingriffen.

> BVerfGE 120, 274, 313-315; 141, 220, 304 Rdn. 210

Geltungsgrund dieses aus Art. 2 Abs. 1 auch in Verbindung mit Art. 1 GG abgeleiteten Grundrechts ist die Freiheitssicherung des individuellen Kommunikationsverhaltens, konkretisiert wird es „um der Freiheit des individuellen Kommunikationsverhaltens willen [...] als Schutz wichtiger infrastruktureller Bedingungen moderner Kommunikationstechniken, die Voraussetzung der Ausübung von Kommunikationsfreiheiten sind".

Hoffmann-Riem JZ 2014, 53, 57

Das Eingriffsgewicht sieht das Gericht auch durch die Gefahr geprägt, es könne schon allein der Zugriff auf dem Rechner und in dessen Datenbeständen Schäden verursachen, „die im Zuge der Prüfung der Angemessenheit einer staatlichen Maßnahme mit zu berücksichtigen sind".

BVerfGE 120, 274, 326

Als mögliche Schadensfolgen beschreibt es neben der versehentlichen oder gezielten Löschung, Veränderung oder Anlegung von Datenbeständen die Weiterleitung von Schadprogrammen durch arglose Nutzer und die Offenhaltung, vielleicht auch die Verdeckung der Sicherheitslücken, die die Infiltration des Systems erst ermöglicht haben.

BVerfGE 120, 274, 325f.

Daran anknüpfend verweist das Gericht auf die Verpflichtung - dort in § 20k Abs. 2 BKAG a.F. -, zugriffsbedingte Veränderungen an den betroffenen Systemen auf das unerlässliche Mindestmaß zu beschränken, sie, soweit technisch möglich, automatisiert rückgängig zu machen und die eingesetzte Software gegen unbefugte Nutzung zu schützen. Gleichzeitig schließt es die Möglichkeit von Folgeschäden nicht völlig aus, ohne dass der Eingriff deshalb „von vornherein unverhältnismäßig" wäre.

BVerfGE 141, 220, 305f. Rdn. 215

Gegen die „technikoffene Bestimmung der Überwachungsmittel in § 20g Abs. 2 Nr. 2 und 3 BKAG"

> Gemeint sind (§ 20g Abs. 2 Nr. 2 BKAG) technische „Mittel außerhalb von Wohnungen in einer für den Betroffenen nicht erkennbaren Weise a) zur Anfertigung von Bildaufnahmen oder -aufzeichnungen [...] oder b) zum Abhören oder Aufzeichnen des außerhalb von Wohnungen nicht öffentlich gesprochenen Wortes" und (Nr. 3) „sonstige besondere für Observationszwecke bestimmte technische Mittel zur Erforschung des Sachverhalts oder zur Bestimmung des Aufenthalts einer in Absatz 1 genannten Person".

hatte das Gericht keine Bedenken: „Der Gesetzgeber ist nicht dazu verpflichtet, die erlaubten Mittel für Überwachungen auf den jeweiligen technischen Stand und Zeitpunkt des Gesetzgebungsverfahrens zu begrenzen. Soweit die Art der erlaubten Überwachung aus der Norm hinreichend erkennbar ist, kann er in die Ermächtigung auch künftige technische Entwicklungen einbeziehen [...], die in ihrer Qualität und in Blick auf das Eingriffsgewicht den bereits bekannten Mitteln entsprechen."

BVerfGE 141, 220, 290 Rdn. 161

Den Einwand schließlich, eine Quellen TKÜ lasse sich schlechthin nicht auf die laufende Telekommunikation beschränken, die entsprechende Vorgabe des damaligen § 20l Abs. 2 Nr. 1 BKAG sei deshalb verfassungswidrig, hat das Bundesverfassungsgericht mit der Erwägung zurückgewiesen, er betreffe nur die Anwendung, nicht aber die Gültigkeit der Norm und brauche in dem aktuellen Verfahren daher nicht geklärt zu werden.

BVerfGE 141, 220, 311 Rdn. 234

Für das sachverständig beratene Gericht lagen die technischen Implikationen, die mit der Infiltration informationstechnischer Systeme nach dem aktuellen Stand der Technik unvermeidbar verbunden sind, nach alledem auf der Hand. Dass sie ausgeräumt werden müssten, weil derartige Maßnahmen andernfalls verfassungswidrig wären, wird nicht einmal angedeutet, im Gegenteil bleibt die Möglichkeit außer Betracht, den Gesetzgeber für die Mängelbeseitigung überhaupt in die Pflicht zu nehmen. Das Gericht konstatiert nicht mehr als einen Zielkonflikt zwischen dem im Einzelfall möglicherweise denkbaren staatlichen Interesse am Fortbestand eingriffstauglicher Sicherheitslücken und dem gleichfalls

öffentlichen Interesse an einer möglichst großen Sicherheit informationstechnischer Systeme, entwickelt aber keinen Hinweis darauf, wie er aufgelöst werden könnte.

> BVerfGE 120, 274, 326; zu diesem Konflikt z.B. Derin/Golla NJW 2019, 1111, 1114f., und ähnlich Buermeyer, Stellungnahme v. 29.05.2017 zur Anhörung des Ausschusses für Recht und Verbraucherschutz v. 31.05.2017 S. 21f. (Ausschussdrucksache 18(6)334); Dietrich, Stellungnahme v. 26.01.2020 zur Anhörung des Ausschusses für Inneres und Heimat v. 27.01.2020 S. 13 (Ausschussdrucksache 19(4)434D)

Die technischen Voraussetzungen und Begleitumstände des Eingriffs haben danach augenscheinlich keine verfassungsrechtlichen Fragen aufgeworfen, seine Folgen für die betroffenen Systeme bestimmen vielmehr nur dessen Gewicht und kommen bei der Festlegung der Eingriffsvoraussetzungen als Abwägungselement in Betracht. Dessen grundsätzliche Zulässigkeit berühren sie nicht. Beide Entscheidungen klären die verfassungsrechtlichen Bedingungen der untersuchten Maßnahmen und ihre namentlich datenschutzrechtlichen Konsequenzen in großer Eindringlichkeit, in den daraus sich ergebenden Gesetzgebungsauftrag werden die faktisch-technischen Voraussetzungen und Begleitumstände dieser Maßnahmen indessen nicht einbezogen. Dass sie auf diese im Sinne eines prinzipiellen Eingriffsverbots zurückwirken und deren Zulässigkeit gänzlich in Frage stellen könnten, deutet das Gericht nicht einmal an, auf das bereits vorhandene rechtliche Instrumentarium zur Problembewältigung und Schadensbegrenzung geht es ebenso wenig ein wie auf die denkbare Notwendigkeit seiner Fortentwicklung.

b) Es ist nicht zu erkennen, dass die im Zeitpunkt der damaligen Urteilsverkündung vom 20. August 2016 bereits in Kraft getretene europäische Datenschutz-Grundverordnung

> 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 (Datenschutz-Grundverordnung) ABl. L 119/1 v. 04.05.2016

(im Folgenden: DSGVO) und die schon damals gleichfalls geltende Richtlinie 2016/680

> Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates ABl. L 119/89 v. 04.05.2016

dem Bundesverfassungsgericht Anlass geben müssten, seine Rechtsprechung zu ändern oder gar im Sinne der Beschwerdeführer zu ergänzen.

Beide Rechtsakte machen ein Vorabentscheidungsverfahren vor dem Europäischen Gerichtshof nach Art. 267 AEUV nicht erforderlich, das die Aufgabe hätte, die Bedeutung des europarechtlichen Datenschutzes für das hessische Polizei- und Datenschutzrecht zu klären. Für die Entscheidung über die aktuelle Verfassungsbeschwerde sind sie unergiebig. Für den Beschwerdeführer zu 3. dürften sie ohnehin nicht einschlägig sein, da sie die Verarbeitung personenbezogener Daten nur zum Schutz natürlicher Personen betreffen. Aber auch die Beschwerdeführer zu 1. und 2. können aus ihnen einen Regelungsauftrag zum Schutz informationstechnischer Systeme nicht herleiten.

Nach Art. 16 Abs. 2 AEUV erlassen das Europäische Parlament und der Rat Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Zunächst mit der Datenschutz-Grundverordnung haben sie von dieser Zuständigkeit ganz weitgehend Gebrauch gemacht, von deren Geltung jedoch die Datenverarbeitung „durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit" ausgenommen (Art. 2 Abs. 2 Buchst. d) DSGVO). Auf diesen Tätigkeitsbereich und damit auf die Aufgaben der hessischen Polizeibehörden nach § 1 Abs. 1 und 4 HSOG findet nach ihrem insoweit wortgleichen Art. 1 Abs. 1 die Richtlinie 2016/680 Anwendung. Damit gilt sie auch für den polizeilichen Eingriff mit technischen Mitteln in informationstechni-

sche Systeme als Verfahren zur Gewinnung dort vorhandener Daten (§§ 15b Abs. 1 und 15c Abs. 1 HSOG). Zugleich entspricht jede dieser Maßnahmen als „Vorgang [...] im Zusammenhang mit personenbezogenen Daten wie das Erheben, Erfassen, [...] das Auslesen, das Abfragen [...]" dem weitgefassten europarechtlichen Begriff der Verarbeitung,

> Art. 3 Nr. 2 der Richtlinie 2016/680 und gleichlautend Art. 4 Nr. 2 DSGVO; Schwabenbauer in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 6. Aufl. 2018, G Rdn. 370 S. 880 im Anschluss an Weinhold/Johannes DVBl. 2016, 1501, 1503: Die Richtlinie sei „auch anwendbar für die ganz oder teilweise automatisierten Ermittlungstechniken, wie bspw. [...] Telekommunikationsüberwachung".

ihre besonderen Zwecke halten sich in den Grenzen polizeilicher Aufgaben; § 15b Abs. 1 HSOG fordert mit der Anknüpfung an die „Voraussetzungen des § 15a Abs. 1", dass der Eingriff zur Abwehr einer dringenden Gefahr für besonders hochwertige Rechtsgüter unerlässlich sein muss, und dasselbe gilt nach § 15c Abs. 1 HSOG für die Voraussetzungen der Online-Durchsuchung.

In welchem Maße die Richtlinie einen Bezug zu der durch die Datenerhebung verursachten Beschaffenheit der Datenquelle aufweist, erscheint dagegen zweifelhaft. Dem Erwägungsgrund Nr. 26 der Richtlinie lässt sich entnehmen, dass die Datenverarbeitung „auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffenen natürlichen Personen nachvollziehbaren Weise erfolgen" muss, ohne dass dies „an sich der Durchführung von Maßnahmen wie verdeckten Ermittlungen oder Videoüberwachung" entgegenstünde. „Diese Maßnahmen können zwecks Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit getroffen werden, sofern sie durch Rechtsvorschriften geregelt sind und eine erforderliche und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft darstellen, bei der die berechtigten Interessen der betroffenen natürlichen Person gebührend berücksichtigt werden." Anforderungen an die Vorgehensweise, mithin an den Mechanismus dieser besonderen Art der Datenverarbeitung ergeben sich daraus nur insofern, als dessen Beschaffenheit Folgen für die so erho-

benen Daten, etwa für deren Inhalt, ihre Authentizität, Integrität, Nutzung und Löschung haben kann. Mit den Voraussetzungen, also mit der Herkunft derjenigen Informationen über Schwachstellen und deren Nutzung, die zur Infiltration informationstechnischer Systeme erforderlich sind, beschäftigt sich die Richtlinie nicht.

Diese Einschränkung ist bei der Verpflichtung der Mitgliedstaaten zu berücksichtigen, im Interesse des Datenschutzes angemessene technische und organisatorische Vorkehrungen zu treffen und bei der Datenverarbeitung den Stand der Technik zu berücksichtigen. Als solche Vorkehrungen werden alle Maßnahmen verstanden, die erforderlich sind, „um die Beachtung des Datenschutzes und der Datensicherheit bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten und den dazu betriebenen Verfahren zu gewährleisten", wobei sich die hier in Betracht kommenden technischen Maßnahmen „auf den Datenverarbeitungsvorgang an sich erstrecken".

> so statt aller der „Sachstand" der Wissenschaftlichen Dienste des Deutschen Bundestages WD 3 – 3000 – 126/19 S. 3

Eine Verpflichtung zum Schutz informationstechnischer Systeme lässt sich damit nicht begründen. Sicherheitslücken,

> hier verstanden i.S.v. § 2 Abs. 6 des BSI-Gesetzes v. 14.08.2009 (BGBl. I S. 2821), zuletzt geändert durch Verordnung v. 19.06.2020 (BGBl. I S. 1328), als „Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können"

ihre Erforschung und Nutzung ebenso wie die Entwicklung und der Einsatz der hierfür erforderlichen Software haben zwar insofern einen datenrelevanten Bezug, als sie zur Erhebung zumindest auch personenbezogener Daten eingesetzt werden. Allein dadurch werden sie jedoch nicht zum Gegenstand des Datenschutzes und fallen deshalb auch nicht in die Kompetenzzuweisung durch Art. 16 AEUV. Vielmehr rechnen sie als Annex zum Gefahrenabwehrrecht der Mitgliedstaaten und fallen deshalb nach dem Grundsatz der begrenzten Ein-

zelermächtigung (Art. 5 Abs. 1 Satz 1 EU-Vertrag und Art. 2 Abs. 6 AEUV) ausschließlich in deren Zuständigkeit. Die beispielhafte, in § 59 Abs. 3 HDSIG wiederholte Aufzählung der von den Mitgliedstaaten zu treffenden Maßnahmen des Art. 29 Abs. 2 der Richtlinie bestätigt, dass weder die Schäden, die die Infiltration an informationstechnischen Systemen möglicherweise hervorrufen könnte, noch der Umgang mit Sicherheitslücken zum Regelungsbereich der Richtlinie gehören.

Wäre der den Art. 29 der Richtlinie einleitende Abs. 1 umfassender zu verstehen,

> Danach sind „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen (zu) treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Artikel 10". Dort werden besondere Anforderungen an die Verarbeitung solcher Daten gestellt, aus denen beispielsweise „die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen".

wollte er also ein angemessenes Schutzniveau nicht nur für Daten, sondern auch für die technischen Verfahren zur Datengewinnung gewährleisten, dann hätte der Landesgesetzgeber die mit der Verfassungsbeschwerde aufgeworfenen Fragen mit dem nahezu gleichlautenden § 59 Abs. 1 Satz 1 HDSIG im Übrigen bereits beantwortet. Vorlagefähige Fragen nach der Auslegung der Richtlinie 2016/680 stellten sich in diesem Fall nicht, das hessische Schwachstellenmanagement wäre am Maßstab des einfachen Landes- und zunächst weder des europäischen noch des Verfassungsrechts zu überprüfen. Normzweck der Richtlinie ist indessen allein der Schutz personenbezogener Daten und nicht die Begründung eines besonderen Schutzniveaus für diejenigen Quellen und Systeme, aus denen und mit deren Hilfe die Daten gewonnen werden. Das Prinzip des Datenschutzes „durch Technikgestaltung und datenschutzfreundliche Voreinstellungen"

> so die Überschrift von Art. 20 der Richtlinie, wiederholt in deren Erwägungsgrund Nr. 53 und sodann in § 66 HDSIG, vielfach unter dem Stichwort „privacy by design and by default" behandelt

und die Notwendigkeit der Folgenabschätzung „insbesondere bei Verwendung neuer Technologien", sofern „aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen" zu erwarten ist,

> Art. 27 Abs. 1 der Richtlinie und § 62 Abs. 1 HDSIG

ändern daran nichts.

Es erscheint daher folgerichtig, dass im Zuge der insoweit beispielhaften Umsetzungsgesetzgebung des Bundes der Integritätsschutz der von verdeckten Eingriffen betroffenen informationstechnischen Systeme, die Anforderungen an die hierbei eingesetzte Software und der Umgang mit Sicherheitslücken außer Betracht geblieben sind. Das Datenschutz-Anpassungs- und -umsetzungsgesetz (EU-DSAnpUG-EU) vom 30. Juni 2017 (BGBl. I S. 2097) wie das Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 vom 20. November 2019 (BGBl. I S. 1724) schützen unter Betonung ihrer Vereinbarkeit mit europäischem Recht

> s. dazu BT-Drs. 18/11325 S. 73; auch in den Anhörungen der beteiligten Ausschüsse spielte die Problematik von Eingriffen in informationstechnische Systeme keine Rolle, vgl. die Anhörungsprotokolle der 110. Sitzung des Innenausschusses v. 27.03.2017 und der 37. Sitzung des Ausschusses für Recht und Verbraucherschutz v. 20.02.2019.

personenbezogene Daten und nicht die Integrität informationstechnischer Systeme. Danach ist die Annahme erlaubt, dass die im weitesten Sinne technischen Fragen des Eingriffs in informationstechnische Systeme aus der Sicht weder der Bundesregierung noch des Bundestages noch der damals befragten Sachverständigen einen spezifisch datenschutzrechtlichen Zusammenhang aufweisen und deren Regelung, soweit sie erforderlich sein sollte, nicht durch europäisches Datenschutzrecht determiniert ist.

c) Als Prüfmaßstab für die mit der Verfassungsbeschwerde behauptete Ergänzungsbedürftigkeit und Verfassungswidrigkeit der §§ 15b und 15c HSOG kommt somit allein das Grundrecht der Beschwerdeführer auf Integrität und Vertraulichkeit informationstechnischer Systeme mit seinem Schwerpunkt im Integritätsschutz in Betracht. Ginge es ihnen um die Abwehr von Eingriffen in ihre Telekommunikation, wären diese am Grundrecht des Art. 10 GG zu messen.

BVerfGE 120, 274, 309; 141, 220, 309 Rdn. 228

Ziel ihrer Verfassungsbeschwerde ist jedoch unabhängig von etwa betroffenen Kommunikationsvorgängen die Sicherung ihrer informationstechnischen Infrastruktur mit der Folge, dass Maßnahmen, die allein deren Schutzbereich berühren, sich an den Schranken des Art. 2 Abs. 1 GG messen lassen müssen.

BVerfGE 141, 220, 265 Rdn. 93

Als verfassungswidrig kämen jene Befugnisnormen daher nur in Betracht, wenn sie mit der Regelung der Voraussetzungen von Quellen-TKÜ und Online-Durchsuchung, ihrer Durchführung und der Bewältigung der Eingriffsfolgen den Anforderungen des legitimen Zwecks, der Eignung, der Erforderlichkeit und der Verhältnismäßigkeit im engeren Sinne

so zuletzt etwa BVerfGE 120, 274, 318f.; 125, 260, 306; 141, 220, 265 Rdn. 93

nicht entsprächen. Tatsächlich sind sie nach Maßgabe des gegenwärtig technisch Möglichen jedoch verfassungskonform.

Auf die Herkunft der von den Polizeibehörden eingesetzten Software kommt es in diesem Zusammenhang, anders als es die Beschwerdeführer möglicherweise sehen, nicht an. Während Hessen insoweit nicht über eigene Erfahrungen verfügt, kommen nach dem Beispiel des Bundeskriminalamtes sowohl Eigenentwicklungen wie der Erwerb von Privatunternehmen, nach Hinweisen in der Literatur angeblich auch auf dem grauen oder schwarzen Markt, in Betracht. Von

dem Schutzbereich des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme wird ein solcher Beschaffungsvorgang nicht erfasst, da er die Voraussetzungen, Modalitäten und Folgen eines Eingriffs unberührt lässt.

Ausgangspunkt der allgemeinen Verhältnismäßigkeitsprüfung ist die von den Beschwerdeführern nicht in Frage gestellte Tatsache, dass der Gesetzgeber mit der Zulassung von Quellen-TKÜ und Online-Durchsuchung ausschließlich verfassungsmäßige Ziele verfolgt. Beide Maßnahmen sind nach seiner nicht zu beanstandenden Einschätzung zur Erreichung eines zweifellos legitimen Zieles geeignet, können also eine dringliche Gefahr für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit abzuwehren helfen, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt (§ 15b Abs. 1 i.V.m. § 15a Abs. 1, § 15c Abs. 1 HSOG). Sofern sie zur Abwehr einer derartigen Gefahr, wie eigens vorausgesetzt, unerlässlich sind, mildere Mittel also wegen deren sicher absehbaren Erfolglosigkeit nicht in Betracht kommen, sind sie angesichts des besonderen Bedrohungspotentials und ihrer Eignung auch erforderlich.

> in diesem Sinne z.B. die Antworten der Bundesregierung v. 12.05.2020 BT-Drs. 19/19105 S. 3 und v. 22.06.2020 BT-Drs. 19/20245 S. 4 für die Gefahrenabwehrbehörden des Bundes

Was die Beschwerdeführer dagegen letztlich bezweifeln, ist die Verhältnismäßigkeit im Sinne einer ausgeglichenen Beziehung zwischen der Schwere der Grundrechtsbeeinträchtigung durch den Eingriff und der Bedeutung der mit dem Eingriff verfolgten öffentlichen Belange. Bei einer Gesamtwürdigung darf dessen Schwere danach nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen.

> BVerfGE 120, 274, 321f.

Der Gesetzgeber hat deshalb „das Individualinteresse, das durch einen Grundrechtseingriff beschnitten wird, den Allgemeininteressen, denen der Eingriff dient, angemessen zuzuordnen. Die Prüfung an diesem Maßstab kann dazu führen, dass ein Mittel nicht zur Durchsetzung von Allgemeininteressen angewandt

werden darf, weil die davon ausgehenden Grundrechtsbeeinträchtigungen schwerer wiegen als die durchzusetzenden Belange".

> BVerfGE 120, 274, 322; später spricht BVerfGE 141, 220, 267 Rdn. 98 von der „Aufgabe des Gesetzgebers, einen Ausgleich zwischen der Schwere der [...] zur Prüfung stehenden Eingriffe in die Grundrechte potentiell Betroffener auf der einen Seite und der Pflicht des Staats zum Schutz der Grundrechte auf der anderen Seite zu schaffen".

In diese Abwägung hat das Bundesverfassungsgericht im Fall der Online-Durchsuchung zahlreiche Risiken auf Seiten der Betroffenen eingestellt: so etwa die Möglichkeit der Polizei, aus der Fülle der gewonnenen Daten ganze Verhaltens- und Kommunikationsprofile abzuleiten, die Gefahr, die Teilnahme der Bürger an einer unbeobachteten Telekommunikation und zum Einsatz eigener Verschlüsselungstechnologie könne beschränkt oder vereitelt werden, das durch seine Heimlichkeit und seine Dauer noch erhöhte Gewicht des Eingriffs und schließlich dessen Prägung dadurch, dass in seiner Folge Schäden an dem betroffenen Rechner nicht ausgeschlossen werden können.

> BVerfGE 120, 274, 322-325; zu diesem letzten Punkt etwa Bäcker in: Rensen/Brink (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts – erörtert von den wissenschaftlichen Mitarbeitern, 2009, S. 99, 125; Hoffmann-Riem JZ 2008, 1009, 1015

In welchem Maße sich dieses zuletzt genannte Risiko tatsächlich verwirklicht, bedürfte der Klärung. Hessische Erfahrungen stehen dafür nicht zur Verfügung, da das Land bisher von den Befugnissen der §§ 15b und 15c HSOG keinen Gebrauch gemacht und eine eigene Software weder entwickelt noch beschafft hat. Entsprechende Daten sind, soweit erkennbar, auch im Übrigen nicht vorhanden, die einer sachnahen Risikoeinschätzung zugrunde gelegt werden könnten. Die Gefahrenbeschreibung der Beschwerdeführer muss deshalb nicht unrichtig sein, bleibt aber abstrakt und lässt eine Bewertung von Nähe und Größe des Schadensrisikos ebenso wenig zu wie eine Qualifizierung der Maßnahmen, die zu dessen Minderung oder Beseitigung getroffen werden müssten. Der Gesetzgeber ist daher lediglich in der Lage, aufgrund seiner Beurteilung der Verhältnismäßigkeit diejenigen Regelungen zu treffen, die nach seiner begründeten und

willkürfreien Einschätzung die vom Bundesverfassungsgericht hervorgehobenen Risiken der zugelassenen Eingriffe nach Möglichkeit ausschließen oder zumindest derart verringern, dass ihnen im Vergleich mit der überragenden Bedeutung der gefährdeten Rechtsgüter ein geringeres Gewicht zukommt.

Auf der Grundlage dieser Abwägung sind verfassungsrechtliche Einwände gegen die §§ 15b und 15c HSOG weder unter dem Gesichtspunkt des behaupteten Schädigungspotentials noch im Hinblick auf die Möglichkeit eines unsachgemäßen Umgangs mit Sicherheitslücken zu erheben.

Dabei ist die Gesamtheit aller Regeln in den Blick zu nehmen, die den Eingriff in das Zielsystem steuern und seine Folgen begrenzen. Beide Bestimmungen sichern die Rechtssphäre möglicher Betroffener in mehrfacher Hinsicht und weit über die Anforderungen des allgemeinen Grundsatzes der Verhältnismäßigkeit (§ 4 HSOG) hinaus gegen polizeiliche Eingriffe ab:

Angesichts der anspruchsvollen Maßstäbe, die das Bundesverfassungsgericht an die Befugnisse des Bundeskriminalamts angelegt hat, dürfen Eingriffe nur in Betracht gezogen werden, wenn mehrere einschränkende Voraussetzungen gleichzeitig erfüllt sind. Sie müssen zur Abwehr einer dringenden Gefahr dienen, diese Gefahr muss höchstwertige Rechtsgüter bedrohen und zur Gefahrenabwehr müssen diese Eingriffe unerlässlich sein (§ 15b Abs. 1 i.V.m. § 15a Abs. 1 Satz 1 HSOG). Zudem müssen sie gerade deshalb notwendig sein, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen. Während die Polizeibehörden die Mittel zur Bewältigung ihrer Aufgaben sonst nach pflichtgemäßem Ermessen zu wählen haben (§ 5 HSOG), werden die Verfahren der Quellen-TKÜ und der Online-Durchsuchung besonderen Anforderungen unterworfen, die Qualitätsstandards für die benutzte Software voraussetzen und durch den Einsatz technischer Mittel verhindern, dass die Einwirkung auf die betroffenen Systeme durch das Verhalten der Anwender bewusst oder versehentlich fehlgesteuert werden könnte. Es genügt daher nicht, durch technische Maßnahmen sicherzustellen, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die

für die Datenerhebung unerlässlich sind (§ 15b Abs. 2 Nr. 1 HSOG). Vielmehr muss technisch weiter sichergestellt sein, dass diese Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert auch wieder rückgängig gemacht werden. Auch die unbefugte Nutzung der Software muss schließlich nach dem Stand der Technik verhindert werden (§ 15b Abs. 2 Satz 2 HSOG). Dieselben rechtlichen und technischen Maßgaben gelten für die Online-Durchsuchung (§ 15c Abs. 1 und 3 Satz 1 i.V.m. § 15b Abs. 2 HSOG), wobei, soweit technisch möglich, sicherzustellen ist, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden (§ 15c Abs. 3 Satz 2 HSOG). Außer bei Gefahr in Verzug dürfen beide Maßnahmen nur nach richterlicher Anordnung unter Angabe ihrer wesentlichen Gründe durchgeführt werden (§ 15b Abs. 3 Satz 2 und § 15c Abs. 3 Satz 3 jeweils i.V.m. § 15 Abs. 5 Satz 1 bis 9 HSOG) und sind - mit Verlängerungsmöglichkeit - auf höchstens drei Monate zu befristen. Dabei hat das Gericht sämtliche Voraussetzungen der beantragten Maßnahmen, also auch die Eignung der Software zu prüfen und kann sich bei Zweifeln sachverständig beraten lassen.

> vgl. die Antwort der Bundesregierung v. 21.08.2018 BT-DRs. 19/2907 S. 5 zu Frage 6., die im Zusammenhang mit § 100a StPO schon zuvor darauf verwiesen hat, die „eingesetzten Softwareprodukte (würden) [...] vor der Einsatzfreigabe umfassend hinsichtlich der Erfüllung der gesetzlichen Vorgaben überprüft. Die Ergebnisse dieser Prüfung stehen den in der Fragestellung genannten Stellen (sc. dem Gericht, der Staatsanwaltschaft und den durchführenden Behörden) auf Anforderung zur Einsichtnahme zur Verfügung", wobei „vor dem Hintergrund der eindeutigen Maßgabe des Artikels 20 Absatz 3 zweiter Halbsatz des Grundgesetzes [...] sich Staatsanwaltschaft und Gericht dabei aus Sicht der Bundesregierung auch auf die Angaben der die Maßnahme durchführenden Behörde verlassen" können (Antwort v. 24.05.2018 BT-Drs. 19/2306 S. 4f., 6. zu Fragen 5.-7., 14.).

Hinzu tritt die Protokollierungspflicht nach § 28 Abs. 1 und 2 Nr. 4 und 5 HSOG, die die nachträgliche Überprüfbarkeit der gesamten Maßnahme gewährleistet, und die Übertragung des Auswertungsvorgangs auf das Gericht (§ 15b Abs. 3 Satz 3 und § 15c Abs. 3 Satz 4 i.V.m. § 15 Abs. 9 Satz 1-7 HSOG); nur bei Gefahr in Verzug kommt eine Auswertung durch die Polizeibehörde in Betracht, muss dann aber gesondert im Verfahren und durch eine nachträgliche gerichtliche Entscheidung abgesichert sein. Neben diese informationstechnischen und

verfahrensrechtlichen Vorgaben, die durch Mitteilungspflichten gegenüber Betroffenen, die Möglichkeit nachträglicher gerichtlicher Überprüfung und denkbare Beweisverwertungsverbote bei unzulässig erlangten Daten noch ergänzt werden, tritt schließlich nach § 17a HSOG die substantielle Rechtfertigungspflicht gegenüber dem Parlament, letztlich auch gegenüber der Öffentlichkeit und die Beobachtung durch den Beauftragten für Datenschutz und Informationsfreiheit (§ 29a HSOG).

Dieser gesamte vom Gesetz vorgegebene Ablauf kann zwar die Tiefe eines konkreten Eingriffs insoweit nicht vermindern, als sich dessen Folgen durch den Einsatz auch der schonendsten Technik nicht gänzlich vermeiden ließen. Er hebt jedoch, vorsorglich auch gegenüber den eingriffsbefugten Polizeibehörden, den einzigartigen Ausnahmecharakter von Quellen-TKÜ und Online-Durchsuchung hervor, reduziert, wie das hessische Beispiel zeigt, ihre Einsatzhäufigkeit auf extreme Bedrohungslagen und wahrt deshalb bei einer Gesamtabwägung die Anforderungen des Verhältnismäßigkeitsgebotes. Damit halten beide Bestimmungen der verfassungsrechtlichen Überprüfung Stand, ohne dass sie im Sinne der Verfassungsbeschwerde ergänzt werden müssten.

Darin konnte sich der Landesgesetzgeber durch das Bundesverfassungsgericht bestätigt sehen: Mit im vorliegenden Zusammenhang unbedeutenden Änderungen sind §§ 15b und 15c HSOG unter Berücksichtigung des Urteils vom 20. April 2016 (BVerfGE 141, 220) dem § 49 BKAG vom 1. Juni 2017 (BGBl. I S. 1354) nachgebildet,

> so die Begründung des Änderungsantrags LT-Drs. 19/6502 S. 39f.

der seinerseits weitgehend dem früheren § 20k BKAG entspricht.

> so die Begründung des Gesetzentwurfs BT-Drs. 18/11163 S. 118; ebenso folgt die Regelung der Quellen-TKÜ in § 51 BKAG der Vorgängernorm des § 20l BKAG (ebenda S. 120).

Die §§ 20k und 20l BKAG in der Fassung des Gesetzes vom 25. Dezember 2008 (BGBl. I. S. 3083) hat das Bundesverfassungsgericht in seinem Urteil vom

20. April 2016 umfassend überprüft und mit Einschränkungen, die für die Beurteilung der Verfassungsbeschwerde nicht maßgeblich sein dürften, gebilligt.

> BVerfGE 141, 220, 303-309 Rdn. 208-226 (zu § 20k), 309-316 Rdn. 227-226 (zu § 20l)

Wie oben (S. 32-35) bereits wiedergegeben hat es dabei auch die technischen Voraussetzungen und Begleitumstände des Eingriffs in informationstechnische Systeme in den Blick genommen, hat ihnen aber letztlich keine für die verfassungsrechtliche Beurteilung maßgebliche Bedeutung zugemessen. Diese Ausführungen lassen sich umstandslos auf die hessische Rechtslage übertragen. Mit ihnen hätten sich die Beschwerdeführer daher auseinandersetzen müssen, um ihre Ansicht zu begründen, der Gesetzgeber habe eine Regelung verfassungswidrig unterlassen, die das Bundesverfassungsgericht nicht für erforderlich gehalten hat. Insoweit entspricht ihre Verfassungsbeschwerde daher schon nicht den Anforderungen an eine substantiierte Begründung (§§ 92 und 23 Abs. 1 BVerfGG) und ist deshalb unzulässig.

Überdies legen die Beschwerdeführer nicht dar, welche Möglichkeiten der Landesgesetzgeber gehabt haben könnte oder gegenwärtig hätte, um die Anforderungen an eine Infiltrationssoftware vollzugstauglich und zugleich in einer Weise zu regeln, die Nachteile für das Zielsystem schlechthin auszuschließen vermag. Die immer schnelleren Innovationszyklen der Informationstechnologie lassen technische Normen für eine derartige Software nicht zu, sodass der Gesetzgeber, wie er es auch getan hat, nur allgemein auf die technischen Möglichkeiten der Schadensvermeidung und auf den aktuellen Stand der Technik jeweils im Sinne eines Optimierungsgebotes verweisen kann. Deren Beachtung macht er den Polizeibehörden damit gleichzeitig zur Pflicht und überlässt ihnen keinesfalls die Entscheidung darüber, ob und wie sie den Eingriff auf das unerlässliche Maß begrenzen und folgenlos wieder rückgängig machen sollten. Um beides „technisch sicherzustellen", müssen sie im Gegenteil die am besten geeigneten objektiv verfügbaren Mittel nutzen, zu deren Bereitstellung das Land gleichzeitig verpflichtet ist. Sollten sich die Begrenzungs- und Beseitigungsanforderungen ge-

genwärtig aus technischen Gründen (noch) nicht erfüllen lassen, liefen die Eingriffsbefugnisse leer, wären aber nicht verfassungswidrig.

vgl. BVerfGE 141, 220, 311 Rdn. 234

Unabhängig davon haben sich die Polizeien von Bund und Ländern neben der als **Anlage** bereits beigefügten Standardisierten Leistungsbeschreibung für eine eingriffstaugliche Software auf einen „einheitlichen Gesamtabnahme-Prozess (eGAP) für Quellen-TKÜ und ODS-Software" verständigt. Er legt keine technischen Standards für die Software fest, sondern schafft ein Verfahren, das über mehrere Schritte hinweg von der Formulierung des Anforderungsprofils für eine konkrete Software über mehrere Tests ihrer Funktionalität und Rechtskonformität zu einer abschließenden Bewertung und Entscheidung über ihre Verwendbarkeit führt. Dieses im Wege der Selbstverpflichtung für Bund und Länder verbindliche Konzept gewährleistet eine flexible Anpassung an den aktuellen Stand der Technik und an die gesetzlichen Anforderungen, sichert die unumgängliche Geheimhaltung des Eingriffsinstrumentariums und erfüllt damit insgesamt den Optimierungsauftrag auch des hessischen Gesetzes. Eine grundrechtlich relevante Ergänzungspflicht des Gesetzgebers, die er bei der erstmaligen Zulassung der Quellen-TKÜ im Jahre 2009 oder gegenwärtig verletzt haben könnte, ist insoweit nicht auszumachen.

Ebenso wenig können die Beschwerdeführer aus ihren Grundrechten einen Anspruch auf spezielle Regeln über die Behandlung derjenigen Schwachstellen herleiten, die den Zugang zu dem jeweiligen Zielsystem ermöglichen. Ihnen geht es dabei um den Umgang namentlich mit sog. Zero-Day-Sicherheitslücken, die der Öffentlichkeit, den Entwicklern und den Vertreibern der betroffenen Systeme bislang unbekannt und die deshalb noch nicht geschlossen sind, während die Polizeibehörden sie - typischerweise im Zusammenhang mit dem beabsichtigten Eingriff - in Erfahrung gebracht haben und einsetzen.

zum Begriff und zur Nutzbarkeit s. etwa Herpig, Schwachstellen-Management für mehr Sicherheit, Stiftung Neue Verantwortung: 2018, S. 10ff.

Das Bundesverfassungsgericht sieht hier „die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder diese sogar aktiv daraufhin wirkt, dass die Lücken unerkannt bleiben", und stellt ihr das Vertrauen der Bevölkerung darauf gegenüber, dass der Staat um eine möglichst hohe Sicherheit informationstechnischer Systeme bemüht sei.

BVerfGE 120, 274, 326; vgl. auch die weiteren Nachweise o. S. 35

Dass dieser so beschriebene Zielkonflikt grundrechtlich relevant sein, also insbesondere den Schutzbereich des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme berühren könnte, deutet das Gericht nicht einmal an. Tatsächlich können sich die Beschwerdeführer insoweit zwar auf eine Schutzpflicht des Landes im Sinne einer allgemeinen Bemühenspflicht, aber nicht auf ein Grundrecht berufen, das das Land verpflichten könnte, für schwachstellenfreie digitale Verbindungen zu sorgen, die Schließung von Sicherheitslücken zumindest aber zu veranlassen.

Quellen-TKÜ und Online-Durchsuchung als Eingriffe mit technischen Mitteln in ein informationstechnisches System setzen dort eine systemimmanente Sicherheitslücke voraus, die der Eingriff nutzt, aber nicht schafft. Die Ursache der Sicherheitslücke ist nicht grundrechtsrelevant, und das gilt ebenso für die Vorgehensweise der Polizeibehörden, mit der sie sich Kenntnis von der Sicherheitslücke verschaffen, solange sie dabei nicht in den Schutzbereich etwa in Betracht kommender anderer Grundrechte eingreifen. Vielmehr schützt das Grundrecht auf Gewährleistung und Vertraulichkeit informationstechnischer Systeme erst vor dem Zugriff auf die dort gespeicherten Daten und vor Online-Durchsuchungen, „mit denen private Computer wie sonstige informationstechnische Systeme manipuliert und ausgelesen, sowie persönliche Daten, die auf externen Servern in einem berechtigten Vertrauen auf Vertraulichkeit ausgelagert sind, erfasst und Bewegungen der Betroffenen im Netz verfolgt werden".

BVerfGE 141, 220, 304 Rdn. 210

Geschützt ist damit zugleich das Vertrauen auf die Integrität des Systems selbst,

Hoffmann-Riem JZ 2008, 1009, 1012

und diesem Vertrauen korrespondiert eine staatliche Schutzpflicht. Sie kann indes nur soweit reichen, wie das Vertrauen sich den Umständen nach als berechtigt erweist. Insoweit mag schon zweifelhaft sein, ob es angesichts der keineswegs auf Maßnahmen nach §§ 15b und 15c HSOG beschränkten, sondern weitergehenden Eingriffsbefugnisse zumal von Bundesbehörden wirklich die unbegrenzte Sicherheit des Systems vor staatlicher Infiltration zum Gegenstand haben kann. Erst recht wird der Nutzungsberechtigte, wie das ständige Auftreten immer neuer Schadsoftware, die entsprechenden Warnungen und die zahlreichen Angebote von Updates und Virenscannern zeigen, vernünftigerweise nicht ohne weiteres darauf vertrauen dürfen, dass die von ihm installierten Abwehrmechanismen greifen und sein System deshalb frei von Sicherheitslücken und gegen Eingriffe schlechthin abgesichert sei. Insoweit verletzt das Land keine Schutzpflichten, wenn es den von einer Maßnahme nach §§ 15b und 15c HSOG Betroffenen zwar nachträglich unterrichtet, ihn aber nicht auch auf das Verfahren und die Sicherheitslücken aufmerksam macht, mit deren Hilfe es Daten erhoben hat.

> Die grundsätzliche Benachrichtigungspflicht nach § 29 Abs. 1 HSOG verweist für deren Umfang im Fall verdeckter Maßnahmen auf § 51 HDSIG; bei den hier besprochenen Maßnahmen kann die Unterrichtung nach § 29 Abs. 5-7 i.V.m. § 28 Abs. 2 Nr. 5 und 6 HSOG überdies zurückgestellt werden oder gänzlich unterbleiben.

Verfassungsrechtliche Bedenken sind in diesem Punkt, soweit feststellbar, bisher mit Grund nicht erhoben worden.

Das beantwortet freilich nicht die Frage, wie die Polizeibehörden des Landes mit ihrer Kenntnis von Sicherheitslücken umzugehen haben, ob es hierfür eines besonderen, vielleicht sogar gesetzlichen Regelwerks bedarf und welche Anforderungen die Schutzpflicht für die Integrität informationstechnischer Systeme allenfalls stellt.

Allgemein wird die Handhabung von Sicherheitslücken durch den Grundsatz der Verhältnismäßigkeit (§ 4 HSOG) bestimmt. Danach wäre es unzulässig, Sicherheitslücken des Zielsystems gleichsam auf Vorrat nur deshalb offenzuhalten, weil sie, ohne dass diese Annahme gerechtfertigt wäre, für spätere Eingriffe möglicherweise noch benötigt werden könnten.

> zu dem wegen seiner Herleitung aus dem Verhältnismäßigkeitsgrundsatz hier sinngemäß anwendbaren Verbot, Polizeiverfügungen nicht lediglich zur Erleichterung polizeilicher Arbeit einzusetzen, s. Graulich in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 6. Aufl. 2018, E Rdn 177 S. 388

Das gesamte Eingriffsverfahren ist auf zeitliche Begrenzung angelegt: Grundlage der richterlichen Genehmigung von Quellen-TKÜ und Online-Durchsuchung (§ 15b Abs. 3 Satz 2 und § 15c Abs. 3 Satz 3 jeweils in Verbindung mit § 15 Abs. 5 Satz 1-9 HSOG) ist eine im Zeitpunkt der Genehmigung bestehende Gefahrenlage von besonderer Dringlichkeit, deren Abwehr einen im Grundsatz auf höchstens drei Monate zu befristenden und allenfalls um neun Monate verlängerbaren Zugriff erfordert, der wiederum unverzüglich beendet werden muss, sobald seine Voraussetzungen entfallen. Je länger der Zugriff dauert und die Sicherheitslücke besteht,

> Die Bundesregierung hat die Einsatzdauer von Software zur Durchführung von Maßnahmen der informationstechnischen Überwachung durch das Bundeskriminalamt mit durchschnittlich ca. 94 Tagen angegeben (BT-Drs. 19/2907 v. 21.06.2018 S. 7 zu Fragen 15. und 16).

desto größer wird die Wahrscheinlichkeit, dass sie auch Dritten bekannt und von ihnen unerlaubt genutzt wird. Damit droht dem Zielsystem die von dem Eingriff zwar nicht verursachte, aber mit seiner Dauer wachsende Gefahr einer Infiltration mit Schadprogrammen, über die die Polizeibehörden, um ihre Maßnahmen nicht offenlegen zu müssen, den Betroffenen nicht unterrichten dürfen, die sie selbst aber auch nicht beheben können. In derartigen Fällen kommt deshalb nur ein von dem konkreten Eingriff ausgelöstes, aber nicht darauf bezogenes Meldeverfahren in Betracht, das letztlich in eine Warnung der Hersteller, Vertreiber und Anwender von Informationstechniken münden kann, wie es in § 3 Abs. 1 Nr. 14

des BSI-Gesetzes vorgesehen und aus Gründen der Verhältnismäßigkeit unverzüglich nach dem Abschluss des Eingriffs einzuleiten ist.

Darin wird sich die Schutzpflicht des Landes aber auch erschöpfen müssen. Eine gesteigerte Verantwortung seiner Polizeibehörden ließe sich allenfalls damit begründen, dass sie die Sicherheitslücke überhaupt erkannt und für ihren rechtmäßigen Eingriff genutzt haben. Da sie die in Anspruch genommenen Schwachstellen nicht verursacht, sie auch nicht aktiv verborgen gehalten oder sonst ihren Fortbestand veranlasst haben und mit ihren Mitteln auch nicht schließen, sondern nur - freilich nicht gegenüber den Betroffenen, sondern allgemein - eine Warnung veranlassen und auf diesem Wege ihre Schließung durch den Systemanbieter ermöglichen können, erwächst dem Land daraus keine Garantenstellung für die Integrität des betroffenen Systems; insoweit gilt nichts anderes als für die übrigen Gegenstände der Daseinsvorsorge, die es im Rahmen seiner Zuständigkeit zu ermöglichen hat, deren Funktionieren es aber nicht unter seinen besonderen Schutz stellen muss, solange ihm die Verfassung keine besonderen Gewährleistungspflichten auferlegt.

Dem entspricht es, dass es ein Grundrecht auf aktiven Integritätsschutz mit dem Ziel der Beseitigung, zumindest aber der Feststellung von und der Warnung vor Sicherheitslücken sowie der Abwehr von Schadsoftware nicht geben kann. Eine derartige mit Erfüllungsansprüchen versehene Verantwortung haben Bund und Länder, soweit ersichtlich, nie übernommen, und sie wären auch außerstande, ihr gerecht zu werden. Ihrer aus dem Integritätsgrundrecht folgenden weniger anspruchsvollen Schutzpflicht müssen sie dagegen nachkommen, sind dabei von Verfassungs wegen jedoch nicht auf bestimmte Maßnahmen festgelegt, solange diese nicht das Untermaßverbot verletzen.

> zur weitreichenden Einschätzungsprärogative des Gesetzgebers etwa BVerfGE 77, 170, 214f.; 88, 203, 262; 117, 202, 227 Rdn. 63; 125, 39, 78 Rdn. 135; zusammenfassend statt aller Dreier in: ders., Grundgesetz-Kommentar, 3. Aufl. 2013, Vorbem. Rdn. 103

Aus der Sicht und mit den Handlungsmöglichkeiten des Landes kommt insoweit nur ein Meldeverfahren für Sicherheitslücken in Betracht, wie es der IT-

Planungsrat auf der Grundlage von § 2 Abs. 1 des IT-Staatsvertrages in seiner gegenwärtig geltenden Fassung

> Nach § 3 Abs. 1 Satz 1 des Vertrages zur Ausführung von Artikel 91c GG (BGBl. 2010 I S. 663) sollen „für den im Rahmen ihrer Aufgabenerfüllung notwendigen Austausch von Daten zwischen Bund und den Ländern [...] gemeinsame Standards für die auszutauschenden Datenobjekte, Datenformate und Standards für Verfahren, die zur Datenübertragung erforderlich sind, sowie IT-Sicherheitsstandards festgelegt werden". Diese Regelung gilt nach Art. 1 Nr. 6 des Ersten Änderungsstaatsvertrages (BGBl. 2019 I S. 1127 = GVBl. 2019 S. 151) mit einer geringfügigen Ergänzung nunmehr als § 2 fort.

für Bund und Länder festgelegt hat. Mit Beschluss des IT-Planungsrates vom 5. Oktober 2017 (Nr. 2017/35) gilt ein „Verbindliches Meldeverfahren zum Informationsaustausch über IT-Sicherheitsvorfälle im VerwaltungsCERT-Verbund (VCV)" (CERT = Computer Emergency Response Team), nach dessen § 2 Abs. 1 Nr. 1 vom Bund und den Ländern IT-Sicherheitsvorfälle zu melden sind, bei denen Auswirkungen auf die Länder oder den Bund nicht ausgeschlossen werden können oder die auch für andere als relevant eingeschätzt werden. Adressaten sind „alle Teilnehmer des VCV zeitgleich" (§ 4 Nr. 2), zu den Meldekategorien zählen nach Anlage 1 Nr. 3 des VCV-Meldestandards neuartige Sicherheitslücken oder Schwachstellen in IT-Produkten, die durch den Meldenden aufgedeckt wurden. Davon werden nach dem Wortlaut dieser für Bund und Länder verbindlichen Vorgabe auch solche Sicherheitslücken erfasst, die die Polizeibehörden der Länder für ihre Eingriffe in informationstechnische Systeme nutzen. Das Bundesamt für Sicherheit in der Informationstechnik wird damit aufgrund seiner Zuständigkeit für die Informationssicherheit auf nationaler Ebene (§ 1 Satz 2 BSI-Gesetz) in die Lage versetzt, nicht nur die Polizeien der Länder bei der Wahrnehmung ihrer gesetzlichen Aufgaben zu unterstützen, sondern auch - unter anderem - Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik zu beraten und zu warnen (§ 3 Abs.1 Nr. 13 Buchst. a) und Nr. 14 BSI-Gesetz). Im Rahmen seiner kompetenziellen Möglichkeiten hat das Land mit seinem Anschluss an das beschriebene Meldeverfahren getan, was zur Erfüllung seiner verfassungsrechtlichen Schutzpflichten für die Integrität informations-

technischer Systeme sinnvoll und erforderlich ist. Etwa in Betracht kommende weitergehende Schutzmaßnahmen könnte allenfalls der Bund treffen.

Die Bundesregierung bemüht sich zwar ihrerseits seit langem, wie sie wiederholt erklärt hat, um ein Schwachstellenmanagement, das die Bedürfnisse der Gefahrenabwehr- und Strafverfolgungsbehörden mit den Integritätsinteressen der Bürger zum Ausgleich bringt.

> „Die Bundesregierung setzt sich inhaltlich mit der Thematik des Umgangs mit Sicherheitslücken und Exploits (auch Zero-Day-Exploits) auseinander. Da die Meinungsbildung innerhalb der Bundesregierung nicht abgeschlossen ist, kann weder zur Frage des möglichen Ankaufs noch zum möglichen Umgang mit (erheblichen) Sicherheitslücken in Software- und Hardwareprodukten eine Aussage getroffen werden" (Antwort v. 25.05.2018 BT-Drs. 19/2337 S. 3 zu Fragen 2. und 3. im Anschluss an ihre Antworten v. 25.09.2017 BT-Drs. 18/13667 S. 7 auf die Schriftlichen Fragen 9. und 10., v. 07.02.2018 BT-Drs. 19/662 S. 4f. zu Frage 7.; ebenso die Antworten v 03.06.2020 BT-Drs. 19/19753 S. 2 und v. 22.06.2020 BT-Drs. 19/20245 S. 7 zu Frage 15.). Für erwägenswert hält sie „die Erarbeitung eines klaren und technikneutralen Ansatzes, der eine Lösung dieser Herausforderung aufzeigt. Die Bundesregierung steht hier noch am Anfang einer Lösungsfindung, die gemeinsam und im Dialog mit allen Beteiligten erarbeitet werden wird" (Antwort v. 06.02.2020 BT-Drs. 19/17055 S. 16 zu Frage 9.).

Ein eigenes Konzept hat sie dazu noch nicht entwickelt, ohne dass ihr deshalb bisher eine Schutzpflichtverletzung vorgeworfen worden wäre. Das von ihr mitunter angesprochene CVD-Prinzip

> s. zu diesem „Coordinated Vulnerability Disclosure" (CVD)-Verfahren die Antworten der Bundesregierung v. 03.06.2020 BT-Drs. 19/19753 S. 2f. zu Fragen 1.-4. und v. 22.06.2020 BT-Drs. 19/20245 S. 7 zu Frage 15. sowie ausführlich Householder/Wassermann/Manion/King, The CERT Guide to Coordinated Vulnerability Disclosure, 2017

will den Hersteller des Systems zur zügigen Beseitigung von Schwachstellen veranlassen, ist auf einen Ausgleich der unterschiedlichen öffentlichen und letztlich auch der Privatinteressen dagegen nicht ausgerichtet. Darum geht es beispielsweise in dem Vulnerabilities Equities Process, mit dessen Thema sich die Bundesregierung nach eigenen Angaben gleichfalls auseinandersetzt, ohne ihre Meinungsbildung bislang allerdings abschließen zu können.

Antwort v. 13.10.2017 BT-Drs. 18/13696 auf die Schriftliche Frage Nr. 25; die im Internet abrufbare Darstellung dieses Verfahrens (Vulnerabilities Equities Policy and Process for the United States Government. November 15, 2017, hier S. 2) beschreibt das Ausgangsproblem: „[...] vulnerability disclosure raises a multitude of considerations that require careful deliberation through an interagency process with a diversity of viewpoints. Competing USG missions require coordination und collaboration to protect information systems und citizens from malicious cyber activity. Additionally, the USG must be able to conduct law enforcement, military and intelligence activities to the fullest extent practical and in accordance with the laws that govern these activities." Ein Vorschlag zur Weiterentwicklung des Verfahrens findet sich bei Herpig, Schwachstellen-Management für mehr Sicherheit, Stiftung Neue Verantwortung, 2018.

Es mag sein, dass ein derartiges Verfahren den Anforderungen an ein Schutzkonzept genügt, das den verfassungsrechtlichen Maßstäben und ebenso den Bedürfnissen von Bund und Ländern in noch größerem Maße gerecht wird, als dies bei dem beschriebenen Meldeverfahren aufgrund des IT-Staatsvertrages der Fall ist. Zumindest lässt es erkennen, dass der Staat seiner Schutzpflicht für die Integrität informationstechnischer Systeme, soweit er den Umgang mit den von seinen Behörden genutzten Sicherheitslücken überhaupt regeln muss, nicht allein durch den schlichten Abgleich (landes-)polizeilicher Eingriffs- und privater Abwehrinteressen genügen kann. Vielmehr bedarf es, bevor Sicherheitslücken dem Hersteller eines Systems mitgeteilt oder öffentlich gemacht werden, eines alle Bundes- und Länderinteressen einbeziehenden Abwägungsverfahrens. Dessen Institutionalisierung ist indessen derart anspruchsvoll, dass sie allein Aufgabe des Bundes sein kann.

Unter diesen Umständen wird sich nicht feststellen lassen, dass Hessen im Zusammenhang mit der Zulassung der Quellen-TKÜ und der Online-Durchsuchung Grundrechte der Beschwerdeführer verletzt hat. Ihre Verfassungsbeschwerde wird daher erfolglos bleiben müssen.

Im Auftrag

gez. Prof. Dr. Günther