Bundesverfassungsgericht
Schloßbezirk 3
76131 Karlsruhe

Darmstadt, 03.07.2019
Mein Zeichen: 46/18 PS/al

Verfassungsbeschwerde

1. **des Herrn**
   Helge HERGET, Goerdelerstraße 112a, 63071 Offenbach am Main

2. **des Herrn**
   Gregory ENGELS, Parkstraße 61, 63067 Offenbach am Main

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

   Verfahrensbevollmächtigter zu 1) - 3):
   Rechtsanwalt Dr. Peter Spengler, Schleiermacherstraße 2, 64283 Darmstadt

   wegen:
   Verletzung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG

Unter Vorlage der Vollmachten zur Durchführung des Verfassungsbeschwerdeverfahrens zeige ich an, dass die Beschwerdeführer mich mit der Wahrnehmung ihrer Interessen beauftragt haben.

Namens und im Auftrag der Beschwerdeführer erhebe ich Verfassungsbeschwerde gegen:

> **§ 15b des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen**
>
> **§ 15c HSOG**
>
> **jeweils in Verbindung mit weiteren Vorschriften des HSOG**

und beantrage 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.**

Gliederung

A. Einleitung

Die Verfassungsbeschwerden richten sich gegen die Ermächtigung der hessischen Polizeibehörden zu verdeckten Eingriffen in informationstechnische Systeme. Die Befugnis, derartige Eingriffe zur Durchführung von Online-Durchsuchungen vorzunehmen, ist in Hessen mit der Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) im Zuge des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen vom 25.06.2018 (GVBl. I Nr. 13 vom 03.07.2018, S. 302, 319 ff.; nachfolgend nur: Gesetz vom 25.06.2018) erstmals geschaffen worden. Gleichzeitig ist die Befugnis der Polizeibehörden, verdeckte Eingriffe in informationstechnische Systeme zum Zweck der Telekommunikationsüberwachung vorzunehmen (Quellen-TKÜ), erheblich ausgeweitet worden.

Das Bundesverfassungsgericht hat bereits grundsätzlich über die Eingriffsschwellen für die heimliche Infiltration informationstechnischer Systeme entschieden. Insbesondere den Zugriff auf diese Systeme zum Zweck der Online-Durchsuchung hat das Gericht den Maßgaben des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme unterworfen, welches es Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG als Ausprägung des allgemeinen Persönlichkeitsrechts entnimmt.

BVerfGE 120, 274 (302 ff., 314 ff.); 141, 220 (303 ff.)

In Fortführung dieser Rechtsprechung bedarf es nach Auffassung der Beschwerdeführer, bezogen auf die Abwehrdimension des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer System, einer Nachschärfung der verfassungsrechtlichen Maßstäbe für die Durchführung verdeckter Eingriffe in informationstechnische Systeme.

Zudem fordert der den Eingriffen dienende Einsatz von Schadsoftware („Staatstrojaner“) zur Aktivierung dieses Grundrechts in seiner Wirkdimension als Schutzpflicht heraus. Der Staat hat einen Gewährleistungsauftrag für die sichere Nutzung informationstechnischer Systeme und die Verlässlichkeit digitaler Infrastrukturen. Mit dem staatlichen „Hacking“ verbinden sich jedoch ernsthafte Risiken. Vor allem dann, wenn zur heimlichen Infiltration der Zielsysteme digitale Sicherheitslücken offen gehalten werden, verstärkt der

Staat Gefahren für die Allgemeinheit und den Einzelnen, statt sie in Erfüllung seiner Schutzpflicht zu bekämpfen.

Das Bundesverfassungsgericht hat in diesem Zusammenhang bereits frühzeitig von einem Zielkonflikt gesprochen, der

> *„das Vertrauen der Bevölkerung beeinträchtigen (könnte), dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist“.*
>
> **BVerfGE 120, 274 (326)**

Die Beschwerdeführer machen daher geltend, dass die Bewältigung dieses Zielkonflikts als für den freiheitlichen Rechtsstaat und die Grundrechtsverwirklichung *wesentliche* Entscheidung dem Gesetzgeber obliegt. Dieser muss jedenfalls grundlegende Fragen des Umgangs mit digitalen Schwachstellen selbst regeln, wenn er Stellen der Exekutive zur heimlichen Infiltration informationstechnischer Systeme ermächtigt. Der hessische Gesetzgeber hat dies jedoch – wie im Zuge gleichartiger Ermächtigungen auch der Bundes- und andere Landesgesetzgeber – unterlassen. Zudem hat er es versäumt, eine wirksame Kontrolle der grundrechts- und sicherheitsrelevanten Eigenschaften des „Hessentrojaners“ gesetzlich sicherzustellen.

B. Sachverhalt

I. Die Ermächtigung zu verdeckten Eingriffen in informationstechnische Systeme durch das HSOG

1. Gang der Gesetzgebung

Im Zuge der Verfassungsschutzreform in der 19. Wahlperiode des Hessischen Landtags beabsichtigten die Koalitionsfraktionen von CDU und Bündnis 90/Die Grünen, das Landesamt für Verfassungsschutz mit Befugnissen zur Durchführung der Quellen-TKÜ sowie von Online-Durchsuchungen auszustatten.

> **Art. 1 §§ 6 Abs. 2 bis 4, 8 des Gesetzentwurfs der Fraktionen der CDU und Bündnis 90/Die Grünen für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen vom 14.11.2017, LT-Drs.19/5412, S. 8, S. 9.**

Nach Kritik aus der Öffentlichkeit und der Opposition und angesichts erheblicher Bedenken der vor dem Innenausschuss des Landtags angehörten Experten

> **Ausschussvorlage INA 19/63 vom 30.01.208; Ausschussprotokoll INA 19/86 vom 06.03.2018**

erfuhr das Vorhaben eine Abwandlung. Ein Änderungsantrag im laufenden Gesetzgebungsverfahren überführte die Rechtsgrundlagen der Quellen-TKÜ und der Online-Durchsuchung aus dem Entwurf eines neuen Hessischen Verfassungsschutzgesetzes nunmehr als polizeiliche Befugnisse in die Bestimmungen zu begleitenden Änderungen des HSOG.

> **Ziffer 4.a) 2e, 2f des Änderungsantrags der Fraktionen der CDU und Bündnis 90/Die Grünen vom 05.06.2018 zu dem Gesetzentwurf der Fraktionen der CDU und Bündnis 90/Die Grünen für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen Drucksache 19/5412, LT-Drs. 19/6502, S. 16 f.**

Ziffer 4.a) 2e des Änderungsantrags vom 05.06.2018 betraf die Änderung des § 15b HSOG, welcher schon zuvor durch das Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze vom 14.12.2009 (GVBl. I Nr. 21 vom 22.12.2009, S. 635, 637;

nachfolgend: Gesetz vom 14.12.2009) als Rechtsgrundlage einer Quellen-TKÜ geschaffen worden war, und sah neben rechtstechnischen Anpassungen insbesondere eine Ausweitung des Anwendungsbereichs dieser Maßnahme vor.

Ziffer 4.a) 2f des Änderungsantrags betraf die Einfügung des § 15c in das HSOG als Rechtsgrundlage der Online-Durchsuchung.

Mit diesen und weiteren Änderungen wurde der Entwurf des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen am 19. und 21.06.2018 in zweiter und dritter Lesung im Hessischen Landtag beraten und das Gesetz schließlich mit den Koalitionsstimmen beschlossen. Nach Ausfertigung am 25.06.2018 wurde es am 03.07.2018 verkündet (GVBl. I Nr. 13 vom 03.07.2018, S. 302). Gemäß seinem Artikel 5 ist es am 04.07.2018 in Kraft getreten.

2. Die angegriffenen Befugnisnormen

Angriffsgegenstand der vorliegenden Verfassungsbeschwerde sind die hiernach durch Art. 3 Nr. 2e des Gesetzes vom 25.06.2018 neu gefasste Befugnisnorm für die Quellen-TKÜ, § 15b HSOG, sowie die durch Art. 3 Nr. 3f des Gesetzes vom 25.06.2018 erstmals geschaffene Befugnisnorm für Online-Durchsuchungen, § 15c HSOG, jeweils in Verbindung mit weiteren Vorschriften des HSOG, welche über ein Geflecht von Verweisungen und Bezugnahmen in die Regelung der Zulässigkeitsvoraussetzungen und Anforderungen an die Durchführung der genannten Maßnahmen einbezogen sind.

a. § 15b HSOG (Quellen-TKÜ)

aa. § 15b HSOG in der Fassung des Gesetzes vom 25.06.2018 lautet:

> *„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) 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.*

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

(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."

Der in Absatz 1 Halbs. 1 der Vorschrift in Bezug genommene § 15a Abs. 1 HSOG regelt die herkömmliche Telekommunikationsüberwachung unter Mitwirkung von Dienstanbietern. Diese ist gemäß § 15a Abs. 1 Satz 1 Halbs. 2 HSOG in der Fassung von Art. 3 Nr. 2d a) des Gesetzes vom 25.06.2018 zulässig,

„(…), wenn (sie) 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 Menschheit berührt, unerlässlich ist."

Dabei regelt § 15a Abs. 1 Satz 2 HSOG unter Bezugnahme auf weitere Vorschriften des HSOG, gegen welche Personen sich die Maßnahme richten darf. Dies sind zunächst die Verantwortlichen gemäß den allgemeinen Bestimmungen über die Störereigenschaft in den §§ 6 und 7 HSOG sowie nicht verantwortliche Personen unter den Voraussetzungen des § 9 HSOG (§ 15a Abs. 1 Satz 2 Nrn. 1 und 2 HSOG). Zielperson der Maßnahmen kann gemäß

§ 15b Abs. 1 Satz 1 i.V.m. § 15a Abs. 1 Satz 2 HSOG zudem eine Person sein,

> *„bei der bestimmte Tatsachen die Annahme rechtfertigen,*
>
> *dass sie für (eine verantwortliche Person) bestimmte oder von dieser herrührende Mitteilungen entgegennimmt oder weitergibt“* (§ 15a Abs. 1 Satz 2 Nr. 3 a) HSOG)

oder dass

> *„eine (verantwortliche Person) deren Telekommunikationsanschluss oder Endgerät benutzten wird, soweit die Maßnahme zur Verhütung terroristischer Straftaten unerlässlich ist“* (§ 15a Abs. 1 Satz 2 Nr. 3 b) HSOG),

zudem eine Person,

> *„die in § 15 Abs. 2 Satz 1 Nr. 2 oder 3 genannt ist, soweit die Maßnahme zur Verhütung terroristischer Straftaten unerlässlich ist.* (§ 15ab Abs. 1 Satz 2 Nr. 4 HSOG).

Über letztere Verweisung sind Personen einbezogen, bei denen

> *„bestimmte Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat mit erheblicher Bedeutung begehen werden, und (die Maßnahme) zur Verhütung dieser Straftat erforderlich ist,“* (§ 15 Abs. 2 Satz 1 Nr. 2 HSOG)

oder

> *„deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines überschaubaren Zeitraums eine terroristische Straftat begehen werden, und (die Maßnahme) zur Verhütung dieser Straftat erforderlich ist“* (§ 15 Abs. 2 Satz 1 Nr. 3 HSOG).

§ 15a Abs. 1 Satz 3 HSOG bestimmt, dass die Maßnahme auch durchgeführt werden darf, wenn andere Personen unvermeidbar betroffen werden.

Durch die Anordnung der entsprechenden Geltung anderer Vorschriften in § 15b Abs. 3 HSOG sind schließlich – zum Teil über mehrfache Weiterverweisung – die eingeschränkte Zulässigkeit von Maßnahmen gegenüber Personen, für welche die Voraussetzungen von Zeugnisverweigerungsrechten nach den §§ 52 bis 55 der Strafprozessordnung vorliegen, der Schutz des Kernbereichs privater Lebensgestaltung sowie die richterliche Anordnung der Maßnahmen geregelt.

bb. Bis zum Inkrafttreten des Gesetzes vom 25.06.2018 regelte § 15b Abs. 1 HSOG in der Ursprungsfassung des Gesetzes vom 14.12.2009 (GVBl. I S. 635, 637) die tatbestandlichen Voraussetzungen der Quellen-TKÜ wie folgt:

> *„(1) Wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib und 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, (…)“*.

Neu ist hiernach die Befugnis, die Quellen-TKÜ zusätzlich auch dann vornehmen zu dürfen, wenn sie zur Abwehr einer dringenden Gefahr

> *„für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschheit berührt.“* (§ 15b Abs. 1 Halbs. 1 i.V.m. § 15a Abs. 1 Satz 1 HSOG n.F.).

Zudem wurde durch die Änderung des Gefahrenbegriffs – nun *dringend* anstelle von bisher *gegenwärtig* – der Anwendungsbereich in ein früheres Stadium der Gefahrenentstehung ausgedehnt.

Zu den Adressaten der Maßnahme hieß es bis zu der jetzt erfolgten Gesetzesänderung in 15b Abs. 3 HSOG in der Fassung des von Art. 18 Nr. 9a des Hessischen Gesetzes zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit vom 03.05.2018, GVBl. I S. 81 (149):

> *„Die Maßnahme darf sich nur gegen eine Person richten, die nach den §§ 6 oder 7 verantwortlich ist. Sie darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.“*

Durch die Bezugnahme des neugefassten § 15b Abs. 1 auf § 15a Abs. 1 Satz 2 HSOG n.F. einschließlich der dortigen Weiterverweisungen ist mithin auch der Kreis möglicher Zielpersonen der Quellen-TKÜ deutlich ausgeweitet worden.

b. § 15c HSOG (Online-Durchsuchung)

§ 15c HSOG lautet:

> *„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 dir Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschheit berührt, unerlässlich ist.*
>
> *(2) 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. Eine Maßnahme nach Abs. 1 ist auch gegen eine nach § 15 Abs. 2 Satz 1 Nr. 2 oder 3 genannte Person zulässig, soweit dies zur Verhütung terroristischer Straftaten unerlässlich ist. 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. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.*
>
> *(3) § 15b Abs. 2 gilt entsprechend. § 15 Abs. 4 Satz 4 bis 6 gilt entsprechend mit der Maßgabe, dass, soweit möglich, technisch sicherzustellen ist, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. § 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 für Erkenntnisse, die nach Abs. 1 und 2 erlangt worden sind.“*

c. Ergänzende Regelungen

Ergänzende Regelungen zu den Befugnissen nach §§ 15b, 15c HSOG sind insbesondere in den §§ 17a HSOG (Berichtspflichten gegenüber dem Hessischen Landtag und der Öffentlichkeit), 20 bis 29a HSOG (Datenverarbeitung) HSOG enthalten, die durch das Gesetz vom 25.06.2018 Änderungen und Erweiterungen erfahren haben.

II. Die Beschwerdeführer

1. Beschwerdeführer zu 1)

Der Beschwerdeführer zu 1) nutzt das Internet – neben der beruflichen Nutzung über IT-Systeme seines Arbeitsgebers – für seine persönlichen Angelegenheiten sowie politische und gesellschaftliche Aktivitäten.

Er ist Vorsitzender des Kreisverbands Offenbach Stadt und Land der Piratenpartei und kandidierte im Jahr 2017 zur Wahl des Oberbürgermeisters in Offenbach am Main. Im Rahmen seiner politischen Betätigung administriert er die Internetseite „piraten-offenbach.de“ sowie die Auftritte des Kreisverbands bei Facebook und Twitter. Zudem betreut er die zentralen E-Mail-Accounts mit Mailinglisten für Rundschreiben und den Account des Kreisverbands bei dem Messenger-Dienst Telegram.

Zu seiner Internetnutzung im persönlichen Bereich gehören insbesondere private E-Mail-Korrespondenz, Kommunikation über Telegram sowie das Online-Banking. Darüber hinaus administriert er gemeinsam mit seiner Ehefrau die Internetseite „tango-diavolo.de“. An diese ist ebenfalls eine Mailingliste angegliedert, über die er Rundbriefe zu dem Interessengebiet Tango Argentino versendet.

Die außerberufliche Internetnutzung des Beschwerdeführers zu 1) erfolgt vor allem über einen „Familien-PC“, auf den neben ihm seine Ehefrau und sein Sohn Zugriff haben, sein Smartphone sowie die Mitbenutzung eines Laptops seiner Ehefrau, die als Vorstandsmitglied des Beschwerdeführers zu 3) und in anderen Parteifunktionen ebenfalls politisch aktiv ist. Seine Telegramm-Nachrichten sind zwischen den drei genannten Geräten synchronisiert.

2. Beschwerdeführer zu 2)

Der Beschwerdeführer zu 2) ist Stadtverordneter in Offenbach am Main und betätigt sich als politischer Aktivist auf nationaler, europäischer und internationaler Ebene. Er ist Beauftragter der Piratenpartei Deutschland für internationale Zusammenarbeit, Mitglied im Vorstand des internationalen Dachver-

bands der Piratenparteien (Pirate Parties International - PPI) und Mitglied der deutschen Delegation bei der Europäischen Piratenpartei (European Pirate Party). In diesen Funktionen steht er in regelmäßigem engem Kontakt mit Aktivisten anderer Piratenparteien. Er unterhält gerade auch Kontakte zu Dissidenten in autoritär geführten Staaten.

Besondere Schwerpunkte sind die Zusammenarbeit mit Partnern in Russland, weiteren osteuropäischen Ländern und dem nordafrikanischen Raum.

So unterstützte der Beschwerdeführer zu 2) die Piratenpartei Russland bei der Gründung und nahm an der Gründungsveranstaltung in Moskau teil. Zusammen mit russischen Aktivisten betrieb er die Internetseite „Ruleaks.net“ als Portal für anonyme Whistleblower-Veröffentlichungen. Als Inhaber der Domain „rublaklist.net“ führt er vor dem Europäischen Gerichtshof für Menschenrechte ein Verfahren (Az. 61919/16) gegen die Russische Föderation wegen der gerichtlich angeordneten Blockade dieser Seite, die von der Nichtregierungsorganisation RosKomSvoboda („Russisches Komitee für die Freiheit“) für die Berichterstattung über russische Netzsperren sowie für Anleitungen zu deren Umgehung genutzt wird.

Hierzu: https://www.politikexpress.de/pirat-verklagt-russland-vor-dem-europaischen-gericht-furmenschenrechte-1533008.html; aufgerufen am 01.07.2019

Intensive Kontakte unterhält der Beschwerdeführer zu 2) auch nach Kasachstan. Im Jahr 2012 war er Beobachter des Prozesses gegen den ehemaligen Präsidentschaftsbewerber Vladimir Kozlov. Seitdem steht er in regelmäßiger Verbindung mit Oppositionspolitikern des Landes, darunter bis zu dessen Tod im Jahr 2015 der vormalige Spitzenpolitiker und Diplomat Rachat Älijew. Mit Aktivisten in Marokko, Libyen und Tunesien tauschte er sich insbesondere während der Unruhen des „Arabischen Frühlings“ aus.

Der Beschwerdeführer zu 2) hat durch die hier beispielhaft genannten Aktivitäten das Interesse verschiedener Geheimdienste auf sich gezogen. Seine Wohnung in Offenbach war bereits Ziel eines Einbruchs, bei dem im Jahr 2016 lediglich ein Laptop entwendet wurde. Zahlreiche Veranstaltungen, an denen er im Ausland teilgenommen hat, standen unter geheimdienstlicher Beobachtung, beispielsweise die im Februar 2013 von der UNESCO in Marrakesch ausgerichtete Tagung „Freedom and Expression of the Internet“

und die Konferenz der PPI in Kazan im Jahr 2015. Keinem Zweifel unterliegt zudem die geheimdienstliche Beobachtung vieler seiner Kontaktpersonen.

Für die Kommunikation mit seinen Kontakten nutzt der Beschwerdeführer zu 2) eine Vielzahl von Kanälen, wobei jeweils das Internet von essenzieller Bedeutung ist. Die wichtigsten Nachrichten werden stets verschlüsselt übertragen. Für die Verschlüsselung von E-Mails nutzt er das Programm „Pretty Good Privacy“ (PGP). Telefonate werden über den Messenger Signal geführt. Dabei wird die Audiokommunikation ende-zu-ende verschlüsselt. Zudem greift der Beschwerdeführer zu 2) auf Torbrowser – um bestimmte Netzsperren in Russland und Kasachstan zu umgehen – sowie auf weitere Tools zurück. Hinsichtlich der eingesetzten Geräte besteht seine IT-Ausstattung derzeit aus zwei MacBook Pro-Notebooks, einem Windows 10 Netbook, einem iPpad Pro und einem iPhone X.

3. Beschwerdeführer zu 3)

Der Beschwerdeführer zu 3) ist der Gebietsverband der Piratenpartei Deutschland auf Landesebene in Hessen.

Die Piratenpartei betrachtet die Kommunikation über digitale Netzwerke wie das Internet angesichts der digitalen Revolutionierung aller Lebensbereiche als essenziell für die soziale Teilhabe sowie die politische Mitwirkung am Ausbau des demokratischen Rechtsstaats und der Gestaltung einer modernen freiheitlichen Gesellschaftsordnung unter den Bedingungen des 21. Jahrhunderts.

Für seine politische Arbeit bedient sich der Beschwerdeführer zu 3) selbst bereits in hohem Maße digitaler Kommunikationsformen und insbesondere auch der Vernetzung über das Internet. Dies betrifft zum einen die innerparteiliche Kommunikation in allen inhaltlichen und organisatorischen Belangen der Parteiarbeit sowie die Arbeit der kommunalen Mandatsträger, zum anderen das politische Wirken in die Öffentlichkeit und den Dialog mit dieser.

Die IT-Infrastruktur des Beschwerdeführers zu 3) umfasst daher verschiedene Anwendungen (Tools) für die Zusammenarbeit, Kommunikation und die Bereitstellung von Informationen im Internet. Die Funktionen einer physisch eingerichteten Geschäftsstelle werden durch diese Tools weitgehend ersetzt, da sie eine in örtlicher Hinsicht dezentrale Zusammenarbeit der Vorstandsmitglieder, Beauftragten und sonstigen – etwa an einzelnen Projekten – Beteiligten aus der Mitgliedschaft und der interessierten Öffentlichkeit erlauben.

Kennzeichnend ist insoweit das nahezu vollständige Fehlen eigener Hardware des Beschwerdeführers zu 3). Die von ihm genutzten Programme sind auf Servern eines Hosting-Unternehmens in Süddeutschland installiert. Die an der Parteiarbeit beteiligten Personen und sonstigen Interessenten greifen darauf über ihre jeweiligen individuellen (privaten) Endgeräte zu.

Je nach Funktion und Einsatzzweck bestehen unterschiedliche Grade des öffentlichen oder beschränkten Zugangs zu den Tools und den mit diesen verarbeiteten Daten. Beim Zuschnitt der Zugangsberechtigungen folgt der Beschwerdeführer zu 3) neben organisatorischen Erfordernissen gerade auch seinen politischen Maximen, wonach informationelle Selbstbestimmung, Transparenz, freier Zugang zu Wissen und Kultur sowie die Wahrung von Privatsphäre und Persönlichkeitsrechten Grundpfeiler einer freiheitlichen Informationsgesellschaft sind.

Neben seiner Internetpräsenz unter der Domain „piratenpartei-hessen.de“ unterhält der Beschwerdeführer zu 3) eine unbeschränkt zugängliche Informationssammlung („Wiki“) unter der Adresse https://wiki.piratenpartei.de/HE:Landesverband. Weiterhin unterhält er über die Bundesorganisation der Piratenpartei ein für Jedermann benutzbares Diskussionsforum unter der Adresse https://forum.piratenpartei.de/.

Eine zugangsbeschränkte Anwendung sind die von dem Beschwerdeführer zu 3) genutzten Cryptpads. Hierbei handelt es sich um verschlüsselte Dateien zur gemeinsamen Nutzung durch mehrere Teilnehmer, die über ein Link von der Seite https://cryptpad.piratenpartei.de/drive/# angesteuert werden. Der Schlüssel ist in dem vollständigen Link der jeweiligen einzelnen Datei enthalten. Internetnutzer, die den Link kennen bzw. zugeleitet bekommen haben, erlangen Zugang zu der betreffenden Datei. Der Vorstand des Be-

schwerdeführers zu 3) schreibt mit Cryptpad beispielsweise bei Telefonkonferenzen ein gemeinsames Protokoll.

Das Tool Cryptpad ist in der Parteiarbeit des Beschwerdeführers zu 3) inzwischen vollständig an die Stelle der zuvor genutzten „Piratenpads“ getreten. Basierend auf dem Tool „Etherpad“ wiesen diese hinsichtlich der kollaborativen Dokumentenbearbeitung eine vergleichbare Funktionalität auf, waren jedoch ohne Verschlüsselung über das Internet zugänglich. Die Manipulation eines Piratenpads durch Unbekannte hatte im Jahr 2011 bei den französischen Sicherheitsbehörden zu der Besorgnis eines Cyberangriffs auf den Energiekonzern EDF über die IT der Piratenpartei Deutschland geführt und eine umfassende Durchsuchung ihrer damals in Offenbach gehosteten IT-Landschaft durch die Staatsanwaltschaft Darmstadt ausgelöst (zu den als „Servergate“ bekannt gewordenen Vorgängen unten noch, C.III.2.c.cc).

Weitere von dem Beschwerdeführer zu 3) genutzte Tools, die eine gemeinsame Bearbeitung von Schriftstücken, Plänen, Prozessdiagrammen (Workflows) und ähnlichem ermöglichen, sind die Verwaltungs- und Projektmanagementprogramme „Redmine“ und „Confluence“.

Redmine findet etwa Einsatz für die öffentliche oder vertrauliche Durchführung von Abstimmungen, Confluence für das Erstellen und Bearbeiten politischer Papiere. Die Tools werden über die Webadressen https://redmine.piratenpartei-hessen.de und https://confluence.piratenpartei-hessen.de geöffnet, wobei der freie oder beschränkte Zugriff auf einen einzelnen Vorgang durch die Vergabe von Zugangsberechtigungen bzw. den Verzicht darauf gesteuert werden. Ein vergleichbares Tool für die arbeitsteilige Erstellung oder Bearbeitung von Software ist das von den IT-Betreuern des Beschwerdeführers zu 3) genutzte Programm „Jira“ (https://jira.piratenpartei-hessen.de).

Darüber hinaus verwendet der Beschwerdeführer zu 3) die Foren- und Kommunikationssoftware „Mattermost“ (https://mattermost.piratenpartei.de/), die Sprachkonferenzsoftware „Mumble“ (https://mumble.piratenpartei-nrw.de), ein Diskussionstool zur Gegenüberstellung von gewichteten Pro- und Contra-Argumenten (https://wikiarguments.piratenpartei-hessen.de), ein Tool zur Abfrage von Meinungsbildern (vMb - virtuelles Meinungsbild,

https://wiki.piratenpartei.de/HE:Meinungsbilder) sowie „Owncloud“ als gemeinsamen Speicher für vorläufige oder vertrauliche Dateien mit individuellen Zugangsrechten.

Der Vorstand des Beschwerdeführers zu 3) führt Telefonkonferenzen über den Telefonserver https://sip.piratenpartei-hessen.de.

Bei dem Hosting-Anbieter ist ein eigener Mailserver des Beschwerdeführers zu 3) eingerichtet. Jedes Parteimitglied kann dort einen Mailaccount bekommen mit der einheitlichen Domainendung des Beschwerdeführers zu 3). Darüber hinaus gibt es verschiedene Funktionsaccounts, etwa vorstand@piratenpartei-hessen.de. Dort eingehende Mails werden automatisch an alle Vorstandsmitglieder weitergeleitet. Wichtige Mails und alle Mails, die personenbezogene Daten enthalten, werden mit dem Programm PGP verschlüsselt. Im Zuge der Parteiarbeit werden verschiedene Mailinglisten bedient und gepflegt.

Die beschriebene dezentrale Ausgestaltung der IT-Landschaft des Beschwerdeführers zu 3) bringt es mit sich, dass es sich bei den individuellen Endgeräten um PCs, Tablets, Smartphones usw. von sehr unterschiedlicher Art und Konfiguration handelt. Entsprechendes gilt in Bezug auf die jeweiligen Betriebssysteme; insoweit werden Windows- und Linux-Versionen sowie das Apple-Betriebssystem MacOS und Android verwandt.

III. Implikationen der heimlichen Infiltration informationstechnischer Systeme durch staatliche Sicherheitsbehörden

Die Beschwerdeführer sind besorgt wegen der zunehmenden staatlichen Überwachung des Internets und ihrer Betroffenheit von den eine große Streubreite aufweisenden Maßnahmen nach §§ 15b, 15c HSOG, aber auch wegen der durch diese Vorschriften implizierten strukturellen Schwächung der IT-Sicherheit, welche die Vertraulichkeit und Integrität informationstechnischer Systeme unterminiert.

1. Unterminierung der Vertraulichkeit und Integrität informationstechnischer Systeme

Diese Problematik ist Gegenstand einer umfangreichen Debatte in und zwischen verschiedenen Disziplinen (und ausweislich u.a. der oben, A., zitierten Ausführungen in BVerfGE 120, 274 (326) durchaus gerichtsbekannt). Sie wurde dem hessischen Gesetzgeber während der Beratungen des Gesetzes vom 25.06.2018 eindringlich vor Augen geführt.

> **Vorlage für den Innenausschuss, INA 19/63, Januar/Februar 2018, mit Stellungnahmen u.a. von: *Chaos Computer Club* (CCC), INA 19/63 Teil 3, S. 290; *dieDatenschützer Rhein Main*, INA 19/63 Teil 2, S. 181 (184 f.); *Roggenkamp*, INA 19/63 Teil 3, S. 262 (268 f.); *Rehak*, INA 19/63 Teil 3, S. 389 (401 ff., 406 f.); *Federrath*, INA 19/63 Teil 3, S.410 ff.; Protokoll des Anhörung vor dem Innenausschuss vom 08.02.2018, INA 19/86 mit Beiträgen von *Kurz*, S. 60 (62); *Peters,* S. 64; *Rehak*, S. 64 (65 f.), S. 84 ff.; *Kurz*, S. 78 (79 ff.); *Peters*, S. 81 ff.; *Erkmann*, S. 83 f.**

In der Stellungnahme des CCC zu dem Entwurf des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen in der Fassung der Landtagsdrucksache 19/5412 heißt es etwa:

> *„(…) Hier wird ein genereller Konflikt offenkundig, in den sich der hessische Gesetzgeber begibt: Spionagesoftware benötigt eine Schwachstelle im angegriffenen Computersystem, die vom Besitzer des Systems nicht geschlossen wurde und daher heimlich genutzt werden kann. Jeder Einsatz eines Staatstrojaners erfordert, dass eine Schadkomponente unbemerkt bei der verdächtigten Person installiert wird. Denn eine Sicherheitslücke sowie der Schadcode bilden das Einfallstor für die Spionagesoftware.*
>
> *Erfahren die Hersteller oder die Entwickler der betreffenden Software von einer solchen Schwachstelle, steht in der Regel nach kurzer Zeit eine Aktualisierung bereit, welche die Lücke schließt. Durch das absichtliche Offenhalten von Schwachstellen untergräbt der Staat jene Vertrauenswürdigkeit, die er eigentlich zu schützen hat.*
>
> *Zudem schafft er erhebliche sekundäre Gefahren. Werden Lücken nicht geschlossen, entsteht ein enormer Schaden für die IT-Sicherheit bei Privatleuten und Unternehmen. (…).*
>
> *Seit die Diskussion in Deutschland um die Einführung einer gesetzlichen Erlaubnis zum staatlichen Hacken vor mehr als zehn Jahren begann, hat sich das Gesamtbild in der IT-Sicherheit und bezüglich der Verbreitung, des Handels und der Abwehr von Schadsoftware stark gewandelt. In der jüngeren Vergangenheit ist Schadsoftware in*

zunehmendem Maße in die Hände Krimineller gelangt. Diese haben die Sicherheitslücken, die von staatlicher Seite geheimgehalten worden waren, genutzt, um in großem Umfang Computer mit Erpressungstrojanern zu infizieren. (…)

Die internationalen Schadenssummen durch Spionagesoftware, welche von staatlichen Akteuren oder in deren Auftrag entwickelt wurde, sind stark gestiegen und liegen im Bereich von vielen Millionen Euro jedes Jahr. Nicht gemeldete Sicherheitslücken gelangten in die Hände von Dritten und schädigten in der Folge Millionen Computersysteme. Im Jahr 2017 richtete die bislang größte Welle von Schadsoftware, die aus einem staatlichen Arsenal entwendet wurde, unter dem Namen ‚Wannacry' bei Unternehmen, Behörden und Privatleuten enormen Schaden an. Vergleichbares gilt für die Angriffswelle mit der Malware ‚NotPetya'. Die Schadenssumme allein für ‚Wannacry' wird international auf über vier Milliarden Euro taxiert. Alarmierend ist dabei die Tatsache, dass in Großbritannien insbesondere Krankenhausinfrastrukturen davon betroffen und Leben und Leben und Gesundheit von Menschen gefährdet waren.

(…) Die Regelungen des Gesetzentwurfs implizieren das absichtliche Offenhalten von Sicherheitslücken in IT-Systemen durch staatliche Stellen. Gleichzeitig wird allerdings die eigentlich zwingend notwendige Einschätzung der Folgeschäden unterlassen und auch für den Einzelfall nicht im Gesetzentwurf vorgesehen.

Für den Einsatz in einem Staatstrojaner sind Sicherheitslücken in besonders weit verbreiteter Software attraktiv, etwa in gängigen Betriebssystemen (Windows, Android, iOS) oder Browsern (Chrome, Firefox): Hiermit können viele verschiedene Geräte angegriffen werden, ohne den Staatstrojaner grundlegend umprogrammieren zu müssen.

Für Kriminelle sind solche Lücken aus dem selben Grund ebenfalls interessant. Es existiert daher ein florierender Grau- und Schwarzmarkt, auf dem Informationen über Sicherheitslücken gehandelt werden. Der Staat gerät hier folglich in einen Zielkonflikt: Auf der einen Seite will er ein möglichst hohes IT-Sicherheitsniveau für Bürger und Wirtschaft garantieren; auf der anderen Seite hat er ein großes Interesse an offenen Sicherheitslücken in möglichst vielen und verbreiteten Systemen, um diese bei Bedarf zum Zwecke der ‚Online-Durchsuchung' oder ‚Quellen-TKÜ' ausnutzen zu können.

(…) Da staatliche Akteure Geld für Informationen über noch unbekannte Sicherheitslücken ausgeben, um diese Lücken für Staatstrojaner nutzen zu können, wächst das Volumen der Schwarzmärkte, auf denen diese Informationen gehandelt werden. Die Hersteller der verwundbaren Software können diese Lücken eigentlich zum Schutz aller Nutzer bei Kenntnis durch Update schließen. Da die Informationen über Existenz und Art der Lücke auf dem Schwarzmarkt jedoch oftmals an den Meistbietenden für bis zu sechs- oder siebenstellige Eurobeträge verkauft werden, erfahren Softwarehersteller nicht von kritischen Lücken in ihren Produkten. Alle ihre Kunden bleiben damit verwundbar.

Staatliche Schadsoftware unterminiert die IT-Sicherheit damit strukturell, da ihre Entwicklung Anreize dafür setzt, Sicherheitslücken anzubieten, zu verkaufen und nicht schließen zu lassen. (…) Durch die Finanzierung und damit einhergehende Setzen falscher Anreize beim Umgang mit Sicherheitslücken hat sich bereits eine ganze Branche entwickelt, die aktiv unser aller Sicherheit gefährdet und die Wirtschaft sowie öffentliche Stellen buchstäblich viele Millionen kostet. Eine verantwortungsvolle Sicherheitsstrategie zielt auf die Schließung von Lücken ab, statt sich an der fragwürdigen Praxis des Handels mit Schwachstellen noch zu beteiligen und indirekt kriminelle Händler zu unterstützen.

Der Gesetzentwurf gibt keine Anhaltspunkte dafür, dass die dargestellten Risiken der Schadsoftware minimiert werden. (…)

An einem Großteil der heute verbreiteten Schadsoftware, die entdeckt und analysiert wurde, waren staatliche Stellen beteiligt, ob als Auftraggeber oder direkt bei der Entwicklung. Die bisher gefährlichsten bekannten Digitalwaffen (‚Stuxnet', ‚Flame', ‚Duqu' und ‚Regin') sind allesamt in staatlichem Auftrag entstanden. (…)

Prinzipiell ist das Ausnutzen von Sicherheitslücken von staatlicher Seite nicht wünschenswert, da es im Interesse aller Behörden liegen sollte, diese Lücken zeitnah und konsequent schließen zu lassen. Das Interesse von Behörden muss es nicht nur sein, die eigenen Systeme zu sichern, sondern auch Folgeschäden ihres Tuns für Wirtschaft und Privatpersonen zu vermeiden. Einem Fortbestand von Sicherheitslücken, die staatlichen Stellen bekannt geworden sind, muss daher konsequent entgegengewirkt werden. Dazu muss im Gesetzentwurf insbesondere eine Meldepflicht (…) aufgenommen werden, insbesondere bei Sicherheitslücken, die die in weitverbreiteter und sicherheitskritischer Software bestehen. Solche Lücken stellen eine enorme Gefahr für eine große Zahl von Geräten dar."

***Kurz/Holz/Hoffmann/Laufenberg*, in: CCC, a.a.O., S. 290 (292 ff.)**

Nach der Verschiebung der Rechtsgrundlagen für die Online-Durchsuchung und die Quellen-TKÜ in den Entwurf zur Änderung des HSOG hat eine neuerliche Expertenanhörung nicht stattgefunden. Die Bedenken des CCC und – im Wesentlichen übereinstimmend – einer Reihe weiterer Institutionen und Experten zu den §§ 6 (Quellen-TKÜ) und 8 (Online-Durchsuchung) der ursprünglichen Entwurfsfassung des Hessischen Verfassungsschutzgesetzes treffen jedoch im Wesentlichen auch auf die Gesetz gewordenen §§ 15b, 15c HSOG zu.

2. Maßgaben für ein Schwachstellenmanagement

Zur gebotenen Einhegung der durch die Infiltration informationstechnischer Systeme implizierten Bedrohungen gehen die Beschwerdeführer von einem

Gestaltungsauftrag des Gesetzgebers aus, dem es von verfassungs wegen verwehrt ist, den Polizeibehörden derartige Befugnisse zu verleihen, ohne 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.

Informationstechnischer Ausgangspunkt der Überlegungen für ein notwendiges Schwachstellenmangement sind die technischen Bedingungen für die heimliche Infiltration informationstechnischer Systeme: Überwachungssoftware kann entweder während eines direkten physischen Zugriffs auf das Zielsystem aufgespielt werden oder aus der Ferne unter Ausnutzung von Schwachstellen des Zielsystems.

Unter Schwachstellen wird dabei verstanden, was etwa das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) als „Sicherheitslücke“ definiert ist, nämlich

> *„(…) 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 System verschaffen oder die Funktion der informationstechnischen System beeinflussen können“* (´§ 2 Abs. 6 BSIG).

Eine im Wesentlichen bedeutungsgleiche Begriffsbestimmung lautet:

> *„Fehler in Hard- oder Software, die jeweils einzeln oder in Verkettung mit anderen Schwachstellen Dritten die Ausnutzung eines Systems ermöglichen, um unautorisiert, und vom Systeminhaber unter Umständen unbemerkt, ein oder mehrere Geräte oder Online-Dienste zu manipulieren.“*
>
> ***Harpig*, Schwachstellenmanagement für mehr Sicherheit – wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte, hrsg. von der Stiftung Neue Verantwortung, August 2018; https://www.stiftung-nv.de/de/publikation/schwachstellen-management-fuer-mehr-sicherheit , Aufruf am 02.07.2019, S. 9**

Grundlegend ist die Unterscheidung zwischen *Zero-Day*-Schwachstellen (unbekannte und daher besonders gefährliche Schwachstellen) und *N-Day*-Schwachstellen (bekannte Schwachstellen).

Zero-Days sind Schwachstellen, die weder dem jeweiligen Betreiber oder Hersteller (Maintainer) noch der Öffentlichkeit bekannt sind. Damit besteht keine Abhilfe (Patch) zur Behebung der Schwachstelle und kein schadensbegrenzender Mechanismus (Mitigation) durch den jeweiligen Maintainer zur Verfügung. Dadurch ist die Schwachstelle äußerst potent für Angreifer und und extrem gefährlich für entsprechend verwundbare Systeme. Mehrere Akteure, etwa Sicherheitsbehörden, können unabhängig voneinander Wissen von ein- und derselben Schwachstelle erhalten haben, ohne zu wissen, dass auch die andere Seite sie Schwachstelle kennt. Gegnerische Nachrichtendienste oder Kriminelle können so parallel offene Zero-Day-Schwachstellen ausnutzen. Unabhängig davon, ob eine solche Schwachstelle ausgenutzt wird oder nicht, bleibt sie eine Zero-Day-Schwachstelle bis zu dem Zeitpunkt, an dem der betroffene Maintainer informiert ist.

***Harpig*, a.a.O., S. 10**

N-Days sind Schwachstellen, die dem Maintainer bekannt sind. Das bedeutet nicht, dass er bereits ein Patch zum Schließen der Schwachstelle entwickelt hat oder dass er grundsätzlich plant, sie zu schließen. Typischerweise tritt das letztgenannte Szenario auf, wenn ein Produkt bereits das Ende seines Lebenszyklus erreicht hat, nicht mehr hergestellt wird, wenn es keinen hauptverantwortlichen Maintainer gibt, dieser nicht die Fähigkeit hat, einen Patch zu entwickeln, nicht existiert oder schlicht kein Interesse hat, die Schwachstelle zu schließen.

***Harpig*, a.a.O., S. 10 f.**

Harpig formuliert die Maßgaben für ein Schwachstellenmanagement wie folgt:

> *„(…) Schwachstellen bilden den Kern offensiver Aktivitäten im Cyber-Raum wie zum Beispiel Hacking durch Strafverfolgungsbehörden, staatlich sanktionierte ‚Hack-Back'-Aktivitäten privater Unternehmen, militärische Operationen und nachrichtendienstliche Aufklärung. Andererseits sind schadensbegrenzende Mechanismen und die Schließung von Schwachstellen von entscheidender Bedeutung zum Schutz privater und staatlicher IT-Systeme und Netzwerke. Behörden ziehen daher nicht nur Nutzen aus dem Zurückhalten von Schwachstellen, denn sie nutzen selbst die entsprechenden Systeme, die nicht mehr sicher sind, wenn erkannte Schwachstellen nicht behoben werden – dies gilt analog für kritische Infrastrukturen. Abgesehen von Behörden und den Betreibern kritischer Infrastrukturen hat auch die Wirtschaft als Ganzes und nicht zuletzt die Öffentlichkeit ein berech-*

tigtes Interesse an der unmittelbaren Schließung von Schwachstellen. Hardware- und Software-Anbieter sowie Anbieter von Online-Diensten im Speziellen haben ein genuines Interesse daran, Schwachstellen schnellstmöglich zu patchen, um ein sicheres Produkt anbieten zu können und um wirtschaftlichen Reputationsschaden abzuwenden. Wirtschaft und Öffentlichkeit erwarten sichere Geräte und Dienste, mit denen sie frei und vertraulich kommunizieren und arbeiten können, ohne Gefahr zu laufen, Opfer von Cyber-Spionage und –Kriminalität zu werden. Das Internet-Ökosystem profitiert als Ganzes davon, wenn Schwachstellen geschlossen werden. Die Offenlegung von Schwachstellen – und das damit verbundene Schließen dieser – sollte daher das primäre Ziel der Politik sein. Nur in berechtigten Ausnahmefällen sollte diese Offenlegung verzögert und die Schwachstellen damit temporär zurückgehalten werden. Das kann beispielsweise bei bestimmten Strafverfolgungsaktivitäten oder nachrichtendienstlichen Operationen der Fall sein. Der Ausbalancierung und dem Management der entstehenden Zielkonflikte und der notwendigen Werteabwägung kommt daher eine herausragende Bedeutung zu. Dabei sind Grundrechte, Interessen des Handels, die öffentliche Sicherheit und die Sicherheit der informationstechnischen Systeme in die Interessenabwägung einzubeziehen."

***Harpig*, a.a.O., S. 7 f., (Hervorhebung nur hier)**

Vielfach wird gefordert, das Ausnutzen von *Zero-Days* bei der sicherheitsbehördlichen Infiltration informationstechnischer System generell auszuschließen.

3. Weitere Implikationen

Beim Einsatz von Staatstrojanern stellt sich aus informationstechnischer Sicht nicht nur die Frage der Sicherheitslücken als Eigenschaften der zu infiltrierenden Systeme bzw. der auf diesen installierten Programme. Auch die Eigenschaften der Überwachungssoftware, also der Trojaner selbst, erfordern sorgfältige Beachtung.

Von der Beschaffenheit und den Funktionalitäten dieser Programme hängt etwa ab, inwieweit infolge der Infiltration unbeabsichtigt Schädigungen des Zielsystems oder ggf. einer Vielzahl von mit diesem über das Internet verbundenen anderen Systemen entstehen können und ob in dem Zielsystem oder den mit diesen verbundenen Systemen Abläufe initiiert werden, die mit Anlass und Zweck der Überwachung gar nichts zu haben.

Durch vom CCC vorgenommene Analysen ist im Jahr 2011 etwa bekannt geworden, dass für die Quellen-TKÜ genutzte „Bundestrojaner“ nicht nur höchst intime Daten ausleiten konnten, sondern auch über eine Fernsteuerungsfunktion zum „Nachladen“ und Ausführen beliebiger weiterer Software verfügten. Der CCC warnte zudem vor dem Entstehen eklatanter Sicherheitslücken in den infiltrierten Rechnern durch grobe Design- und Implementierungsfehler der Überwachungssoftware, die geeignet waren, von Dritten ausgenutzt zu werden.

> ***Chaos Computer Club*, Analyse einer Regierungs-Malware, Berlin, 8. Oktober 2011.**

Als große Herausforderung hat sich für die Sicherheitsbehörden die eigene Entwicklung von Überwachungssoftware, etwa beim Bundeskriminalamt (BKA), erwiesen. Es wurde auch von fragwürdigen Kooperationen des BKA mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und der National Security Agency (NSA) in den USA berichtet.

> **Hierzu etwa: https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/, Aufruf am 01.07.2019; www.netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/, Aufruf am 01.07.2019.**

Bei der Beschaffung von Trojanern bei einschlägigen Software-Herstellern im In- und Ausland taten sich in der Vergangenheit gravierende Sicherheitsmängel auf. Zudem ist bei der Fremdbeschaffung nicht notwendig gewährleistet, dass die Anwenderbehörde überhaupt den Quellcode der von ihr eingesetzten Software kennt und damit die Funktionalitäten und Sicherheitsrisiken des jeweiligen Trojaners überschauen kann, auch hinsichtlich der Ausleitung von bei der Überwachung entstehenden Daten an den Hersteller. Zudem bleibt auch unbekannt, an welche anderen Nutzer und für welche Einsetzzwecke die jeweilige Software verkauft oder vermietet wird.

> **Hierzu etwa *Kurz*, a.a.O., INA 19/86, S. 61 f., S. 79 f.; *Rehak*, a.a.O., INA 19/63, S. 389 (403), INA 19/86, S. 66, S. 85; *Roggenkamp,* INA 19/86, S. 24 f.; www.netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/, Aufruf am 01.07.2019.**

C. Zulässigkeit der Verfassungsbeschwerden

Die Verfassungsbeschwerden sind zulässig.

I. Statthaftigkeit

Die Verfassungsbeschwerden sind statthaft. Insbesondere wendet sich auch der Beschwerdeführer zu 3) – nicht anders als die Beschwerdeführer zu 1) und 2) – gegen Grundrechtsverletzungen und nicht etwa gegen eine Beeinträchtigung in seinem verfassungsrechtlichen Status als politische Partei.

II. Beschwerdefähigkeit

Die Beschwerdeführer sind beschwerdefähig. Sie rügen die Verletzung in einem ihrer Grundrechte (§ 90 Abs. 1 BVerfGG), nämlich dem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. alleine aus Art. 2 Abs. 1 GG.

1. Beschwerdeführer zu 1) und 2)

Die Beschwerdeführer zu 1) und 2) sind als natürliche Personen ohne Weiteres Träger dieses Grundrechts und damit beschwerdefähig.

2. Beschwerdeführer zu 3)

Der Beschwerdeführer zu 3) ist dies ebenfalls.

Auch die als nicht-rechtsfähige Vereinigungen organisierten politischen Parteien sind beschwerdefähig, soweit ihnen das jeweilige Grundrecht seinem Wesen nach gemäß Art. 19 Abs. 3 GG zustehen kann.

BVerfGE 3, 383 (391), 84, 290 (299); 111, 54 (81); 121, 30 (56 f.).

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme kann seinem Wesen nach einer juristischen Person oder Personenvereinigung zustehen, da es sich nicht nur individuell, sondern auch kollektiv wahrnehmen lässt.

Vgl. *Gersdorf*, in: Gersdorf/Paal, Beck-OK Informations- und Medienrecht, 24. Ed. Stand: 01.05.2019, Art. 2 GG Rn. 33.

Für andere Ausprägungen des allgemeinen Persönlichkeitsrechts, jedenfalls soweit dieses auf Art. 2 Abs. 1 GG fußt, hat das Bundesverfassungsgericht dies bereits anerkannt, etwa für das Recht am gesprochenen Wort und das Grundrecht auf informationelle Selbstbestimmung.

BVerfGE 106, 28 (43); 118, 168 (203 f.).

Bereits die Sachverwandtschaft mit diesen Rechten spricht für die Geltung auch des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für Vereinigungen. Verbindend zwischen diesen Rechten ist etwa der Bezug zur kommunikativen Entfaltung. „Kommunikationsfreiheiten“ werden aber gerade im Zusammenwirken mit anderen genutzt.

***Hoffmann-Riem*, JZ 2008, S. 1009 (1010)**

Informationstechnischen Systemen kommt zudem ein herausragender Stellenwert für kollektive Freiheitsbetätigungen zu. Exemplarisch zeigt sich das gerade für eine politische Partei an der oben (B.II.3) dargestellten Arbeitsweise des Beschwerdeführers zu 3). Ohne die von ihm eingerichtete IT-Infrastruktur und die darin zusammengefassten Anwendungen für die Kommunikation über das Internet und die dezentrale kollaborative Bearbeitung von Projekten wäre er in seiner Aktivität erheblich eingeschränkt. Umgekehrt vermittelt ihm die Verfügbarkeit dieser Infrastruktur anders nicht zu erlangende Entfaltungsmöglichkeiten und ein Maximum an Selbstbestimmung bei der Organisation und Ausgestaltung seiner Arbeit einschließlich der Bestimmung über die allgemeine Zugänglichkeit oder gestufte Vertraulichkeit einzelner Vorgänge.

Vor diesem Hintergrund beeinträchtigen Gefährdungen der Vertraulichkeit und Integrität der von ihm genutzten informationstechnischen Systeme den Beschwerdeführer zu 3) als Kollektiv in vergleichbarer Weise wie dies bei einem Einzelnen als Grundrechtsträger der Fall ist.

Hierzu BVerfGE 120, 274 (303 ff.)

Die Grundrechtsberechtigung des Beschwerdeführers zu 3) und damit seine Beschwerdefähigkeit lassen sich hiernach nicht ernstlich bezweifeln.

III. Beschwerdebefugnis

Die Beschwerdeführer sind beschwerdebefugt. Durch die angegriffenen Vorschriften sind sie unmittelbar, selbst und gegenwärtig betroffen.

1. Unmittelbare Betroffenheit

Den Beschwerdeführern fehlt es – insoweit ohne Unterschied zwischen ihnen – nicht an der erforderlichen unmittelbaren Betroffenheit.

Zwar ist ein Beschwerdeführer nur dann von einer gesetzlichen Maßnahme unmittelbar betroffen, wenn diese, ohne dass es eines weiteren Vollzugsakts bedürfte, in seinen Rechtskreis eingreift. Erfordert das Gesetz zu seiner Durchführung rechtsnotwendig oder auch nur nach der tatsächlichen staatlichen Praxis einen besonderen, vom Willen der vollziehenden Stellen beeinflussten Vollzugsakt, muss der Beschwerdeführer grundsätzlich zunächst diesen Akt angreifen und den gegen ihn eröffneten Rechtsweg erschöpfen.

BVerfGE 1, 97 (102); 109, 299 (306), 133, 277 (311)

a. Ungenügender Zugang zu fachgerichtlichem Rechtsschutz gegenüber heimlichen Eingriffen

Von einer unmittelbaren Betroffenheit ist jedoch dann auszugehen, wenn der Beschwerdeführer den Rechtsweg nicht beschreiten kann, weil er keine Kenntnis von der betreffenden Vollzugsmaßnahme erhält, und sei es nachträglich, weil die Vollzugsmaßnahmen nach der gesetzlichen Konzeptzion

heimlich ausgeführt werden und Vorschriften, die eine nachträgliche Bekanntgabe der Maßnahme vorsehen, aufgrund weit reichender Ausnahmetatbestände eine Kenntnisnahme möglichweise auch langfristig nicht sicherstellen. Unter diesen Umständen ist ebenfalls nicht gewährleistet, dass der Betroffene effektiven fachgerichtlichen Rechtsschutz erlangen kann.

> **BVerfGE 109, 299 (306 f.); 133, 277 (311); 141, 220 (261); jeweils mit weiteren Nachweisen; Landesverfassungsgericht Mecklenburg-Vorpommern, LKV 2000, S. 345 (346)**

So ist es hier.

aa. Die vorliegend angegriffenen Ermächtigungen erlauben gerade die heimliche Infiltration informationstechnischer Systeme. Allerdings statuiert das HSOG in seinem Bestimmungen zum Datenschutz Benachrichtigungspflichten in Bezug auf die nach §§ 15b, 15c HSOG durchgeführten Maßnahmen.

Zunächst bestehen in Bezug auf diese Maßnahmen Protokollierungspflichten nach § 28 Abs. 1, Abs. 2 Nrn. 5 und 6 HSOG. Sodann bestimmt § 29 Abs. 5 Satz 1 HSOG:

> *„Wurden personenbezogene Daten durch Maßnahmen nach § 28 Abs. 2 erlangt, sind die dort jeweils bezeichneten betroffenen Personen hierüber nach Abschluss der Maßnahmen zu benachrichtigen“.*

Dies sind im Falle des § 15b HSOG die Beteiligten der überwachten Telekommunikation, im Falle des § 15c HSOG die Zielperson sowie mitbetroffene Personen.

bb. Hiervon ausgehend sehen die §§ 28, 29 HSOG jedoch weitreichende Ausnahmen von der Benachrichtigungspflicht vor.

Bereits nach § 28 Abs. 3 Satz 1 HSOG sind

> *„Nachforschungen zur Feststellung der Identität einer der in Abs. 2 bezeichneten Personen nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.“*

Die gleichen Einschränkungen bestehen nach § 29 Abs. 5 Satz 2 HSOG hinsichtlich Nachforschungen zur Feststellung der Identität oder zur Anschrift einer zu benachrichtigenden Person.

Die hiernach verbleibenden Benachrichtigungspflichten sind weiter dadurch eingeschränkt, dass die Benachrichtigung gemäß § 29 Abs. 6 HSOG zurückzustellen ist, solange sie

> *„1. den Zweck der Maßnahme*
>
> *2. ein sich an den auslösenden Sachverhalt anschließendes strafrechtliches Ermittlungsverfahren,*
>
> *3. den Bestand des Staates*
>
> *4. Leib, Leben oder Freiheit einer Person oder*
>
> *5. Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,*
>
> *gefährden würde.“*

Ausweislich des § 29 Abs. 6 Satz 5 HSOG schweben dem Gesetzgeber hierbei durchaus Ketten mehrfacher Zurückstellungen in halbjährlichen Intervallen vor, was eine großzügige Beurteilungspraxis der zuständigen Behördenleitungen oder der von diesen beauftragten Bediensteten (§ 29 Abs. 6 Satz 3 HSOG) in Bezug auf das Erfordernis von Zurückstellungen begünstigen dürfte; nach der genannten Vorschrift ist der Hessische Datenschutzbeauftragte spätestens sechs Monate nach Abschluss einer Maßnahme und danach in halbjährlichen Abständen über die Zurückstellung zu benachrichtigen.

Gemäß § 29 Abs. 7 Satz 1 HSOG unterbleibt eine Benachrichtigung nach Absatz 5, soweit dies im überwiegenden Interesse einer betroffenen Person liegt. Zudem kann gemäß § 29 Abs. 7 Satz 2 HSOG die Benachrichtigung einer in § 28 Abs. 2 Nr. 5 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen ist und anzunehmen ist, dass sie kein Interesse an der Benachrichtigung hat. Die Entscheidungen nach § 29 Abs. 7 Satz 1 und 2 HSOG und somit die entsprechende Beurteilung der jeweiligen Sachverhalte obliegen den Behördenleitungen oder von diesen beauftragten Bediensteten.

Gemäß § 29 Abs. 8 HSOG bedarf die Benachrichtigung der Zustimmung der Staatsanwaltschaft, sofern die personenbezogenen Daten in ein anhängiges Strafverfahren eingeführt sind.

cc. Die Heimlichkeit von Maßnahmen nach den §§ 15b, 15c HSOG wird nach alledem durch die Pflicht zu nachträglicher Benachrichtigung nur teilweise aufgefangen. Diese Pflichten greifen möglicherweise erst spät ein und kennen weitreichende Ausnahmen, wobei die Anwendung der Ausnahmetatbestände keiner gerichtlichen Kontrolle unterliegt.

Dies muss wie in den dem Bundesverfassungsgericht bereits vorgelegten vergleichbaren Konstellationen auch hier zur Annahme der unmittelbaren Betroffenheit der Beschwerdeführer führen.

Vgl. etwa BVerfGE 141, 220 (261 f.)

b. Inkaufnahme faktischer Rechtsgutbeeinträchtigungen durch den Gesetzgeber

Die Ermächtigung der Polizeibehörden zu Maßnahmen nach §§ 15b und 15c HSOG setzen die Beschwerdeführer zusätzlich faktischen Beeinträchtigen aus, die ihrerseits eigenständig die unmittelbare Betroffenheit der Beschwerdeführer in dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme begründen, ohne dass die Beschwerdeführer hiergegen fachgerichtlichen Rechtsschutz erlangen könnten. Diese Beeinträchtigungen gehen über bloße Reflexe hinaus. Sie wirken sich gegenüber den Beschwerdeführern wie Eingriffe aus und sind dem hessischen Gesetzgeber zuzurechnen.

Die Ermächtigungen in §§ 15b und 15c HSOG bewirken bei der gebotenen Gesamtbetrachtung der von dem hessischen Gesetzgeber getroffenen Regelung – insbesondere hinsichtlich eines Schwachstellenmanagements, aber auch näherer Anforderungen an die Herkunft, Beschaffenheit, Funktionsweise und Anwendungskontrolle der zur Infiltration der Zielsysteme einzusetzenden technischen Mittel – ernsthafte Gefährdungen der Vertraulichkeit und Integrität der von den Beschwerdeführern genutzten informationstechnischen Systeme. Zwar gehen diese Gefährdungen nicht direkt und unmittel-

bar zielgerichtet von dem gesetzgeberischen Handeln aus, sondern beruhen vielmehr auf komplexen Geschehensabläufen, die maßgeblich auch vom Verhalten anderer Personen abhängen, insbesondere dem kommerziellen Handel mit und der kriminellen Ausnutzung von digitalen Schwachstellen der informationstechnischen Systeme und Programme. Jedoch hat der hessische Gesetzgeber das Problem dieser Gefährdungen in verfassungsrechtlich zu beanstandender Weise ungelöst gelassen:

aa. Hängt die Beeinträchtigung grundrechtlich geschützter Interessen vom Verhalten anderer Personen ab oder beruht sie auf einem komplexen Geschehensablauf, setzt die Bejahung eines eingriffsgleichen staatlichen Handelns voraus, dass der Staat die fragliche Beeinträchtigung – etwa durch kriminelle oder terroristische Handlungen – als für ihn vorhersehbare Folge seines Handelns zumindest in Kauf nimmt.

> **BVerfGE 105, 279 (300); BVerfG, Beschl. v. 15.03.2018 – 2 BvR 1371/13 – , Juris Rn. 29.**

In Anwendung dieses verfassungsrechtlichen Maßstabs hat das Bundesverfassungsgericht im dem Beschluss vom 15.03.2018 betreffend die Stationierung von Atomwaffen im Fliegerhost Büchel eine eingriffsgleiche Gefährdung der Beschwerdeführerin in ihren Grundrechten aus den folgenden Erwägungen verneint:

> *„Da das Risiko terroristischer Anschläge der deutschen Staatsgewalt nicht zuzurechnen ist – die Bedrohung der durch Art. 2 Abs. 2 Satz 1 und Art. 14 Abs. 1 GG geschützten Rechtsgüter geht von Dritten, insbesondere terroristischen Vereinigungen aus – kommt als Anknüpfungspunkt allein der Umstand in Betracht, dass die Bundesrepublik Deutschland den USA (…) die Stationierung der Atomwaffen in Büchel gestattet hat. Dies stellt jedoch keinen Eingriff in die Grundrechte der Beschwerdeführerin dar, weil es zum einen an der Finalität einer möglichen Nachteilszufügung fehlt – die gerügten Gefahren sind hinsichtlich ihres Realisierungsrisikos für die deutschen Staatsorgane nicht vorhersehbar und werden von diesen auch nicht in Kauf genommen – und weil zum anderen der Zurechnungszusammenhang unterbrochen wäre. Weder reicht der deutsche Staat Terroristen die Hand, noch verleiht er deren Aktivitäten den Anschein der Legalität oder billigt und unterstützt sie in sonstiger Weise“.*
>
> **BVerfG, Beschl. v. 15.03.2018, a.a.O., Rn. 44 (Hervorhebungen nur hier)**

bb. Vorliegend ist dem hessischen Gesetzgeber ein vergleichbar unbedenkliches Handeln nicht zu attestieren. Dieser hat ein für ihn vorhersehbares relevantes Realisierungsrisiko ignoriert und ungeachtet aller Bedenken und Warnungen von Expertenseite keine wirksamen Vorkehrungen gegen Vollzugspraktiken getroffen, bei denen der Staat Cyberkriminellen in gewisser Weise durchaus „die Hand reicht“, den Schwarzmarkt der Schwachstellen stimuliert und kriminelles Hacken jedenfalls begünstigt.

Namentlich hat der Gesetzgeber es unterlassen, den Einsatz der für die Infiltration informationstechnischer Systeme erforderlichen Software („Staatstrojaner“) an ein qualifiziertes Schwachstellenmanagement für den Umgang mit digitalen Sicherheitslücken zu knüpfen, sondern hat im Gegenteil Anreize für einen Umgang mit diesen Sicherheitslücken geschaffen, der strukturell die IT-Sicherheit und damit die Vertraulichkeit und Integrität informationstechnischer Systeme unterminiert. Zudem lässt die getroffene Regelung notwendige Anforderungen an die Beschaffenheit, Funktionalität und Anwendungskontrolle der für die Maßnahmen nach den §§ 15b, 15c HSOG einzusetzenden Trojaner vermissen.

cc. Fachgerichtlichen Rechtsschutz gegen die dem Gesetzgeber zuzurechnenden faktischen Beeinträchtigungen können die Beschwerdeführer nicht erlangen. Soweit die §§ 15b, 15c HSOG ohne Vorkehrungen für ein Schwachstellenmanagement und weitere notwendige Vorgaben für den Einsatz der technischen Mittel zur Infiltration informationstechnischer Systeme erlassen worden sind, sehen die Beschwerdeführer sich einem „unechten Unterlassen“ des Gesetzgebers gegenüber, gegen welches unmittelbar die Gesetzesverfassungsbeschwerde, ggf. mit der Folge einer Nachbesserung durch den Gesetzgeber gegeben ist.

> **BVerfGE 56, 54 (71); vgl. *Bethge*, in: Maunz/Schmidt-Bleibtreu/Klein/Bethge, BVerfGG, 56. EL Februar 2019, § 90 Rn. 222, 226; *Grünewald*, in Walter/Grünewald, Beck-OK, BVerfGG, 6. Ed. Stand 01.12.2017, § 90 Rn. 68.**

c. Verletzung der staatlichen Schutzpflicht

aa. Durch das beschriebene Unterlassen hat der hessische Gesetzgeber zugleich eine ihn treffende Schutzpflicht aus dem Grundrecht auf Gewähr-

leistung der Vertraulichkeit und Integrität informationstechnischer Systeme verletzt. Wird eine den Staat zunächst als Ausfluss der objektiven Wertentscheidungen des Grundgesetzes bindende grundrechtliche Schutzpflicht verletzt, liegt darin zugleich eine Verletzung des jeweiligen Grundrechts gegenüber den Betroffenen.

BVerfGE 77, 170 (214).

Auch insoweit sind die Beschwerdeführer unmittelbar in ihrer grundrechtlich geschützten Position betroffenen.

bb. Zu der Wirkdimension des Grundrechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme hat das Bundesverfassungsgericht sich zwar noch nicht explizit geäußert. Das Potential für den sich in dieser Wirkdimension entfaltenden objektiv-rechtlichen Gehalt dieser Grundrechtsausprägung hat das Gericht allerdings bereits dadurch anerkannt, dass es zu deren Kennzeichnung den Begriff „Gewährleistung“ gewählt hat.

***Hoffmann-Riem*, JZ 2014, S. 53 (57); *ders.*, JZ 2008, S. 1009 (1019 f.); vgl. *Gersdorf,* in: Gersdorf/Paal, a.a.O., Art. 2 GG Rn. 29.**

Dieses Potenzial gilt es zu aktivieren: Schutzdimensionen außerhalb des rein abwehrrechtlichen Schutzes der Grundrechte treten umso eher in das Zentrum grundrechtlicher Garantien, je mehr die realen Voraussetzungen der Freiheitsausübung der Bürger einerseits durch den Staat, andererseits aber auch durch Private oder im Zuge von Kooperationsakten zwischen Staat und Privaten geschaffen und erhalten werden müssen, aber gegebenenfalls auch von ihnen in Frage gestellt werden.

***Hoffmann-Riem*, JZ 2008, S. 1009 (1013)**

Auf die Sicherung der Voraussetzungen für die Freiheitsausübung in Kontexten umfassender digitaler Vernetzung trifft dies in hohem Maße zu, und zwar gerade auch im Hinblick auf den hier interessierenden Schutz vor der Infiltration informationstechnischer Systeme durch Dritte zu kriminellen oder sonst persönlichkeitsverletzten Zwecken.

Der Einzelne kann solche Zugriffe zum Teil gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren.

BVerfGE 120, 274 (306)

Die Aktivierung der schutzrechtlichen Wirkdimension des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist daher gerade hier geboten.

2. Eigene und gegenwärtige Betroffenheit

Durch die angegriffenen Vorschriften sind die Beschwerdeführer auch selbst und gegenwärtig betroffen.

Die Möglichkeit einer eigenen und gegenwärtigen Betroffenheit ist grundsätzlich erfüllt, wenn der Beschwerdeführer mit einiger Wahrscheinlichkeit durch die auf den angegriffenen Rechtsnormen beruhenden Maßnahmen in seinen Grundrechten berührt wird. Der geforderte Grad der Wahrscheinlichkeit wird dadurch beeinflusst, welche Möglichkeiten der Beschwerdeführer hat, seine Betroffenheit darzulegen. So ist bedeutsam, ob die Maßnahme auf einen tatbestandlich eng umgrenzten Täterkreis zielt oder ob sie eine große Streubreite hat und Dritte auch zufällig erfassen kann. Darlegungen, durch die sich der Beschwerdeführer selbst der Ungesetzlichkeit bezichtigen müsste, dürfen zum Beleg der eigenen gegenwärtigen Betroffenheit nicht verlangt werden. Besteht die Möglichkeit, Objekt der betreffenden Maßnahme zu werden, praktisch für jedermann, ist der Kreis der selbst und gegenwärtig Betroffenen entsprechend weit. Bei Maßnahmen der Telekommunikationsüberwachung umfasst er zudem nicht nur die möglichen Verantwortlichen selbst oder dessen Kontakt- und Begleitpersonen, sondern auch Personen, die mit den Adressaten der Maßnahmen über Telekommunikationseinrichtungen in Verbindung stehen.

BVerfGE 109, 279 (307); 113, 348 (Juris Rn. 77 f.)

a. Beschwerdeführer zu 1)

Der Beschwerdeführer ist nach diesen Maßstäben sowohl hinsichtlich etwaiger Maßnahmen nach § 15b HSOG als auch solcher nach § 15c HSOG selbst und gegenwärtig betroffen.

Wie dargelegt, nutzt er das Internet in vielfältiger Weise und kommuniziert über dieses per E-Mail und den Messenger Telegram. Aufgrund seines politischen und gesellschaftlich-kulturellen Engagements erreicht diese Kommunikation ein erhebliches Ausmaß, und zwar mit einem beträchtlichen Anteil von Kommunikationspartnern, die er persönlich nur wenig oder gar nicht kennt. Durch die gemeinsame Nutzung von Geräten mit seiner politisch und gesellschaftlich ebenfalls vielfältig engagierten Ehefrau und seinem Sohn multipliziert sich die Streubreite.

aa. Damit besteht eine hier jedenfalls hinreichende Wahrscheinlichkeit, dass der Beschwerdeführer zu 1) alleine schon zufällig Mitbetroffener einer anderen Zielpersonen geltenden Quellen-TKÜ nach § 15b HSOG sein kann. Soweit erwogen werden mag, die zufällige Streubreite der Quellen-TKÜ sei gegenüber der „herkömmlichen" TKÜ geringer, da die Quellen-TKÜ lediglich die verschlüsselte Kommunikation der Zielpersonen betrifft, folgt daraus jedenfalls für die Betroffenheitswahrscheinlichkeit des Beschwerdeführers zu 1) kein relevanter Unterschied. Vor dem Hintergrund seiner netzpolitischen Anschauungen und aus seinem Bewusstsein für digitale Gefahren bedient er sich bei der E-Mail-Korrespondenz ganz überwiegend der Verschlüsselung. Bei der Messenger-Nutzung ist ohnehin durchweg der Fall.

Zudem wird der durch Infiltration informationstechnischer Systeme erfolgenden Überwachung generell eine große Streubreite mitbetroffener Personen zugeschrieben. Dies bringt mit sich, dass Dritte

> *„nicht nur betroffen werden, soweit dies ‚im Einzelfall unvermeidbar' ist, sondern potenziell grundsätzlich und – vermutlich häufig – ohne jede im Vorwege vorzunehmende Eingrenzung und (…) ohne dass sie sich ‚eigenbestimmt' dagegen wehren können.'*
>
> ***Hoffmann-Riem*, JZ 2008, S. 1009 (1018)**

bb. Hiervon ausgehend kann auch eine hinreichende Wahrscheinlichkeit der Mitbetroffenheit des Beschwerdeführers zu 1) von Maßnahmen nach § 15c HSOG nicht von der Hand gewiesen werden.

cc. Der Gefahrerhöhung durch die unzureichende Ausgestaltung der gesetzlichen Befugnisse (oben 1.b, 1.c) ist der Beschwerdeführer zu 1) evident selbst und gegenwärtig ausgesetzt. Hier geht es um eine ubiquitär wirkende Beeinträchtigung, die eine Betroffenheit für praktisch jedermann und damit auch für den Beschwerdeführer zu 1) begründet. Dabei besteht allerdings ein gesteigertes Schutzbedürfnis des Beschwerdeführers zu 1) durch sein politisches und gesellschaftliches Engagement, das mit einem großen Kommunikationsumfang über digitale Medien einschließlich der Administratorenstellung für Internetseiten und E-Mail-Verteiler verbunden ist. Zudem ist naturgemäß nicht auszuschließen, dass die Gefährdung sich bereits in Gestalt einer heimlichen Infiltration der von ihm genutzten informationstechnischen Systeme durch eine bisher von ihm nicht bemerkte Hacker-Attacke realisiert hat. In diesem Fall versagte bei einer geheim gehaltenen Sicherheitslücke gerade auch sein Eigenschutz, da die Sicherheitslücke in der betreffenden Anwendung noch nicht gepatched und in seinem Antivirenprogramm noch nicht berücksichtigt wäre.

b. Beschwerdeführer zu 2)

aa. Zunächst einmal nicht anders beurteilt sich die Wahrscheinlichkeit der Betroffenheit des Beschwerdeführers zu 2) von Maßnahmen nach § 15b HSOG und § 15c HSOG.

bb. Hinsichtlich der Beeinträchtigung durch die Vernachlässigung gesetzlicher Regelungserfordernisse besteht in seinem Fall jedoch eine zusätzlich gesteigerte Schutzbedürftigkeit. Die von dem Beschwerdeführer zu 2) genutzten informationstechnischen Systeme sind wahrscheinliche Zielobjekte geheimdienstlicher Überwachungsmaßnahmen, so dass er gegenüber Beeinträchtigungen von deren Vertraulichkeit und Integrität besonders sensibel ist. Für den Beschwerdeführer zu 2) haben diese Güter zudem mit Blick auf den Schutz seiner Kontaktpersonen im Ausland in Belangen wie der körperlichen Unversehrtheit und persönlichen Freiheit herausragenden Stellenwert.

c. Beschwerdeführer zu 3)

aa. Durch die allgemeine Streubreite der Maßnahmen nach § 15b und § 15c HSOG ist der Beschwerdeführer zu 3) zunächst einmal in gleicher Weise wie die anderen Beschwerdeführer betroffen. Eine Einschränkung mag sich insoweit ergeben, als die von ihm ohne Zugangsbeschränkung für einen öffentlichen Zugriff zur Verfügung gestellten Anwendungen bereits eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung nicht begründen dürften. Es verbleiben jedoch eine Vielzahl von Anwendungen mit beschränkter Zugangsberechtigung, auf die der Grundrechtsschutz sich jedenfalls erstreckt, weil der Beschwerdeführer zu 3) insoweit davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt.

Vgl. BVerfGE 120, 274 (315)

Als physische Bezugsobjekte dieses Schutzes sieht die Verfassungsbeschwerde die von dem Beschwerdeführer zu 3) bei dem Hosting-Unternehmen in Anspruch genommenen Speichermedien und sonstigen Hardwarebestandteile, aber auch die einzelnen privaten Endgeräte, soweit sie im Rahmen der Parteiarbeit genutzt werden, an.

Hebt die Vielzahl der bisweilen an der Kommunikation und der kollaborativen Nutzung der beschränkt zugänglichen Anwendungen beteiligten Einzelpersonen die grundrechtliche Schutzerwartung nicht auf, so erhöht sie jedoch die Wahrscheinlichkeit zufälliger Mitbetroffenheit von Maßnahmen, die nicht gegen den Beschwerdeführer zu 3), seine Mitglieder und sonst an seiner Arbeit beteiligte Personen, sondern gegen dritte Zielpersonen gerichtet sind.

bb. Ungeachtet dessen erhöht sich mit der Anzahl zugangsberechtigter Personen allerdings die Wahrscheinlichkeit, dass die informationstechnischen Systeme des Beschwerdeführers zu 3) zu Zielobjekten von polizeilichen Maßnahmen, insbesondere auch der Online-Überwachung werden könnten, weil die Zielperson dem Kreis der berechtigten Nutzer angehört und die Annahme besteht, dass sie auf dem System aufklärungsrelevante Informationen speichert.

cc. Eine relevante Wahrscheinlichkeit, hinsichtlich seiner dem Grundrechtsschutz unterstehenden informationstechnischen Systeme Überwachungsmaßnahmen nach § 15c HSOG ausgesetzt zu werden, resultiert für den Beschwerdeführer zu 3) aber auch daraus, dass Dritte das System ihrerseits heimlich infiltrieren und für die Verarbeitung solcher Informationen missbrauchen könnten, etwa im Zusammenhang mit Anschlagsplanungen oder zur Durchführung eines Cyberangriffs auf eine Infrastruktureinrichtung.

Im Ansatz so geschehen ist dies im Jahr 2011 im Fall „Servergate“. Dabei hatten Unbekannte in einem „Piratenpad“ (oben B.II.3) eine Schadsoftware platziert, die nach anfänglichen Erkenntnissen französischer Sicherheitsbehörden zu einem Angriff auf den Energiekonzern EDF benutzt werden sollte. Dies führte zur Einschaltung der deutschen Polizei und der Beschlagnahme und Durchsuchung der Server der Bundespartei.

> **zu Einzelheiten: https://netzpolitik.org/2011/piratenpartei-server-auf-polizeiliche-anweisung-offline/ (aufgerufen am 01.07.2019); https://wiki.piratenpartei.de/Servergate**

Ein vergleichbarer Missbrauch der von dem Beschwerdeführer zu 3) nunmehr genutzten Cryptpads, die eine Zugangssicherung aufweisen und daher dem Grundrechtsschutz unterliegen, ist unter Berücksichtigung des Ereignisses im Jahr 2011 hinreichend wahrscheinlich. Der Zugangsschutz der Cryptpads stellt für die potenziellen Verantwortlichen eines Cyberangriffs keine diese Wahrscheinlichkeit signifikant verringernde Hürde da. Vielmehr könnte ein polizeiliche Überwachungsmaßnahmen auslösendes Szenario etwa darin bestehen, dass das informationstechnische System des Beschwerdeführers zu 3) heimlich von dezentral zusammenwirkenden Verantwortlichen infiltriert wird, um in seinem Schutz Tatverabredungen zu treffen oder es – wie bei „Servergate“ von den Behörden zunächst vermutet – als Ausgangssystem eines Cyberangriffs zu missbrauchen.

IV. Beschwerdefrist

Die Beschwerdefrist nach § 93 Abs. 3 BVerfGG gegen die am 04.07.2019 in Kraft getretenen Befugnisnormen ist gewahrt. Soweit § 15b HSOG in seiner geänderten Fassung angegriffen wird, haben die Ausweitung des Zulässigkeitstatbestands (§ 15b Abs. 1 i.V., § 15a Abs. 1 Satz 1 HSOG) für die Quel-

len-TKÜ und die Erweiterung des Kreises möglicher Zielpersonen dieser Maßnahme (§ 15b Abs. 1 i.V.m. §§ 15a Abs. 1 Satz 2, 15 Abs. 2 Satz 1 Nr. 2 und 3 HSOG) das materielle Gewicht der Regelung erheblich verstärkt und die Frist neu in Gang gesetzt.

D. Begründetheit der Verfassungsbeschwerde

Die Verfassungsbeschwerden sind begründet.

§§ 15b und 15c HSOG in ihrer gegenwärtigen Ausgestaltung verletzten die Beschwerdeführer in ihrem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme.

II. Verfassungswidriges unechtes Unterlassen des Gesetzgebers der §§ 15b, 15c HSOG

1. Objektiver Verfassungsverstoß

Das von den Beschwerdeführern beanstandete Regelungsdefizit (C.III.1.b, c) bedeutet einen Verstoß gegen den objektiven Gewährleistungsgehalt des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

a. **Zentraler Zielkonflikt beim Einsatz von „Staatstrojanern**“

Bei der Forderung nach ergänzenden Regelungen für ein Schwachstellenmanagement geht es um nichts anderes als die Lösung des zentralen Zielkonflikts, der mit der heimlichen Infiltration informationstechnischer Systeme durch staatliche Sicherheitsbehörden aufgeworfen ist.

Das Bundesverfassungsgericht hat diesen Konflikt in seinem Urteil vom 27.02.2008 bereits wie folgt benannt:

> *„Werden zur Infiltration bislang unbekannte Sicherheitslücken des Betriebssystems genutzt, kann dies einen Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme auslösen.“*
>
> **BVerfGE 120, 274 (326)**

Zugleich erkannte das Gericht die Möglichkeit, dass die Sicherheitsbehörden bei der Auflösung des Zielkonflikts, wird sie ihnen überantwortet, zu hohes

Gewicht auf ihre Aufklärungs- und Ermittlungsinteressen legen könnten.
Es führte aus:

> *„In der Folge besteht die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sie sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben.“*
>
> **Ebd.**

Daran anschließend zeigte das Gericht die folgende Konsequenz auf:

> *„Der Zielkonflikt könnte daher das Vertrauen der Bevölkerung beeinträchtigen, dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist.“*
>
> **Ebd.**

Neben diese für sich schon nicht hinnehmbare Beeinträchtigung tritt als weitere jedenfalls in Betracht zu ziehende Folge eines einseitig von den behördlichen Interessen geleitenden exekutiven Handelns die tatsächliche Erhöhung von Gefahren für die Sicherheit der Informationstechnologie durch das gezielte Geheimhalten von Sicherheitslücken.

b. Auflösung des Zielkonflikts als wesentliches Element einer Ermächtigung zum Trojanereinsatz

aa. Hiernach ist von verfassungs wegen unabweisbar, dass der Gesetzgeber die Auflösung des Zielkonflikts nicht der Exekutive überlässt. Es handelt sich um eine für den freiheitlichen Rechtsstaat und für die Grundrechtsverwirklichung wesentliche Entscheidung und damit um ein notwendiges Element jeder Regelung, durch welche der Gesetzgeber die Exekutive zu heimlichen Eingriffen in informationstechnische Systeme mit technischen Mitteln ermächtigt.

Durch das vollständige Fehlen dieses Elements in der von dem hessischen Gesetzgeber getroffenen Regelung sind die Ermächtigungen durch die §§ 15b, 15c HSOG in ihrer derzeitigen Gestalt mit dem objektiven Gewährleistungsgehalt des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht vereinbar, unabhängig von den dem Gesetzgeber für die konkrete Auflösung des Zielkonflikts verblei-

benden Gestaltungs- und Differenzierungsmöglichkeiten.

bb. Das Fehlen der Regelung wird auch nicht dadurch ausgeglichen, dass die hessischen Polizeibehörden etwa bereits durch sonstiges Gesetzesrecht zu einem den Anforderungen des Grundrechts genügenden Umgang mit digitalen Sicherheitslücken verpflichtet wären. Solche Vorschriften existieren nicht, insbesondere auch nicht im Rahmen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Soweit ersichtlich, bestehen auch im Zuge derzeitiger Novellierungsbestrebungen

> **Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat – Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0) vom 27.03.2019; https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2_ ; Aufruf am 19.05.2019**

keine Absichten, dies zu ändern.

cc. Dem Befund des objektiven Verfassungsverstoßes steht auch hinsichtlich § 15b HSOG nicht entgegen, dass nach bisheriger Rechtsprechung des Bundesverfassungsgerichts

> **BVerfGE 120, 274 (307); 141, 220 (309 ff.)**

der Eingriff durch die Quellen-TKÜ alleine an Art. 10 Abs. 1 GG zu messen ist, soweit er sich auf eine staatliche Maßnahme beschränkt, durch welche – wie nach § 15b Abs. 1 Nr. 1 HSOG sicherzustellen – die Inhalte und Umstände ausschließlich der laufenden Telekommunikation im Rechnernetz oder darauf bezogene Daten erhoben werden. Diese Rechtsprechung betrifft die Schrankenanforderungen für die Eingriffe gegenüber den Zielpersonen und Mitbetroffenen der Quellen-TKÜ. Vom Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist deshalb aber nicht jedes erdenkliche im Zusammenhang mit der Quellen-TKÜ stehende Geschehen ausgenommen. Maßgebend ist vielmehr, inwieweit IT-spezifische Gefährdungen des Persönlichkeitsschutzes mit Art. 10 GG abgewehrt werden können.

> **Vgl. etwa *Hoffmann-Riem*, JZ 2009, S. 1009 (1021 f.)**

Hinsichtlich der Gefährdungen durch einen inadäquaten Umgang der Sicherheitsbehörden mit digitalen Sicherheitslücken scheidet ein Schutz durch Art. 10 GG evident aus. Quellen-TKÜ und Online-Durchsuchung unterscheiden sich hinsichtlich der technischen Bedingungen für die Infiltration des Zielsystems in keiner Weise.

2. Subjektive Rechtsverletzung

Die Beschwerdeführer können das unechte Unterlassen des Gesetzgebers auch als Verletzung ihrer durch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschützten Rechtsposition geltend machen. Dies folgt aus der bereits oben (C.III.1.b) dargelegten Inkaufnahme der faktischen Beeinträchtigung dieser Position durch das ungenügende Regelungskonzept der §§ 15b, 15c HSOG.

Die dem hessischen Gesetzgeber zuzurechnende Risikoerhöhung durch den objektiv verfassungswidrigen Rechtssetzungsakt trifft zum einen auf grundrechtlich geschützte Belange der Beschwerdeführer von erheblichem Gewicht, zum anderen ist diesen ein zuverlässiger Eigenschutz nicht möglich. Das Bundesverfassungsgericht hat zu den spezifischen Schutzbedürfnissen des Einzelnen gegenüber digitalen Bedrohungen aus dem Internet etwa ausgeführt:

> *„Vor allem aber öffnet die Vernetzung des Systems Dritten eine technische Zugriffsmöglichkeit, die genutzt werden kann, um die auf dem System vorhandenen Daten auszuspähen oder zu manipulieren. Der Einzelne kann solche Zugriffe zum Teil gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren. Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. Ein technischer Selbstschutz kann zudem mit einem hohen Aufwand oder mit Funktionseinbußen des geschützten Systems verbunden sein. Viele Selbstschutzmöglichkeiten - etwa die Verschlüsselung oder die Verschleierung sensibler Daten - werden überdies weitgehend wirkungslos, wenn Dritten die Infiltration des Systems, auf dem die Daten abgelegt worden sind, einmal gelungen ist. Schließlich kann angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in Zukunft verbleiben, sich technisch selbst zu schützen.“*
>
> **BVerfGE 120, 274 (306)**

Dieses Schutzes bedarf es nicht nur gegenüber Eingriffen des Staates, die alleine Gegenstand Urteils vom 27.02.2008 waren. Er ist auch gegenüber den vielfältigen Bedrohungen von anderer Seite vonnöten. Der Gesetzgeber darf dies bei der Zulassung gefahrenerhöhender staatlicher Maßnahmen genauso wenig außer Betracht lassen wie bei der Ausgestaltung des Rechtsrahmens für risikobehaftete private Aktivitäten, etwa im Bereich des Umwelt- und Technikrechts.

Das gilt umso mehr als sich das Ausmaß der Vernetzung und die damit verbundenen Risiken seit dem Jahr 2008 wohl mehrfach potenziert haben. Wie dargelegt (B.II), machen alle drei Beschwerdeführer von den durch diese Entwicklung der Vernetzung entstandenen Möglichkeiten sehr umfangreich Gebrauch.

3. Verletzung staatlicher Schutzpflicht

Unabhängig von der Qualifizierung der dem hessischen Gesetzgeber zuzurechnenden Risikoerhöhung als Eingriff, die die Abwehrdimension des Grundrechtsschutzes betrifft, stellt sein Unterlassen sich auch als Verletzung der staatlichen Schutzpflicht aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dar, und zwar auch in subjektiv-rechtlicher Hinsicht gegenüber den Beschwerdeführern.

Wie aufgezeigt (C.III.1.c), ist dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme die Wirkdimension einer Schutzpflicht zuzuerkennen.

> **Vgl. *Gersdorf,* in: Gersdorf/Paal, a.a.O., Art. 2 GG Rn. 29; *Heckmann*, in: Rüßmann (Hrsg.), Festschrift für Gerhard Käfer, 2009, S. 129; *Hoffmann-Riem*, JZ 2008, S. 1009 (1023 f.); *ders.*, JZ 2014, S. 53 (57); *Roßnagel/Schnabel,* NJW 2008, S. 3534 (3535 ff.); *Sachs/Krings,* JuS 2008, S. 481 (486); *Schaar*, ZRP 2013, S. 214 (215).**

Wird die Schutzpflicht verletzt, so liegt darin zugleich eine Verletzung des Grundrechts, gegen die sich der Betroffene mit Hilfe der Verfassungsbeschwerde zur Wehr setzen kann. Der damit verbundene Anspruch ist mit

Blick auf die weite gesetzgeberische Gestaltungsfreiheit darauf beschränkt, dass die öffentliche Gewalt Vorkehrungen zum Schutze des Grundrechts trifft, die nicht gänzlich ungeeignet oder völlig unzulänglich sind. Nur unter ganz besonderen Umständen kann sich diese Gestaltungsfreiheit in der Weise verengen, dass allein durch eine bestimmte Maßnahme der Schutzpflicht genüge getan werden kann.

BVerfGE 77, 170 (214)

Die Beschwerdeführer machen hier das pflichtwidrige Absehen des hessischen Gesetzgebers vor irgendwelchen Regelungen zur Auflösung des Zielkonflikts zwischen dem staatlichen Interesse an der Nutzung von Sicherheitslücken im Rahmen der ihnen aufgegebenen Gefahrenwehr und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geltend, eine bestimmte Neukonzeption nach der Nichtigerklärung der Ermächtigungen verlangen sie nicht. Mit diesem Begehren müssen sie unbeschadet der gesetzgeberischen Gestaltungsfreiheit durchdringen.

II. Regelungsausfall in Bezug auf Beschaffenheit, Funktionalität und Anwendungskotrolle der Überwachungssoftware

Die Beschwerdeführer machen eine Verletzung in dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auch als von den Überwachungsmaßnahmen potentiell Betroffene geltend, sei es als Mitbetroffene oder zufällig Betroffene.

Die Ausgestaltung der Ermächtigungen zur Online-Durchsuchung und Quellen-TKÜ weist auch insoweit ein verfassungsrechtlich nicht hinzunehmendes Defizit auf, als sie nicht sicherstellt, dass die mögliche Kompromittierung der ihnen von den Beschwerdeführern als eigene genutzten informationstechnischen Systeme auf unvermeidbare und verhältnismäßige Beeinträchtigungen begrenzt bleibt.

Je nach eingesetzter Infiltrationstechnik kann die Infiltration auch weitere Schäden verursachen, die im Zuge der Angemessenheit einer staatlichen Maßnahme mit zu berücksichtigen sind. Die Möglichkeit von Folgeschäden,

welche die Vertraulichkeit und Integrität der betroffenen informationstechnischen Systeme beeinträchtigen macht eine Überwachungsmaßnahme nicht von vornherein unverhältnismäßig.

BVerfGE 120, 274 (326); 141, 220 (305 f.)

In diesem Kontext verlangen §§ 15b Abs. 2, 15c Abs. 3 Satz 1 HSOG, technisch sicherzustellen, dass an dem informationstechnischen System nur Veränderungen vorgenommenen werden, die für die Datenerhebung unerlässlich sind (§ 15b Abs.2 Satz 1 Nr. 1), und die vorgenommenen Änderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden (§ 15b Abs. 2 Satz 1 Nr. 2). Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen (§ 15b Abs. 2 Satz 2). Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen (§ 15b Abs. 2 Satz 3).

Diese Vorgaben sind unvollziehbar, solange sie nicht durch ein Regelwerk ergänzt werden, welches Anforderungen an die Herkunft und Beschaffung, Beschaffenheit, Eigenschaften und Funktionalitäten der Trojaner (vgl. oben, B.III.3) konkretisiert. Solche Regelungen hat der hessische Gesetzgeber weder selbst getroffen, noch hat er – was wohl praktikabler wäre – untergesetzliche Regelungen vorgesehen. Die gesetzliche Bindung an einen Stand der Technik gerät jedoch zur bloßen Leerformel, wenn das Gesetz noch nicht einmal sicherstellt, dass die Behörde beispielsweise den Quellcode der von ihr eingesetzten Überwachungssoftware kennt. Sie kann so bereits nicht nachvollziehen, welche Eigenschaften und Fähigkeiten ein von ihr auf dem Markt beschaffter Trojaner nach seinem Design tatsächlich besitzt. Nach welchen Standards die Abwesenheit von nach dem Design dieser komplexen Softwareprodukte nicht vorgesehen Eigenschaften und Schadmöglichkeiten gesichert werden soll, bleibt ebenfalls völlig offen.

Eine richterliche Kontrolle (§§ 15b Abs. 3 Satz 2, 15c Abs. 3 Satz 3, jeweils i.V.m. § 15 Abs. 5 Satz 1 bis 9 HSOG) der Bindung des einzelnen Trojanereinsatzes an die Maßgaben der §§ 15b Abs. 2, 15c Abs. 3 Satz 1 HSOG ist hiernach unmöglich. Um diese sicherzustellen, bedarf es Kriterien, die auch in der Eilsituation einer richterlichen Anordnung operationabel sind.

Die große Streubreite möglicher Beeinträchtigungen durch fehlerhafte oder etwa nicht hinreichend gegen unbefugte Nutzung geschützte Software gebietet es, den Beschwerdeführer hiergegen Schutz und vorliegend auch den abwehrenden Rechtsschutz zu gewähren. Sie sind durch das gesetzgeberische Unterlassen in Bezug auf die notwendige Konkretisierung der Anforderungen an die Eigenschaften (usw.) in ihrem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verletzt.

E. Ergebnis

Den Verfassungsbeschwerden ist nach alledem stattzugeben.

Dr. Peter Spengler
Rechtsanwalt