BUNDESVERFASSUNGSGERICHT

- 1 BvR 1552/19 -

In dem Verfahren

über

die Verfassungsbeschwerde

1. des Herrn (…),

2. des Herrn (…),

3. des Landesverbands (…),
vertreten durch (…),

- Bevollmächtigter: (…) -

gegen § 15b und § 15c des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen vom 25. Juni 2018 (Gesetz- und Verordnungsblatt Seite 302)

hat die 1. Kammer des Ersten Senats des Bundesverfassungsgerichts durch

den Präsidenten Harbarth,

die Richterin Britz

und den Richter Radtke

gemäß § 93b in Verbindung mit § 93a BVerfGG in der Fassung der Bekanntmachung vom 11. August 1993 (BGBl I S. 1473)

am 20. Januar 2022 einstimmig beschlossen:

Die Verfassungsbeschwerde wird nicht zur Entscheidung angenommen.

G r ü n d e :

A.

Gegenstand der Verfassungsbeschwerde sind zwei Ermächtigungen nach dem Hessischen Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) zu verdeckten Zugriffen auf informationstechnische Systeme mit technischen Mitteln. 1

1. Die beiden angegriffenen Bestimmungen des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung traten in ihrer gegenwärtigen Fassung zum 4. Juli 2018 in Kraft. Während die Ermächtigung zur Online-Durchsuchung des § 15c HSOG damit neu eingefügt wurde, änderte der Landesgesetzgeber die bestehende Ermächtigung zur Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) des § 15b HSOG mit Geltung zu diesem Datum lediglich ab. 2

Die Bestimmungen lauten folgendermaßen: 3

§ 15b HSOG

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.

§ 15c HSOG

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) 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 in § 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.

2. Die Beschwerdeführer rügen mit ihrer am 3. Juli 2019 erhobenen und mit Schriftsatz vom 21. Juni 2021 ergänzten Verfassungsbeschwerde eine Verletzung ihres Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG, in Hinblick auf den Beschwerdeführer zu 3) aus Art. 2 Abs. 1 GG. 4

a) Ihre Betroffenheit leiten die Beschwerdeführer aus der intensiven Nutzung eigener wie fremder informationstechnischer Systeme, des Internets sowie unterschiedlicher Programme ab, wobei dies insbesondere im Rahmen politischer Aktivitäten, im Fall des Beschwerdeführers zu 2) auch zur Pflege von Kontakten zu Dissidenten in autoritär geführten Staaten, geschehe. Da sie von den heimlichen und mit großer Streubreite verbundenen Zugriffen möglicherweise auch langfristig nicht erführen und diese mit weiteren faktischen Beeinträchtigungen einhergehen könnten, stehe ihnen gegen die Maßnahmen kein effektiver fachgerichtlicher Rechtsschutz zur Verfügung. 5

b) Mit ihrem Vorbringen bemängeln sie im Schwerpunkt ein Regelungsdefizit für den behördlichen Umgang mit IT-Sicherheitslücken. Hierbei handelt es sich der bundesrechtlichen Begriffsbestimmung in § 2 Abs. 6 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik folgend um Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung sich Dritte gegen den Willen der Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können. Der Staat habe ein Interesse insbesondere an der Geheimhaltung von dem Programmhersteller noch unbekannten Sicherheitslücken (sogenannte Zero-Days), um diese für Online-Durchsuchung und Quellen-TKÜ ausnutzen zu können (näher zu technischen Hintergründen sowie individuellen und gesamtgesellschaftlichen Folgerisiken BVerfG, Beschluss des Ersten Senats vom 8. Juni 2021 - 1 BvR 2771/18 -, Rn. 5, 7, 36 ff. – IT-Sicherheitslücken). Werden den Polizeibehörden entsprechende Befugnisse verliehen, stelle es eine Verletzung des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme dar, dass die angegriffenen Normen und ihr weiteres Normumfeld keine Vorgaben zum Umgang mit solchen Sicherheitslücken enthielten. Nach dem objektiven Gehalt der grundrechtlichen Gewährleistung 6

müsse der Gesetzgeber den Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme auflösen, indem er grundlegende Fragen selbst regele. Sein unechtes Unterlassen führe vorliegend, da er von jedweder Regelung abgesehen habe, auch zur Verletzung eines subjektiven Rechts, insbesondere der in der grundrechtlichen Gewährleistung enthaltenen entsprechenden Schutzpflicht.

c) Weiterhin verletzten die angegriffenen Normen das Grundrecht in seiner Abwehrdimension, da der Gesetzgeber nicht sichergestellt habe, dass eine „Kompromittierung“ informationstechnischer Systeme durch die Überwachungssoftware auf unvermeidbare und verhältnismäßige Beeinträchtigungen begrenzt bleibe. Die in § 15b Abs. 2, § 15c Abs. 3 Satz 1 HSOG enthaltenen Vorgaben seien ohne Ergänzung durch ein Regelwerk, das Anforderungen an Herkunft, Beschaffung, Beschaffenheit, Eigenschaften und Funktionalitäten der Software konkretisiere, nicht vollziehbar. Stelle das Gesetz nicht einmal sicher, dass die Behörde bei Einsatz von Fremdsoftware den Quellcode kenne, könne jene deren Eigenschaften und Fähigkeiten nicht nachvollziehen und nicht für die Behebung ihrer Mängel, etwa Schadensgefahren für das Ziel- und weitere Systeme sowie unzureichenden Schutzes gegen unbefugte Nutzung, sorgen. Eine richterliche Kontrolle (vgl. § 15b Abs. 3 Satz 2, § 15c Abs. 3 Satz 3, jeweils i.V.m. § 15 Abs. 5 Satz 1 bis 9 HSOG) sei, insbesondere in Eilsituationen, mangels Kriterien nicht operationabel. 7

3. Zu der Verfassungsbeschwerde haben die Bundesregierung, die Hessische Landesregierung, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) sowie der Bayerische Landesbeauftragte für den Datenschutz und der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz Stellung genommen. 8

a) Die Bundesregierung hält das bestehende Regulierungssystem zur Gewährleistung der IT-Sicherheit und des Datenschutzes in Deutschland auch angesichts der mit Sicherheitslücken verbundenen Gefahren für ausreichend. 9

b) Nach Ansicht der Hessischen Landesregierung ist die Verfassungsbeschwerde bereits unzulässig. Sie wahre nicht den Grundsatz der Subsidiarität, weil es den Beschwerdeführern nach der jüngeren Rechtsprechung des Bundesverwaltungsgerichts potentiell möglich gewesen wäre, sich im Wege der vorbeugenden Unterlassungsklage gegen Maßnahmen nach den §§ 15b und 15c HSOG zu wenden. Dies sei zumutbar, weil sich vorliegend nicht allein verfassungsrechtliche 10

Fragen stellten, sondern es in Hinblick auf die von den Beschwerdeführern angenommene Regelungslücke technisch-fachlichen Voraufklärungsbedarf gebe.

Die Verfassungsbeschwerde setze sich auch weder substantiiert mit der einschlägigen Verfassungsrechtsprechung noch mit den Regelungen auseinander, die den vorgetragenen Defiziten entgegenwirken könnten. 11

Verfassungsrechtliche Einwände gegen die §§ 15b und 15c HSOG seien weder unter dem Gesichtspunkt eines unsachgemäßen Umgangs mit Sicherheitslücken noch dem des Schädigungspotentials der Infiltrationssoftware zu erheben. Im Hinblick auf die Möglichkeit eines unsachgemäßen Umgangs mit Sicherheitslücken sei die Gesamtheit aller Regelungen in den Blick zu nehmen, die den Eingriff in das Zielsystem steuerten und seine Folgen begrenzten. Anforderungen an die Infiltrationssoftware ließen sich nicht vollzugstauglich und zugleich in einer Weise regeln, die Nachteile für das Zielsystem schlechthin ausschlössen. Angesichts der immer schnelleren Innovationszyklen der Informationstechnologie erscheine nur das gesetzgeberische Konzept der Vorgabe technischer Möglichkeiten der Schadensvermeidung und der Ausrichtung am aktuellen Stand der Technik jeweils im Sinne eines verpflichtenden Optimierungsgebotes vollzugstauglich. Im Vorfeld einer – bislang in Hessen noch nicht erfolgten – Anwendung der Befugnisse zur präventiven Quellen-TKÜ oder Online-Durchsuchung müsse die zu nutzende Software den einheitlichen Gesamtabnahmeprozess des Bundeskriminalamts durchlaufen. Sollten sich Begrenzungs- und Beseitigungsanforderungen aus technischen Gründen nicht erfüllen lassen, liefen die Eingriffsbefugnisse leer, wären aber nach der Rechtsprechung des Bundesverfassungsgerichts nicht verfassungswidrig. 12

c) Die Datenschutzbeauftragten erachten für die Nutzung von Sicherheitslücken einen Ausgleich des benannten Zielkonflikts durch klarere und bestimmte Regelungen für geboten; der BfDI hält zudem konkretere gesetzliche Vorgaben für die Beschaffenheit der eingesetzten Überwachungssoftware für notwendig. 13

B.

Die Verfassungsbeschwerde ist nicht zur Entscheidung anzunehmen. Die Voraussetzungen des § 93a Abs. 2 BVerfGG liegen nicht vor. Der Verfassungsbeschwerde kommt weder grundsätzliche verfassungsrechtliche Bedeutung zu, noch ist sie zur Durchsetzung von Grundrechten oder grundrechtsgleichen Rechten der 14

Beschwerdeführer angezeigt, da sie keine hinreichende Aussicht auf Erfolg hat (vgl. BVerfGE 90, 22 <25 f.>). Sie ist unzulässig, weil sie die Begründungserfordernisse nach § 23 Abs. 1 Satz 2, § 92 BVerfGG nicht erfüllt.

I.

Soweit die Beschwerdeführer unzureichende Vorgaben zum Umgang mit Sicherheitslücken rügen, haben sie weder ihre Beschwerdebefugnis noch die Wahrung des Grundsatzes der Subsidiarität im weiteren Sinne hinreichend begründet. 15

1. Bei einer gegen ein Gesetz gerichteten Verfassungsbeschwerde müssen die Beschwerdeführenden bezüglich ihrer Beschwerdebefugnis darlegen und entsprechend begründen, durch die angegriffenen Normen selbst, gegenwärtig und unmittelbar betroffen zu sein (vgl. BVerfGE 102, 197 <206>; 108, 370 <384>). Weiterhin muss sich aus ihrem Vorbringen mit hinreichender Deutlichkeit die Möglichkeit einer Verletzung von Grundrechten oder grundrechtsgleichen Rechten ergeben (vgl. BVerfGE 28, 17 <19>; 89, 155 <171>; 99, 84 <87>; stRspr). Die Beschwerdeführenden müssen aufzeigen, mit welchen verfassungsrechtlichen Anforderungen die angegriffene Maßnahme kollidiert (vgl. BVerfGE 108, 370 <386>). Im Falle der Behauptung einer gesetzgeberischen Schutzpflichtverletzung ergeben sich zudem spezifische Darlegungslasten dahingehend, dass über den Vortrag angeblicher Unzulänglichkeiten der Rechtslage hinaus der gesetzliche Regelungszusammenhang insgesamt erfasst sein muss, wozu – je nach Fallgestaltung – zumindest gehört, dass die einschlägigen Regelungen des als unzureichend beanstandeten Normkomplexes jedenfalls in Grundzügen dargestellt werden und begründet wird, warum vom Versagen der gesetzgeberischen Konzeption ausgegangen wird (vgl. BVerfG, Beschluss des Ersten Senats vom 8. Juni 2021 - 1 BvR 2771/18 -, Rn. 51 – IT-Sicherheitslücken). 16

Zwar kann durch die angegriffenen Befugnisse die grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in ihrer Schutzdimension betroffen sein und sich hieraus eine konkrete Schutzpflicht des Gesetzgebers ergeben, den Umgang mit Sicherheitslücken zu regeln (vgl. BVerfG, a.a.O., Rn. 26 ff.). Die Verfassungsbeschwerde setzt sich mit dem bestehenden gesetzlichen Regelungskonzept und seinen Defiziten in Hinblick auf die Erfüllung einer solchen Schutzpflicht jedoch allenfalls ansatzweise auseinander. Die Beschwerdeführer bemängeln lediglich, dass die §§ 15b und 15c HSOG selbst keine Regelungselemente zur Auflösung des zu adressierenden Zielkonflikts bereitstel- 17

len. Die in den angegriffenen Regelungen enthaltenen expliziten Anforderungen an den Einsatz der darin zugelassenen Maßnahmen werden bloß benannt und in Hinblick auf ihre Tauglichkeit zur Steuerung der Beschaffenheit, der Funktionalität und der Anwendungskontrolle der Überwachungssoftware hin knapp untersucht. Auf eine mögliche Auslegung der angegriffenen sowie weiterer Normen dahingehend, dass ihnen im Wege der (verfassungskonformen) Auslegung Elemente eines Regelungskonzepts für die Erfüllung der Schutzpflicht zugewiesen werden können, gehen die Beschwerdeführer nicht ein. Denkbar wäre etwa, die gesetzliche Vorgabe zum Schutz des eingesetzten Mittels gegen unbefugte Nutzung (so ausdrücklich § 15b Abs. 2 Satz 2 HSOG) in dem Sinne zu deuten, dass dies (auch) durch eine Meldung an den Hersteller geschehen könne (vgl. BVerfG, a.a.O., Rn. 54 f.). Soweit die Beschwerdeführer weiterhin der Ansicht sind, das von ihnen angeführte Defizit der angegriffenen Normen werde auch sonst nicht durch gesetzliche Bestimmungen ausgeglichen, hätte es insbesondere zusätzlichen Vortrags bedurft, warum das bestehende Meldeverfahren des IT-Planungsrats nicht bereits einen wirkungsvollen Beitrag zu einem hinreichenden Umgang mit Sicherheitslücken leiste (vgl. BVerfG, a.a.O., Rn. 65 f.). Weiterhin mangelt es der Verfassungsbeschwerde an einer näheren Auseinandersetzung mit der möglichen Schutzwirkung unionsrechtlicher Regelungen, namentlich der 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 und dem unter anderem zu deren Umsetzung erlassenen Hessischen Datenschutz- und Informationsfreiheitsgesetz, dessen § 62 etwa die Durchführung einer Datenschutz-Folgenabschätzung vorsieht (vgl. hierzu BVerfG, a.a.O., Rn. 56 ff.).

2. Ferner ist insoweit auch nicht genügend dargetan, dass die Anforderungen 18
des Grundsatzes der Subsidiarität im weiteren Sinne gewahrt sind. Dieser erfordert, dass über die Ergreifung der zur Erreichung des unmittelbaren Prozessziels förmlich eröffneten Rechtsmittel hinaus alle Mittel genutzt werden, die der geltend gemachten Grundrechtsverletzung abhelfen können. Das gilt auch, wenn zweifelhaft ist, ob ein entsprechender Rechtsbehelf statthaft ist und im konkreten Fall in zulässiger Weise eingelegt werden kann. Zur Erfüllung der hierauf bezogenen Darlegungserfordernisse hätte es einer hinreichenden Begründung bedurft, warum vorliegend die Erhebung einer verwaltungsgerichtlichen Feststellungs- oder Unter-

lassungsklage trotz der wie ausgeführt bestehenden Fragen zur Auslegung des einfachen Rechts nicht möglich oder nicht erforderlich gewesen sein sollte (näher BVerfG, a.a.O., Rn. 68 ff. m.w.N.).

II.

Soweit die Beschwerdeführer eine Verletzung der grundrechtlichen Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch die angegriffenen Regelungen zudem in Hinblick auf fehlende Vorgaben für die Beschaffenheit, Funktionalität und Anwendungskontrolle der Überwachungssoftware rügen, genügt die Verfassungsbeschwerde – unabhängig davon, ob man hierin eine Schutzpflichtverletzung oder wie vorgetragen eine Verletzung in der Abwehrdimension des Grundrechts erblickte – ebenfalls nicht den Begründungsanforderungen. Die hierfür relevante Rechtsprechung des Bundesverfassungsgerichts wird lediglich angeführt, ohne sich mit ihrer Bedeutung für die vorliegende Konstellation näher auseinanderzusetzen. Dies gilt vor allem für die Entscheidung zum Bundeskriminalamtsgesetz, in der vergleichbare Regelungen zur Minimierung möglicher Folgeschäden heimlicher Überwachungsmaßnahmen als verhältnismäßig angesehen wurden (vgl. BVerfGE 141, 220 <305 f. Rn. 215>, dort unter Verweis auf BVerfGE 120, 274 <325 f.>). Eine weitere normative Konkretisierung der gesetzlichen Schutzvorkehrungen wurde in der Entscheidung nicht eingefordert, sondern ausdrücklich betont, dass deren fehlende technische Umsetzbarkeit keinen Mangel darstelle, der auf die Gültigkeit der Norm durchschlage, sondern lediglich ein Leerlaufen der Vorschrift zur Folge habe (vgl. BVerfGE 141, 220 <311 Rn. 234>). Im Übrigen fehlt es auch an einer hinreichenden Auseinandersetzung mit einfachrechtlichen Normen des nationalen wie des Unionsrechts sowie behördlicher Prüfungsprozesse, insbesondere im Rahmen der Einbindung in den einheitlichen Gesamtabnahmeprozess des Bundeskriminalamts. 19

Ob der Vortrag darüber hinaus auch hinsichtlich der Wahrung des Grundsatzes der Subsidiarität den Begründungsanforderungen nicht genügt oder damit ein hinreichender Grad der Wahrscheinlichkeit der Selbstbetroffenheit der Beschwerdeführer (vgl. BVerfG, Beschluss der 3. Kammer des Ersten Senats vom 19. April 2021 - 1 BvR 1732/14 -, Rn. 31 ff.) auch in Hinblick auf die von ihnen gerügte grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ausgewiesen ist, kann danach dahinstehen. 20

Von einer weiteren Begründung wird nach § 93d Abs. 1 Satz 3 BVerfGG abgesehen. 21

Diese Entscheidung ist unanfechtbar. 22

Harbarth Britz Radtke