L e i t s ä t z e

zum Beschluss des Ersten Senats vom 8. Juni 2021

- 1 BvR 2771/18 -

(IT-Sicherheitslücken)

1. Art. 10 Abs. 1 GG begründet neben einem Abwehrrecht einen Auftrag an den Staat, vor dem Zugriff privater Dritter auf die dem Fernmeldegeheimnis unterfallende Kommunikation zu schützen (Bestätigung von BVerfGE 106, 28 <37>).

2. a) Die grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verpflichtet den Staat, zum Schutz der Systeme vor Angriffen durch Dritte beizutragen.

   b) Die grundrechtliche Schutzpflicht des Staates verlangt auch eine Regelung zur grundrechtskonformen Auflösung des Zielkonflikts zwischen dem Schutz informationstechnischer Systeme vor Angriffen Dritter mittels unbekannter Sicherheitslücken einerseits und der Offenhaltung solcher Lücken zur Ermöglichung einer der Gefahrenabwehr dienenden Quellen-Telekommunikationsüberwachung andererseits.

3. Für die Geltendmachung einer gesetzgeberischen Schutzpflichtverletzung bestehen spezifische Darlegungslasten. Eine solche Verfassungsbeschwerde muss den gesetzlichen Regelungszusammenhang insgesamt erfassen. Dazu gehört, dass die einschlägigen Regelungen des beanstandeten Normkomplexes jedenfalls in Grundzügen dargestellt werden und begründet wird, warum diese verfassungsrechtlich unzureichend schützen.

4. Richtet sich eine Verfassungsbeschwerde unmittelbar gegen ein Gesetz, kann nach dem Grundsatz der Subsidiarität auch die Erhebung einer verwaltungsgerichtlichen Feststellungs- oder Unterlassungsklage zu den zuvor zu ergreifenden Rechtsbehelfen gehören. Das ist nicht erforderlich, wenn die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft und von einer vorausgegangenen fachgerichtlichen Prüfung keine verbesserte Entscheidungsgrundlage zu erwarten wäre (stRspr). Dies gilt auch im Falle der Rüge einer gesetzgeberischen Schutzpflichtverletzung.

BUNDESVERFASSUNGSGERICHT

- 1 BvR 2771/18 -

IM NAMEN DES VOLKES

In dem Verfahren
über
die Verfassungsbeschwerde

1. des Herrn Dr. K…,
2. des Herrn M…,
3. des Herrn W…,
4. des Herrn F.-D…,
5. des C... e.V.,
   vertreten durch den Vorstand,
6. der I… eG,
   vertreten durch den Vorstand,
7. der O… GbR,
   vertreten durch ihre geschäftsführenden Gesellschafter

- Bevollmächtigter: … -

gegen § 54 Absatz 2 des Polizeigesetzes Baden-Württemberg (PolG BW) in der Fassung des Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 für die Polizei in Baden-Württemberg und zur Änderung weiterer polizeirechtlicher Vorschriften vom 6. Oktober 2020 (Gesetzblatt Seite 735)

hat das Bundesverfassungsgericht – Erster Senat –
unter Mitwirkung der Richterinnen und Richter
Präsident Harbarth,
Paulus,
Baer,
Britz,
Ott,
Christ,
Radtke,
Härtel
am 8. Juni 2021 beschlossen:

Die Verfassungsbeschwerde wird zurückgewiesen.

G r ü n d e :

A.

Die Verfassungsbeschwerde betrifft den Umgang der Polizeibehörden mit Sicherheitslücken in Programmen oder sonstigen informationstechnischen Systemen, die den Systemherstellern nicht bekannt sind (sogenannte Zero-Day-Schwachstellen). Die Beschwerdeführenden wenden sich dagegen, dass die Behörden ihnen bekannte Sicherheitslücken möglicherweise nicht melden, weil sie deren Schließung durch den Hersteller vermeiden wollen, um die Lücken für die Durchführung einer polizeilichen Überwachungsmaßnahme verwenden zu können. Hintergrund der Verfassungsbeschwerde ist die landesrechtliche Ermächtigung der Polizeibehörden zur Quellen-Telekommunikationsüberwachung, die mit Hilfe solcher Zero-Day-Schwachstellen durchgeführt werden kann. 1

I.

1. Mit Wirkung vom 8. Dezember 2017 fügte der Landesgesetzgeber in das Polizeigesetz Baden-Württemberg einen neuen § 23b ein (GBl 2017 S. 624), der in seinem Absatz 2 die hier angegriffene Ermächtigung zur Quellen-Telekommunikationsüberwachung enthielt. Mit dem nach Eingang der Verfassungsbeschwerde verabschiedeten Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 für die Polizei in Baden-Württemberg und zur Änderung weiterer polizeirechtlicher Vorschriften vom 6. Oktober 2020 (GBl S. 735), das am 17. Januar 2021 in Kraft trat, wurde die Befugnis zur Quellen-Telekommunikationsüberwachung in den hier relevanten Teilen unverändert in den neuen § 54 Abs. 2 PolG BW übernommen. Die Beschwerdeführenden haben ihre Verfassungsbeschwerde mit Schriftsatz vom 10. März 2021 auf den neuen § 54 Abs. 2 PolG BW umgestellt. 2

§ 54 PolG BW hat in den hier relevanten Absätzen folgenden Wortlaut: 3

§ 54 PolG BW

Überwachung der Telekommunikation

(1) Der Polizeivollzugsdienst kann ohne Wissen der betroffenen Person die Telekommunikation einer Person überwachen und aufzeichnen,

1. die nach den §§ 6 oder 7 verantwortlich ist, und dies zur Abwehr einer dringenden und erheblichen Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen geboten ist,

2. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat begehen wird, die sich gegen die in Nummer 1 genannten Rechtsgüter richtet und dazu bestimmt ist,

a) die Bevölkerung auf erhebliche Weise einzuschüchtern,

b) eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder

c) die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen,

und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können,

3. deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines überschaubaren Zeitraums eine Straftat begehen wird, die sich gegen die in Nummer 1 genannten Rechtsgüter richtet und dazu bestimmt ist,

a) die Bevölkerung auf erhebliche Weise einzuschüchtern,

b) eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder

c) die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen,

und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können,

4. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach Nummer 1 bestimmte oder von dieser herrührende Mitteilungen entgegennimmt oder weitergibt, oder

5. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person nach Nummer 1 deren Telekommunikationsanschluss oder Endgerät benutzen wird.

Datenerhebungen dürfen nur durchgeführt werden, wenn sonst die Erfüllung der polizeilichen Aufgabe aussichtslos oder wesentlich erschwert würde. Die Datenerhebung darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Die Überwachung und Aufzeichnung der Telekommunikation darf ohne Wissen der betroffenen Person in der Weise erfolgen, dass mit technischen Mitteln in von ihr genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und

2. der Eingriff notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

(3) Bei Maßnahmen nach Absatz 2 ist 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 gegen unbefugte Nutzung zu schützen. Kopierte Daten sind gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

[…]

2. Die Beschwerdeführenden wenden sich gegen die Befugnis zur Quellen-Telekommunikationsüberwachung, weil diese zur Folge habe, dass zur Durchführung der Überwachung Sicherheitslücken des informationstechnischen Systems, 4

die der Behörde, nicht aber dem Hersteller bekannt seien, offen gehalten würden, was Angriffe von dritter Seite ermögliche.

a) Die Ausnutzung von Sicherheitslücken im informationstechnischen System ist eine von mehreren Möglichkeiten, wie eine Quellen-Telekommunikationsüberwachung nach § 54 PolG BW durchgeführt werden kann. Zur Ermöglichung einer solchen Überwachung muss das Zielsystem mit einer Überwachungssoftware infiltriert werden. Auf welche Weise dies geschieht, ist gesetzlich nicht geregelt. Denkbar ist eine Infiltration auf „physischem“ Weg. Dabei wird die Software durch einen Ermittler vor Ort auf das Zielsystem aufgespielt, etwa nach einem heimlichen Betreten der Wohnung, einem Zugang zur Wohnung durch verdeckte Ermittler oder außerhalb der Wohnung beispielsweise bei einer Zoll- oder Verkehrskontrolle. Alternativ kann das Zielsystem über einen Fernzugriff infiltriert werden. Dies kann geschehen, indem der Zielperson die Infiltrationssoftware als E-Mail-Anhang zugespielt und dann von dieser Person geöffnet wird oder indem Sicherheitslücken in der Hard- oder Software des Zielsystems ausgenutzt werden. Letzteres kann insbesondere im Vergleich zu den sich aus Art. 13 GG ergebenden Grenzen für ein physisches Betreten der Wohnung und zu Zugriffen, die ein Fehlverhalten des Nutzers voraussetzen, praktische Vorteile bieten. Die Verfassungsbeschwerde richtet sich allein gegen diese Ausnutzung von Sicherheitslücken. 5

b) Was unter einer Sicherheitslücke zu verstehen ist, ist in § 2 Abs. 6 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz <BSIG>) gesetzlich definiert: 6

§ 2 BSIG

Begriffsbestimmungen

[…]

(6) Sicherheitslücken im Sinne dieses Gesetzes sind Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können.

Sicherheitslücken lassen sich danach unterscheiden, ob sie dem Hersteller bereits bekannt sind (sogenannte N-Days, weil der Hersteller sie bereits eine be- 7

stimmte Zahl von Tagen kennt) oder noch unbekannt sind (sogenannte Zero-Days, weil der Hersteller sie noch null Tage kennt). Zwischen beiden besteht aus der Perspektive der Sicherheit in der Informationstechnik (IT-Sicherheit) ein grundlegender Unterschied, da der Hersteller ihm bekannte Sicherheitslücken schließen kann, ihm unbekannte Lücken hingegen allenfalls zufällig im Zuge anderer Aktualisierungen geschlossen werden. Auch aus Sicht der Polizeibehörden besteht ein Unterschied. Eine N-Day-Schwachstelle kann nur dann noch zur Infiltration des Zielsystems genutzt werden, wenn der Hersteller trotz Kenntnis noch keine Aktualisierung bereitgestellt hat oder solche Updates generell nicht mehr erfolgen. Außerdem können N-Day-Schwachstellen dann noch genutzt werden, wenn zwar ein Update vom Hersteller bereitgestellt wurde, der betroffene Nutzer dieses aber noch nicht installiert hat. Eine Zero-Day-Schwachstelle kann hingegen ohne Weiteres zur Infiltration des Zielsystems genutzt werden, weil der Hersteller mangels Kenntnis von der jeweiligen Schwachstelle keine Aktualisierung entwickeln und zur Verfügung stellen kann, welche die Lücke schließen würde.

II.

Mit ihrer Verfassungsbeschwerde wenden sich die Beschwerdeführenden gegen § 54 Abs. 2 PolG BW. Sie machen im Kern geltend, diese Befugnis gefährde die Vertraulichkeit und Integrität ihrer informationstechnischen Systeme, weil die Behörden kein Interesse daran hätten, die ihnen bekannten Schwachstellen an die Hersteller zu melden, da sie diese Sicherheitslücken für eine Infiltration informationstechnischer Systeme zur durch § 54 Abs. 2 PolG BW gestatteten Quellen-Telekommunikationsüberwachung nutzen könnten. 8

Mit ihrer am 7. Dezember 2018 erhobenen und mit Schriftsatz vom 10. März 2021 ergänzten Verfassungsbeschwerde rügen die Beschwerdeführenden eine Verletzung der grundrechtlich gewährleisteten Vertraulichkeit und Integrität informationstechnischer Systeme. Sie greifen § 54 Abs. 2 PolG BW ausdrücklich nicht deshalb an, weil der Staat hierdurch zum Eingriff in ihre Grundrechte ermächtigt werde. Vielmehr beanstanden sie, dass das Land Baden-Württemberg durch die Einführung der Befugnis zur Quellen-Telekommunikationsüberwachung seine aus der objektiv-rechtlichen Dimension des Grundrechts erwachsende Schutzpflicht verletzt habe. Zwar bestehe diese Schutzpflicht unabhängig von der Befugnis zur Quellen-Telekommunikationsüberwachung. Die Einführung der Befugnis aktualisiere diese aber im Hinblick auf die damit einhergehende Risikoerhöhung und mache konkrete gesetzliche Vorgaben zum Schutz informationstechnischer Systeme 9

erforderlich. Der Gesetzgeber begründe durch § 54 Abs. 2 PolG BW einen Anreiz für Polizeibehörden, Sicherheitslücken – die auch für Kriminelle oder ausländische Geheimdienste interessant seien – nicht zu melden. Auch für die Sicherheitsforschung entstehe ein Anreiz, entdeckte Schwachstellen nicht dem Hersteller zu melden, um sie vielmehr an Behörden verkaufen zu können. § 54 Abs. 2 PolG BW schaffe damit eine Gefahr, zu deren Abwehr der Gesetzgeber verfassungsrechtlich verpflichtet sei.

Das Land habe versäumt, die zwingend gebotenen Begleitregelungen für ein Schwachstellen-Management zu schaffen, das insbesondere die Verwendung von Sicherheitslücken verbieten müsse, die dem Hersteller des betreffenden Systems nicht bekannt seien. Selbst wenn man eine Ausnutzung von Zero-Day-Lücken nicht für schlechthin mit der staatlichen Schutzpflicht unvereinbar halte, müsse jedenfalls ein Verwaltungsverfahren vorgesehen – und angesichts der Grundrechtsrelevanz durch formelles Gesetz eingeführt – werden, mit dem eine damit zu betrauende Behörde die ihr bekannt werdenden Sicherheitslücken auf ihre Bedeutung hin untersuchen und einstufen müsse, um auf dieser Grundlage über den Umgang mit den Lücken zu entscheiden. Außerdem müsse der Staat Vorkehrungen dagegen treffen, dass seine Kenntnis von Sicherheitslücken von Dritten erbeutet werde. Bislang gebe es keinen Prozess zur Bewertung von Schwachstellen, die baden-württembergische Behörden zur Quellen-Telekommunikationsüberwachung nutzen wollten, und auch keine Verfahren und Kriterien, nach denen über eine Meldung der betreffenden Schwachstelle an die Hersteller entschieden werden könne. 10

Die angegriffene Norm betreffe die Beschwerdeführenden unmittelbar, weil es keiner weiteren gegen sie gerichteten Akte bedürfe. Ihre Betroffenheit folge gerade aus der durch staatliche Stellen erhöhten Gefahr für ihre informationstechnischen Systeme, weil die Polizei wegen § 54 Abs. 2 PolG BW die von ihr in Erfahrung gebrachten Sicherheitslücken nicht an die Hersteller der betroffenen Programme melde. Es könne ihnen nicht abverlangt werden, zur Begründung ihrer Verfassungsbeschwerde eine bestimmte, vom Staat geheim gehaltene Schwachstelle zu benennen, da sie von den konkreten den Behörden bekannten Schwachstellen keine Kenntnis erlangten. Die Gefährdungslage bestehe auch unabhängig davon, ob die Polizei in Baden-Württemberg derzeit tatsächlich Zero-Day-Schwachstellen beschaffe oder sammele. Entscheidend sei allein, dass sie solche Schwachstellen – etwa durch von anderen Stellen bereitgestellte Ausforschungssoftware, deren Bestandteil die Schwachstellen seien – nutze. Bereits dadurch 11

entstehe ein Anreiz dafür, dass Schwachstellen nicht an Hersteller gemeldet würden.

III.

1. Die Bundesregierung hält das bestehende Regulierungssystem zur Gewährleistung der IT-Sicherheit und des Datenschutzes in Deutschland auch angesichts der mit Schwachstellen informationstechnischer Systeme verbundenen Gefahren für ausreichend. Das Spannungsverhältnis zwischen den mit der Quellen-Telekommunikationsüberwachung verfolgten Zielen, die dem Schutz überragend wichtiger anderer Rechtsgüter dienten, und dem Ziel der Gewährleistung einer größtmöglichen IT-Sicherheit sei innerhalb der Spielräume des Gesetzgebers unter größtmöglichem Schutz für alle betroffenen Rechtsgüter aufzulösen. Einerseits gingen von Schwachstellen informationstechnischer Systeme Gefahren aus, weshalb grundsätzlich eine möglichst geringe Zahl an offenen Schwachstellen anzustreben sei. Andererseits liefen rechtliche Befugnisse zur Quellen-Telekommunikationsüberwachung ohne die Möglichkeit, Schwachstellen zu nutzen, vielfach ins Leere, wenn eine Infiltration auf anderen Wegen nicht gelänge. Die Quellen-Telekommunikationsüberwachung sei aber als Mittel zur Gefahrenabwehr zunehmend erforderlich, da immer häufiger eine Ende-zu-Ende-Verschlüsselung genutzt werde, um Tat- und Kommunikationsmittel bewusst einem Zugriff durch Strafverfolgungs- und Sicherheitsbehörden zu entziehen. 12

2. Für die Landesregierung Baden-Württemberg hat das Ministerium für Inneres, Digitalisierung und Migration Stellung genommen. Es hält die Verfassungsbeschwerde für unbegründet. Es bestehe bereits deswegen keine verfassungsrechtliche Pflicht zur Schaffung weitergehender Schutzvorschriften, weil die baden-württembergische Polizei im Zusammenhang mit der präventivpolizeilichen Quellen-Telekommunikationsüberwachung nicht gezielt Zero-Day-Sicherheitslücken beschaffe oder sammle. Jedenfalls sei das bestehende System aus Rechtsvorschriften und weiteren Schutzmaßnahmen geeignet und ausreichend, um den behaupteten negativen Folgen der Quellen-Telekommunikationsüberwachung entgegenzuwirken und vor kriminellen Eingriffen in informationstechnische Systeme durch die Nutzung solcher Schwachstellen effektiv zu schützen. 13

Aus der grundrechtlichen Schutzpflicht lasse sich keine Meldepflicht der Polizei für Schwachstellen an die Softwarehersteller ableiten. Die Gewährleistung der IT-Sicherheit und der Schutz vor unberechtigtem Zugriff auf informationstechni- 14

sche Systeme obliege in erster Linie den Herstellern und Anbietern von Software, die dem mit erheblichem Aufwand nachkämen. Eine teilweise Verlagerung der Verantwortung für die Sicherheit der Systeme auf die Polizei durch die Schaffung von gesetzlichen Meldepflichten an die Hersteller sei verfassungsrechtlich nicht geboten. Außerdem sei zu berücksichtigen, dass die Befugnis zur Quellen-Telekommunikationsüberwachung der Erfüllung der polizeilichen Aufgabe der Gefahrenabwehr in Fällen besonders dringender oder erheblicher Gefahren für bedeutende Rechtsgüter diene. Da die Telekommunikation zunehmend von-Ende-zu-Ende verschlüsselt werde, laufe parallel auch die allgemeine Befugnis zur präventiven Telekommunikationsüberwachung ohne die Befugnis zur Quellen-Telekommunikationsüberwachung allmählich leer. Dabei sei die Polizei auf die Ausnutzung von Schwachstellen angewiesen, wenn kein direkter Zugriff auf das genutzte Gerät möglich sei. Auch der mögliche Zielkonflikt zwischen der Gewährleistung der IT-Sicherheit und der Erfüllung des gesetzlichen Auftrags der Polizei erzeuge keinen gesetzgeberischen Handlungsbedarf. Da die bloße Nutzung unbekannter Sicherheitslücken die IT-Sicherheit nicht gefährde, bestehe kein Anlass für ein gesetzliches Verbot oder für Regelungen, die die Nutzung solcher Sicherheitslücken einschränkten oder zu deren Meldung an die Hersteller verpflichteten.

Eine verfassungsrechtliche Notwendigkeit für weitergehende gesetzliche Re- 15
gelungen bestehe auch deshalb nicht, weil der Schutz informationstechnischer Systeme gegen den unberechtigten Zugriff Dritter durch zahlreiche Vorschriften gewährleistet werde. Die Regelungen des § 54 PolG BW – insbesondere § 54 Abs. 3 Satz 2 PolG BW – stellten sicher, dass die Durchführung der Quellen-Telekommunikationsüberwachung Dritten nicht die Möglichkeit biete, auf das betroffene System oder die der Polizei bekannten Sicherheitslücken zuzugreifen. Außerdem sei Aufgabe der Polizei auch die Verhinderung von Straftaten, bei denen Dritte unbekannte Sicherheitslücken ausnutzten und informationstechnische Systeme manipulierten, weshalb sie gemäß § 3 PolG BW nach pflichtgemäßem Ermessen die erforderlichen Maßnahmen zu ergreifen habe, wenn ihr entsprechende Sicherheitslücken bekannt würden. Die Polizei habe bei ihrer Gefährdungsanalyse im Rahmen der §§ 1, 3 und 5 PolG BW ohnehin die Gesichtspunkte der Verbreitung und des Gewichts der Sicherheitslücke zu berücksichtigen, ebenso wie die Wahrscheinlichkeit von Gegenmaßnahmen und einer technischen Lösung für die Schließung der Lücke, die Wahrscheinlichkeit, dass die Lücke von Dritten aufgefunden werde, und schließlich den möglichen Schaden durch eine kriminelle Ausnutzung der Lücke. Eine weitere gesetzliche Regelung habe keinen Mehrwert. Zudem schütze der Staat diese Systeme durch das Strafrecht vor

Übergriffen Privater. Aus dem Datenschutzrecht sei insbesondere die Umsetzung des Art. 29 der Richtlinie (EU) 2016/680 (JI-Richtlinie <JI-RL>) zur Gewährleistung der Sicherheit der Datenverarbeitung in § 78 PolG BW zu berücksichtigen.

Weiter verweist die Landesregierung auf die Aufgaben des Bundesamts für Sicherheit in der Informationstechnik. Der Verbesserung der Cybersicherheit diene außerdem der Entwurf des – zwischenzeitlich verabschiedeten (unten Rn. 63 f.) – baden-württembergischen Gesetzes zur Verbesserung der Cybersicherheit. Danach solle die Landesoberbehörde „Cybersicherheitsagentur Baden-Württemberg“ errichtet werden. Eine ihrer wesentlichen Aufgaben werde der Betrieb einer zentralen Koordinierungs- und Meldestelle für die Zusammenarbeit der öffentlichen Stellen in allen Angelegenheiten der Cybersicherheit in Baden-Württemberg sein. 16

3. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist der Auffassung, die angegriffene Rechtsvorschrift genüge nicht dem verfassungsrechtlichen Gebot, informationstechnische Systeme gegen Dritte zu schützen. Sicherheitslücken informationstechnischer Systeme – insbesondere solche, die dem Hersteller nicht bekannt seien – begründeten ein enormes Gefährdungspotential für die Vertraulichkeit der Kommunikation und für die Privatsphäre der Bürgerinnen und Bürger, da die Gefahr einer Ausspähung durch Dritte bestehe. Erlaube ein Gesetz den Sicherheitsbehörden die Ausnutzung von Sicherheitslücken, müsse es auch die Einzelheiten regeln. Dazu gehöre etwa, in welchem Umfang Sicherheitsbehörden Informationen über Sicherheitslücken „bevorraten“ dürften, oder die Verpflichtung zur Weitergabe der Information an die betroffenen Hersteller oder das Bundesamt für Sicherheit in der Informationstechnik. Diese Anforderungen seien nicht erfüllt. 17

4. Der Bayerische Landesbeauftragte für den Datenschutz teilt die verfassungsrechtlichen Bedenken der Beschwerdeführenden. Die verfassungsrechtliche Notwendigkeit von Schutzmaßnahmen ergebe sich auch daraus, dass die öffentliche Hand selbst das Sicherheitsniveau informationstechnischer Systeme nichtöffentlicher Stellen rechtlich steuere. Es könne ein Widerspruch entstehen, wenn staatliche Stellen ein hinreichendes Sicherheitsniveau bei informationstechnischen Systemen bescheinigten, die dann aber von der Polizei durch Ausnutzung unbekannter Sicherheitslücken infiltriert würden. Dieses Spannungsverhältnis sei durch hinreichend klare und bestimmte Regelungen aufzulösen. Diese müssten sowohl die Voraussetzungen der Infiltration des Zielsystems als auch die Grenzen der 18

Beschaffung und der Zurückhaltung von Erkenntnissen über bislang allgemein unbekannt gebliebene Sicherheitslücken hinreichend klar beschreiben.

5. Der Landesdatenschutzbeauftragte Rheinland-Pfalz ist ebenfalls der Auf- 19
fassung, dass die Regelungen des Polizeigesetzes Baden-Württemberg keine hinreichend konkreten gesetzlichen Anforderungen an den allgemeinen Schutz informationstechnischer Systeme enthielten. Der Grundrechtsschutz werde in Bezug auf die Gefahren, die von offen gehaltenen Zero-Day-Sicherheitslücken ausgingen, nicht hinreichend effektiv gewährleistet. Es fehle an Vorschriften, die dazu verpflichteten, die Sicherheitslücken, die zum Aufspielen der Software genutzt würden, zu schließen oder allgemein eine Bewertung der Auswirkungen der Maßnahmen in Bezug auf die kollektive IT-Sicherheit vorzunehmen.

B.

Die Verfassungsbeschwerde ist unzulässig, weil die Möglichkeit einer Verlet- 20
zung der bestehenden Schutzpflicht nicht hinreichend dargelegt ist und weil sie die Anforderungen der Subsidiarität im weiteren Sinne nicht wahrt.

I.

Die Beschwerdeführenden können grundsätzlich Träger von Grundrechten 21
und damit beschwerdefähig sein. Das gilt auch für die Beschwerdeführenden zu 5 bis 7, die als eingetragener Verein (vgl. BVerfGE 3, 383 <390>; 10, 221 <225>; 24, 278 <282>; 97, 228 <253>; 105, 279 <292 f.>), als eingetragene Genossenschaft (vgl. BVerfGE 118, 168 <168, 203>) und als Gesellschaft des bürgerlichen Rechts (vgl. BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 2. September 2002 - 1 BvR 1103/02 -, Rn. 6) und damit als inländische juristische Personen im Sinne des Art. 19 Abs. 3 GG grundrechtsberechtigt sind. Juristische Personen können sich grundsätzlich auf die von den Beschwerdeführenden geltend gemachte grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme berufen, soweit dieses nicht auf Art. 1 Abs. 1 GG gestützt ist (vgl. Drallé, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, 2010, S. 68 ff.; Heinemann, Grundrechtlicher Schutz informationstechnischer Systeme, 2015, S. 153; Gersdorf, in: BeckOK InfoMedienR, 30. Ed. 1. August 2019, GG, Art. 2 Rn. 33). Ihr Schutzbedürfnis ist hier dem natürlicher Personen ähnlich. Allerdings ergibt sich insoweit ein Unterschied, als der Tätigkeitskreis juristischer Personen anders als der natürlicher Personen in der Regel durch eine bestimmte Zwecksetzung be-

grenzt wird. Die Unterschiede, die zwischen den Schutzbedürfnissen natürlicher und juristischer Personen bestehen, sind bei der Bestimmung der grundrechtlichen Gewährleistung zu beachten (vgl. entsprechend zum Recht auf informationelle Selbstbestimmung BVerfGE 118, 168 <203 f.>; 128, 1 <43>; vgl. zu Art. 10 Abs. 1 GG BVerfGE 100, 313 <356>; 106, 28 <43>; 107, 299 <310>).

II.

Die Verfassungsbeschwerde hat einen zulässigen Beschwerdegegenstand. Die Beschwerdeführenden wenden sich unmittelbar gegen § 54 Abs. 2 PolG BW. Dieser verletze ihre Grundrechte, soweit er erlaube, zur Durchführung von Eingriffen in informationstechnische Systeme mit technischen Mitteln auch Schwachstellen dieser Systeme auszunutzen, die den jeweiligen Herstellern noch nicht bekannt sind, ohne diese zuvor dem Hersteller melden zu müssen. Hilfsweise machen sie geltend, der Gesetzgeber verletze ihre Grundrechte, indem er es unterlassen habe, begleitend zu § 54 Abs. 2 PolG BW ein gesetzliches Schwachstellenmanagement-Verfahren zur Bewertung von Sicherheitslücken im Einzelfall einzuführen. Beides stützen die Beschwerdeführenden auf die Schutzdimension der grundrechtlichen Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Sie machen geltend, der Gesetzgeber habe durch das Unterlassen entsprechender Begleitregelungen gegen seine Schutzpflicht verstoßen. Ihre Beschwerde richtet sich also gegen eine aus ihrer Sicht grundrechtlich unzureichende gesetzliche Vorschrift. Dies ist zulässig (vgl. zuletzt BVerfG, Beschluss des Ersten Senats vom 24. März 2021 - 1 BvR 2656/18 u.a. -, Rn. 95 – Klimaschutz). 22

III.

Dass im hier relevanten Kontext mit der JI-Richtlinie datenschutzrechtliche Vorschriften der Europäischen Union bestehen, steht der Zulässigkeit der Verfassungsbeschwerde nicht entgegen. Weder die angegriffene Vorschrift selbst noch die von den Beschwerdeführenden als fehlend gerügten Regelungselemente sind vollständig unionsrechtlich determiniert (vgl. BVerfGE 121, 1 <15>; 125, 260 <306 f.>; 130, 151 <177 f.>; 133, 277 <313 f. Rn. 88>; 152, 152 <168 Rn. 39>; 152, 216 <233 Rn. 42 f.>; 154, 152 <214 f. Rn. 84>; 155, 119 <165 Rn. 87>). 23

IV.

Die Jahresfrist zur Erhebung der Verfassungsbeschwerde aus § 93 Abs. 3 BVerfGG ist gewahrt. Dies galt, soweit die am 7. Dezember 2018 erhobene Verfassungsbeschwerde ursprünglich gegen den am 8. Dezember 2017 in Kraft getretenen § 23b Abs. 2 PolG BW a.F. gerichtet war. Die Beschwerdeführenden haben ihre Verfassungsbeschwerde am 10. März 2021 aber auch fristgemäß auf den am 17. Januar 2021 in Kraft getretenen § 54 Abs. 2 PolG BW n.F. umgestellt (vgl. dazu BVerfGE 155, 119 <158 Rn. 67>). 24

V.

Die Beschwerdeführenden haben jedoch nicht den Anforderungen der § 23 Abs. 1 Satz 2, § 92 BVerfGG entsprechend dargelegt, beschwerdebefugt zu sein. Die Zulässigkeit einer Verfassungsbeschwerde setzt gemäß Art. 93 Abs. 1 Nr. 4a GG, § 90 Abs. 1 BVerfGG voraus, dass die Beschwerdeführenden behaupten, durch die öffentliche Gewalt in einem ihrer Grundrechte oder grundrechtsgleichen Rechte verletzt zu sein, und dass dies zumindest möglich erscheint (vgl. BVerfGE 79, 1 <13 ff.>; 83, 216 <226>; 83, 341 <351 f.>; 129, 49 <67>). Dem genügt die Verfassungsbeschwerde nicht. Zwar besteht eine grundrechtliche Schutzpflicht (1) und die Beschwerdeführenden haben hinreichend begründet, dass sie selbst, gegenwärtig und unmittelbar in Grundrechten betroffen sind (2). Jedoch ergibt sich aus der Verfassungsbeschwerde nicht hinreichend, dass die Schutzpflicht verletzt sein könnte (3). 25

1. Der Staat trägt zum Schutz der Grundrechte eine Verantwortung für die Sicherheit informationstechnischer Systeme. In der hier zu beurteilenden Konstellation, in der die Behörden von einer Sicherheitslücke wissen, die der Hersteller nicht kennt, trifft den Staat eine konkrete grundrechtliche Schutzpflicht. Er ist verpflichtet, die Nutzerinnen und Nutzer informationstechnischer Systeme vor Angriffen Dritter auf diese Systeme zu schützen. 26

a) Betroffen sind hier das Fernmeldegeheimnis und die grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. 27

Sofern Zugriffe Dritter Inhalte und Umstände der laufenden Telekommunikation erfassen, ist das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis betroffen (vgl. BVerfGE 120, 274 <307>; 141, 220 <309 Rn. 228>). 28

Im Übrigen betrifft die Infiltration eines informationstechnischen Systems die aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG hergeleitete grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (vgl. BVerfGE 120, 274 <307 ff.>). Zwar ermächtigt die angegriffene Regelung die zuständigen Behörden nur bezüglich laufender Telekommunikationsvorgänge zur Quellen-Telekommunikationsüberwachung (vgl. § 54 Abs. 2 Nr. 1 PolG BW), so dass ein auf § 54 Abs. 2 PolG BW gestützter staatlicher Eingriff insoweit an Art. 10 Abs. 1 GG zu messen wäre. Dringen aber Dritte über eine unbekannte Schutzlücke in das System ein, könnten sie nicht nur auf laufende Kommunikation, sondern auf das gesamte informationstechnische System und seinen Datenbestand zugreifen. Sie können dieses ausspähen, manipulieren und erpresserisch mit der Manipulation, insbesondere der Vernichtung von Daten, drohen. 29

b) Die Grundrechte sind in ihrer Schutzdimension betroffen, aus der sich hier eine konkrete grundrechtliche Schutzpflicht des Staates ergibt. 30

aa) Nach ständiger Rechtsprechung des Bundesverfassungsgerichts erschöpft sich der Gewährleistungsgehalt von Grundrechten nicht in ihrer Abwehrfunktion, sondern sie enthalten zugleich eine objektive Wertentscheidung der Verfassung, die staatliche Schutzpflichten begründen kann (vgl. BVerfGE 39, 1 <42>; stRspr). 31

Art. 10 Abs. 1 GG begründet neben einem Abwehrrecht einen Auftrag an den Staat, vor dem Zugriff privater Dritter auf die dem Fernmeldegeheimnis unterfallende Kommunikation zu schützen (vgl. BVerfGE 106, 28 <37>; zur Schutzdimension des Grundrechts auf informationelle Selbstbestimmung BVerfG, Beschluss der 3. Kammer des Ersten Senats vom 17. Juli 2013 - 1 BvR 3167/08 -, Rn. 19 f.; zur Ausstrahlungswirkung in das Privatrecht BVerfGE 152, 152 <189 ff. Rn. 85 ff.> – Recht auf Vergessen I). 32

Auch die grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hat eine Schutzdimension. Das besondere, grundrechtlich erhebliche Schutzbedürfnis folgt aus der Angewiesenheit auf die Nutzung informationstechnischer Systeme für die Freiheitsverwirklichung und die allgemeine Entfaltung der Persönlichkeit sowie aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind (vgl. bereits BVerfGE 120, 274 <306>). Wie sehr die grundrechtlich geschützte Entfaltungsfreiheit inzwischen die Nutzung der Informationstechnik voraussetzt, hat der Senat bereits im Jahr 2008 näher ausge- 33

führt (a.a.O., S. 303 ff.). Der Zusammenhang von Entfaltungsfreiheit und Informationstechnik hat sich seitdem noch verstärkt. Die Umstellung ehemals analoger Vorgänge auf digitale Prozesse und nicht zuletzt die immer breitere mobile Nutzung informationstechnischer Systeme erhöhen die Abhängigkeit von Informationstechnologie ständig weiter. Die Einzelnen können von ihren grundrechtlichen Freiheiten ohne die Nutzung informationstechnischer Systeme immer weniger Gebrauch machen und können sich auch den Gefahren der Nutzung informationstechnischer Systeme immer weniger dadurch entziehen, dass sie auf diese Nutzung verzichten. Vor diesem Hintergrund gebieten die Grundrechte nicht nur, dass der Staat selbst die berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet (vgl. BVerfGE 120, 274 <306>). Vielmehr trifft den Staat auch eine Pflicht, dazu beizutragen, dass die Integrität und Vertraulichkeit informationstechnischer Systeme gegen Angriffe durch Dritte geschützt werden (siehe auch Petri, DuD 2008, S. 443 <446 f.>; Roßnagel/Schnabel, NJW 2008, S. 3534 <3535>; Hoffmann-Riem, AöR 134 <2009>, S. 513 <533 ff.>; Gudermann, Online-Durchsuchung im Lichte des Verfassungsrechts, 2010, S. 228 f.; Kutscha, DuD 2012, S. 391 <393 f.>; Schulz, DuD 2012, S. 395 <396>; Kutscha/Thomé, Grundrechtsschutz im Internet, 2013, S. 60 f.; Schliesky/Hoffmann/Luch/Schulz/Borchers, Schutzpflichten und Drittwirkung im Internet, 2014, S. 107 ff., S. 115 f.; Heinemann, Grundrechtlicher Schutz informationstechnischer Systeme, 2015, S. 209 ff.; Derin/Golla, NJW 2019, S. 1111 <1114 f.>; Poscher/Lasahn, in: Hornung/Schallbruch <Hrsg.>, IT-Sicherheitsrecht, 2021, § 7 Rn. 40 ff.).

bb) Weiß der Staat von Sicherheitslücken, die den Herstellern und Nutzern unbekannt sind, verdichtet sich der allgemeine Schutzauftrag zu einer konkreten grundrechtlichen Verpflichtung, die Nutzerinnen und Nutzer informationstechnischer Systeme davor zu schützen, dass Dritte über unbekannte Sicherheitslücken die genutzten Systeme infiltrieren (1). Diese konkrete grundrechtliche Schutzpflicht des Staates schließt nicht aus, eine Quellen-Telekommunikationsüberwachung mittels einer unbekannten Schutzlücke durchzuführen. Sie verlangt aber eine Regelung zur Auflösung des im vorliegenden Verfahren in Rede stehenden Zielkonflikts zwischen dem Schutz vor Infiltration durch Dritte einerseits und der Ermöglichung einer Quellen-Telekommunikationsüberwachung mittels unbekannter Sicherheitslücken zum Zwecke der Gefahrenabwehr andererseits (2). 34

(1) Werden den staatlichen Behörden Sicherheitslücken bekannt, verdichtet sich der allgemeine Schutzauftrag des Staates zu einer konkreten grundrechtlichen Schutzpflicht (vgl. entsprechend zu Art. 2 Abs. 2 Satz 1 GG BVerfGE 142, 35

313 <338 Rn. 71>). Diese konkrete Schutzpflicht beruht auf dem hohen Gefährdungs- und Schädigungspotenzial von Sicherheitslücken (a), auf der fehlenden Möglichkeit der Betroffenen, sich selbst zu schützen (b), und darauf, dass die Behörde hier Kenntnis von der Sicherheitslücke hat (c).

(a) Wenn Sicherheitslücken offenbleiben, sind damit besondere Gefahren für die informationelle Selbstbestimmung verbunden. Informationstechnische Systeme eröffnen ein breites Spektrum von Nutzungsmöglichkeiten, die sämtlich mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden sind. Wer Zugang zu diesen Daten erlangt, kann weitgehende Kenntnisse über die Persönlichkeit der Nutzerin oder des Nutzers gewinnen (näher bereits BVerfGE 120, 274 <305 f.>). Wird ein komplexes informationstechnisches System technisch infiltriert, ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen und solche weitreichenden Informationen zu erlangen (vgl. BVerfGE 120, 274 <308 f.>). 36

Wegen der Breite der Nutzungen informationstechnischer Systeme und der allgemeinen Angewiesenheit auf diese Nutzung haben Sicherheitslücken zudem ein über die Offenbarung persönlichkeitsrelevanter Informationen weit hinaus gehendes Schädigungspotenzial – etwa im betrieblichen Bereich und im Handel. Dringen Dritte über Sicherheitslücken in das informationstechnische System ein und manipulieren sie es, können Abläufe unterschiedlichster Art zum Schaden der Betroffenen gestört werden. Mit dem Risiko der Infiltration durch Dritte ist so auch eine besondere Erpressungsgefahr verbunden. 37

Diese Gefahren sind groß, weil viele unerkannte Schwachstellen existieren dürften. So empfiehlt das Bundesamt für Sicherheit in der Informationstechnik, immer davon auszugehen, dass die eingesetzte Software Schwachstellen enthält („Assume-Breach-Paradigma“, vgl. Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2017, S. 18; Die Lage der IT-Sicherheit in Deutschland 2019, S. 8; Die Lage der IT-Sicherheit in Deutschland, 2020, S. 22 ff., 34, 44 f., 79, 81). 38

(b) Vor der Gefahr einer Ausnutzung von Zero-Day-Schwachstellen, die dem Hersteller nicht bekannt sind und die deshalb noch nicht durch eine Aktualisierung des Systems geschlossen werden können, können sich die Einzelnen in der Regel 39

nicht selbst wirksam schützen. Sie können solche Zugriffe zum Teil gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren (vgl. BVerfGE 120, 274 <305 f.>).

(c) Zugleich sind es gerade die zuständigen Behörden, die in der hier zu beurteilenden Konstellation Kenntnis von der Sicherheitslücke haben und damit Abhilfe schaffen können. Die Beschwerdeführenden machen nicht etwa geltend, dass die Behörden aktiv nach Sicherheitslücken suchen müssten. Vielmehr mahnen sie einen grundrechtsschützenden Umgang mit Lücken an, die den Behörden, nicht aber dem Hersteller bekannt geworden sind. In Rede stehen mithin nur solche Konstellationen, in denen die Behörde bereits von einer Sicherheitslücke weiß; sei es, dass sie diese selbst entdeckt oder von Dritten beschafft hat. Gerade aus dieser Kenntnis und der gleichzeitigen Unkenntnis des Herstellers und der fehlenden Selbstschutzmöglichkeit der Betroffenen erwächst die besondere Schutzverpflichtung des Staates (vgl. auch BVerfGE 142, 313 <338 f. Rn. 73> zu Art. 2 Abs. 2 Satz 1 GG). 40

(2) Die Schutzpflicht schließt hier eine Verpflichtung des Gesetzgebers ein, den Umgang der Polizeibehörden mit Sicherheitslücken, die den Herstellern nicht bekannt sind, zu regeln. 41

Bestünde keine Ermächtigung zur Quellen-Telekommunikationsüberwachung und hätten die Behörden daher kein eigenes Interesse, Sicherheitslücken zu nutzen, um darüber informationstechnische Systeme infiltrieren zu können, würden sie die ihnen bekannt werdenden Lücken zur Erfüllung ihrer grundrechtlichen Schutzpflicht dem Hersteller regelmäßig melden, damit dieser die Lücke schließen kann. Ist eine Behörde aber ermächtigt, zum Zweck der Gefahrenabwehr eine Quellen-Telekommunikationsüberwachung durchzuführen, löst dies für sie einen Zielkonflikt zwischen den öffentlichen Interessen an einer möglichst großen Sicherheit informationstechnischer Systeme einerseits und der Ermöglichung einer dem Schutz von anderen hochrangigen Rechtsgütern dienenden Quellen-Telekommunikationsüberwachung andererseits aus. In der Folge besteht die Gefahr, dass die Behörde es unterlässt, die Schließung der Lücke anzuregen oder sogar aktiv darauf hinwirkt, dass die Lücke unerkannt bleibt (vgl. bereits BVerfGE 120, 274 <326> zur Online-Durchsuchung). Zugleich könnte allein die Existenz der staatlichen Überwachungsbefugnis einen Anreiz für Dritte schaffen, ihnen bekannte Sicherheitslücken nicht den Herstellern zu melden, um ihre Kenntnis vielmehr 42

staatlichen Behörden gegen eine Bezahlung anbieten zu können. Dies verstärkt die Gefahr, dass Sicherheitslücken dem Hersteller nicht gemeldet werden.

Wegen dieser Gefahren für die Sicherheit informationstechnischer Systeme unterliegt die Quellen-Telekommunikationsüberwachung durch Nutzung unerkannter Sicherheitslücken zwar erhöhten Rechtfertigungsanforderungen, ist aber verfassungsrechtlich nicht von vornherein unzulässig (vgl. bereits zur Online-Durchsuchung BVerfGE 120, 274 <325 f., 328>; 141, 220 <304 f. Rn. 211 f.>). Die grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verleiht daher keinen Anspruch darauf, die Quellen-Telekommunikationsüberwachung durch Nutzung unerkannter Sicherheitslücken vollständig zu untersagen. Sie begründet auch keinen Anspruch auf Verpflichtung der Behörde, jede unerkannte Sicherheitslücke sofort und unbedingt dem Hersteller zu melden. 43

Indessen verlangt die grundrechtliche Schutzpflicht eine Regelung darüber, wie die Behörde bei der Entscheidung über ein Offenhalten unerkannter Sicherheitslücken den Zielkonflikt zwischen dem notwendigen Schutz vor Infiltration durch Dritte einerseits und der Ermöglichung von Quellen-Telekommunikationsüberwachungen andererseits aufzulösen hat. Der Behörde muss eine Abwägung der gegenläufigen Belange für den Fall aufgegeben werden, dass ihr eine Zero-Day-Schutzlücke bekannt wird. Es ist sicherzustellen, dass die Behörde bei jeder Entscheidung über ein Offenhalten einer unerkannten Sicherheitslücke einerseits die Gefahr einer weiteren Verbreitung der Kenntnis von dieser Sicherheitslücke ermittelt und andererseits den Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücke quantitativ und qualitativ bestimmt, beides zueinander ins Verhältnis setzt und die Sicherheitslücke an den Hersteller meldet, wenn nicht das Interesse an der Offenhaltung der Lücke überwiegt. 44

2. Die Beschwerdeführenden haben aufgezeigt, dass sie durch eine Verletzung dieser Schutzpflicht selbst, unmittelbar und gegenwärtig betroffen wären. 45

Sie haben dargelegt, dass sie selbst betroffen sind, da sie informationstechnische Systeme nutzen, die potentiell unbekannte Schwachstellen aufweisen und damit durch Dritte auf diesem Weg infiltriert werden könnten. Zwar dürften dieser Gefahr viele Bürgerinnen und Bürger ausgesetzt sein. Einer weiteren Individualisierung bedarf es gleichwohl nicht. Im Verfassungsbeschwerdeverfahren wird eine über die eigene Betroffenheit hinausgehende besondere Betroffenheit, die die Be- 46

schwerdeführenden von der Allgemeinheit abheben würde, regelmäßig nicht verlangt (vgl. BVerfG, Beschluss des Ersten Senats vom 24. März 2021 - 1 BvR 2656/18 u.a. -, Rn. 110 – Klimaschutz).

Die Beschwerdeführenden sind auch unmittelbar und gegenwärtig betroffen. Die angegriffene Vorschrift entfaltet unmittelbar das Risiko einer (kriminellen) Ausnutzung nicht gemeldeter Sicherheitslücken, ohne dass dafür von der Ermächtigung zur Quellen-Telekommunikationsüberwachung Gebrauch gemacht werden müsste. Die Beschwerdeführenden wenden sich dagegen, dass § 54 Abs. 2 PolG BW unmittelbar die Gefahr erhöhe, dass Schwachstellen, die ohne das Bestehen dieser Überwachungsbefugnis von Behörden an Hersteller gemeldet und durch diese geschlossen würden, nun nicht gemeldet werden und deswegen weiterhin auch von Dritten ausgenutzt werden können. Dem steht nicht entgegen, dass die Landesregierung geltend macht, derzeit würden Schwachstellen im Zusammenhang mit der präventiv-polizeilichen Quellen-Telekommunikationsüberwachung nicht beschafft oder gesammelt. Denn daraus ergibt sich nicht, dass nicht jetzt schon etwa zufällig oder über andere (öffentliche) Stellen erworbene Kenntnisse über Schwachstellen vorhanden sind, die dem Hersteller aber mit Blick auf § 54 Abs. 2 PolG BW nicht gemeldet werden. 47

3. Die Beschwerdeführenden haben jedoch nicht hinreichend dargelegt, dass die grundrechtliche Schutzpflicht verletzt sein könnte. 48

a) Die aus den Grundrechten folgenden subjektiven Abwehrrechte gegen staatliche Eingriffe einerseits und die sich aus der objektiven Bedeutung der Grundrechte ergebenden Schutzpflichten andererseits unterscheiden sich insofern grundlegend voneinander, als das Abwehrrecht in Zielsetzung und Inhalt ein bestimmtes staatliches Verhalten verbietet, während die Schutzpflicht grundsätzlich unbestimmt ist. Die Aufstellung und normative Umsetzung eines Schutzkonzepts ist Sache des Gesetzgebers, dem grundsätzlich auch dann ein Einschätzungs-, Wertungs- und Gestaltungsspielraum zukommt, wenn er dem Grunde nach verpflichtet ist, Maßnahmen zum Schutz eines Rechtsguts zu ergreifen. Dieser lässt auch Raum, etwa konkurrierende öffentliche und private Interessen zu berücksichtigen (vgl. BVerfGE 96, 56 <64>; 121, 317 <356, 360>; 133, 59 <76 Rn. 45>; 142, 313 <337 Rn. 70>; stRspr). 49

Das Bundesverfassungsgericht kann die Verletzung einer solchen Schutzpflicht nur feststellen, wenn Schutzvorkehrungen entweder überhaupt nicht getrof- 50

fen sind, wenn die getroffenen Regelungen und Maßnahmen offensichtlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder wenn sie erheblich hinter dem Schutzziel zurückbleiben (so zu Art. 2 Abs. 2 Satz 1 GG zuletzt BVerfG, Beschluss des Ersten Senats vom 24. März 2021 - 1 BvR 2656/18 u.a. -, Rn. 152 m.w.N. – Klimaschutz; stRspr). Die Entscheidung, welche Maßnahmen geboten sind, um den Schutz zu gewähren, ist damit verfassungsgerichtlich nur begrenzt überprüfbar. Nur unter besonderen Umständen kann sich die Gestaltungsfreiheit des Gesetzgebers in der Weise verengen, dass allein durch eine bestimmte Maßnahme der Schutzpflicht Genüge getan werden kann (vgl. BVerfGE 56, 54 <73 ff.>; 77, 170 <214 f.>; 79, 174 <202>; 142, 313 <337 f. Rn. 70 f.>).

Mit den Anforderungen an die Feststellung einer gesetzgeberischen Schutzpflichtverletzung sind spezifische Darlegungslasten der Beschwerdeführenden verbunden. Eine mögliche Grundrechtsverletzung der Beschwerdeführenden geht aus dem Vortrag regelmäßig nur dann hervor, wenn sich dieser nicht in pauschalen Behauptungen und punktuell herausgegriffenen, angeblichen Unzulänglichkeiten der Rechtslage erschöpft. Erforderlich ist vielmehr, den gesetzlichen Regelungszusammenhang insgesamt zu erfassen, 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 auszugehen ist. 51

Aus der Entscheidung des Senats zum Klimaschutzgesetz folgt nichts Anderes. Dort ist zwar festgestellt, dass die Beschwerdeführenden zur Begründung der Beschwerdebefugnis nicht alle relevanten Maßnahmen ermitteln müssen. Dies war aber deshalb verzichtbar, weil der Gesetzgeber selbst eine zusammenfassende Regelung getroffen hatte, auf die sich der Angriff der Beschwerdeführenden beschränken konnte (vgl. BVerfG, Beschluss des Ersten Senats vom 24. März 2021 - 1 BvR 2656/18 u.a. -, Rn. 134). Das ist hier nicht der Fall. 52

b) Den genannten Darlegungsanforderungen genügt die Verfassungsbeschwerde nicht. Es bestehen unterschiedliche gesetzliche Regelungen zum Schutz informationstechnischer Systeme, denen – ohne dass dies hier abschließend verfassungsrechtlich bewertet werden kann – auch im vorliegenden Kontext Bedeutung zukommen könnte. In ihrer Verfassungsbeschwerde haben die Beschwerdeführenden die bestehenden Regelungen weder in ihren Grundzügen 53

dargestellt, noch haben sie ausgeführt, aus welchen konkreten Gründen vom Versagen der Regelungen auszugehen ist. Soweit sie hierzu in ihrer Stellungnahme vom 10. März 2021 ergänzend vorgetragen haben, führt auch dies im Ergebnis nicht dazu, dass die Möglichkeit der Schutzpflichtverletzung hinreichend dargelegt wäre.

aa) Zunächst enthält die Ermächtigungsgrundlage selbst diverse Schutzvorkehrungen, die der Gesetzgeber gerade mit dem Ziel geregelt hat, „die Datensicherheit auch mit Rücksicht auf Eingriffe von dritter Seite zu schützen“ (LTDrucks 16/2741, S. 31). Die Beschwerdeführenden hätten jedenfalls auf § 54 Abs. 3 Satz 2 PolG BW eingehen müssen, wonach das eingesetzte Mittel gegen unbefugte Nutzung zu schützen ist. Es ist nicht offensichtlich ausgeschlossen, dass diese Vorschrift Auslegungsspielräume eröffnet, um auf der Ebene der Normanwendung dem Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme angemessen begegnen zu können. 54

Zwar ist denkbar, dass das in § 54 Abs. 3 Satz 2 PolG BW genannte „Mittel“ die Infiltrationssoftware, nicht aber die zu ihrer Einbringung genutzte Sicherheitslücke bezeichnet, weil diese Lücke im Zielsystem unabhängig vom Handeln der Polizei besteht. Jedoch könnte § 54 Abs. 3 Satz 2 PolG BW fachrechtlich auch in einer Weise auszulegen sein, die unter das Tatbestandsmerkmal des „eingesetzten Mittels“ auch die ausgenutzte Schwachstelle fasst. Dies hätte zur Folge, dass diese – etwa durch eine Meldung an den Hersteller – gegen eine unbefugte Nutzung zu schützen wäre. Die Beschwerdeführenden sind hierauf zwar in ihrem ergänzenden Schriftsatz vom 10. März 2021 sehr knapp eingegangen. Zu diesem Zeitpunkt war die Verfassungsbeschwerdefrist jedoch abgelaufen, so dass dieser Vortrag die Beschwerde- und Begründungsfrist nicht wahrt (vgl. BVerfGE 145, 20 <52 Rn. 79>). Es handelt sich auch nicht um eine bloße Ergänzung einer bereits zuvor hinreichend begründeten und damit zulässigen Verfassungsbeschwerde (vgl. dazu BVerfGE 127, 87 <110>). 55

bb) Der Zielkonflikt zwischen den öffentlichen Interessen an einem behördlichen Zugriff auf Telekommunikation einerseits und an einer möglichst großen Sicherheit informationstechnischer Systeme andererseits könnte auch im Rahmen der Datenschutz-Folgenabschätzung zu adressieren sein. Diese ist in § 80 PolG BW geregelt, der mit dem Änderungsgesetz vom 6. Oktober 2020 zur Umsetzung von Art. 27 JI-RL eingefügt wurde. § 80 PolG BW hat folgenden Wortlaut: 56

§ 80 PolG BW

Datenschutz-Folgenabschätzung

(1) Hat eine bestimmte Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechtsgüter betroffener Personen zur Folge, so hat die Polizei vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durchzuführen.

(2) Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohem Gefahrenpotenzial kann eine gemeinsame Folgenabschätzung vorgenommen werden.

(3) Die Folgenabschätzung hat den Rechten und den berechtigten Interessen der von der Verarbeitung betroffenen Personen Rechnung zu tragen und zumindest Folgendes zu enthalten:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,

2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zwecke,

3. eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen und

4. die Maßnahmen, mit denen bestehenden Gefahren abgeholfen werden soll, einschließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden soll.

Hierauf gehen die Beschwerdeführenden nicht ein. Dies war hier nicht etwa deswegen entbehrlich, weil die Regelung zur Datenschutz-Folgenabschätzung in § 80 PolG BW erst nach Erhebung der Verfassungsbeschwerde und nach Ablauf der Beschwerdefrist ergangen ist. Die Beschwerdeführenden müssen ihren Vortrag ergänzen, wenn sich die Sach- und Rechtslage nach Ablauf der Beschwerdefrist ändert (vgl. BVerfGE 106, 210 <214 f.>). Dies gilt insbesondere, wenn sie eine Schutzpflichtverletzung geltend machen und nach Ablauf der Beschwerdefrist ein Gesetz in Kraft tritt, das diese Schutzpflicht möglicherweise erfüllen könnte. Im Übrigen war der Gesetzgeber schon im Zeitpunkt der Verfassungsbeschwerde nach Art. 27 JI-RL verpflichtet, eine Datenschutzfolgenabschätzung zu regeln, so 57

dass sich die Beschwerdeführenden vor der Umsetzung in das Landesrecht jedenfalls mit dieser unionsrechtlichen Regelung hätten befassen müssen.

Ob beim Offenhalten einer Zero-Day-Sicherheitslücke eine solche Folgenabschätzung vorzunehmen ist, erscheint fraglich. Zweifellos ist eine Datenschutz-Folgenabschätzung vor dem Einsatz von Überwachungssoftware auf Grundlage des § 54 Abs. 2 PolG BW durchzuführen. Weniger eindeutig ist zwar, dass dies auch schon für die Entscheidung gilt, eine der Behörde bekannte Sicherheitslücke nicht dem Hersteller zu melden und so offen zu halten. Dafür könnte aber Art. 27 JI-RL sprechen, dessen Umsetzung § 80 PolG BW dient und der folgenden Wortlaut hat: 58

Art. 27 JI-RL

Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so sehen die Mitgliedstaaten vor, dass der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführt.

(2) Die Folgenabschätzung gemäß Absatz 1 trägt den Rechten und den berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener Rechnung und enthält zumindest eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken sowie der geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Richtlinie eingehalten wird.

Art. 27 JI-RL könnte eine Auslegung des § 80 PolG BW dahingehend gebieten, dass nicht nur die Risiken für Rechtsgüter von Personen erfasst sind, die unmittelbar oder mittelbar vom konkreten Verarbeitungsvorgang (hier also der Maßnahme der Quellen-Telekommunikationsüberwachung) betroffen sind, sondern grundsätzlich auch Risiken für (unbeteiligte) Personen. Dafür spricht, dass Art. 27 Abs. 1 JI-RL allgemein die Risiken für die Rechte und Freiheiten natürlicher Personen nennt und dass Art. 27 Abs. 2 JI-RL zwar zwischen den von der Datenver- 59

arbeitung betroffenen Personen und sonstigen Betroffenen unterscheidet, jedoch die Rechte und berechtigten Interessen beider in die Folgenabschätzung einzustellen sind.

Fraglich ist aber auch, ob das Offenhalten einer Sicherheitslücke ein „Verarbeitungsvorgang“ im Sinne von § 80 Abs. 1 PolG BW ist (zum Tatbestandsmerkmal der „Verarbeitung“ § 12 Nr. 2 PolG BW). Es erscheint zumindest nicht ausgeschlossen, den Verarbeitungsvorgang als einheitlichen Lebenssachverhalt zu begreifen, der nicht erst mit dem Ausleiten von Daten bei der eigentlichen Telekommunikationsüberwachung beginnt, sondern bereits davor liegende, vorbereitende Schritte erfasst. Das Offenhalten einer der Behörde bekannten Sicherheitslücke könnte so als vorbereitender Schritt einer Quellen-Telekommunikationsüberwachung angesehen werden und wäre damit von § 80 PolG BW erfasst. Ob darüber hinaus die hier maßgebliche Gefahr, dass Dritte die Sicherheitslücke zur Infiltration des informationstechnischen Systems nutzen, auch im Sinne von § 80 Abs. 1 PolG BW als „Folge“ dieses Verarbeitungsvorgangs (nämlich der Offenhaltung der Sicherheitslücke) gilt, bedürfte weiterer Klärung. 60

Auf diese Fragen sind die Beschwerdeführenden nicht eingegangen. Es ist nicht Aufgabe des Bundesverfassungsgerichts, das Fachrecht eigenständig daraufhin auszuleuchten, inwiefern als Schutznormen in Betracht kommende Regelungen in einer Weise auszulegen sind, dass sie dem grundrechtlichen Schutzauftrag gerecht werden oder diesen aber verfehlen. 61

Auch eine Vorlage des Bundesverfassungsgerichts nach Art. 267 AEUV, die Fragen der Auslegung der unionsrechtlichen Regelung zur Folgenabschätzung (Art. 27 JI-RL) klären könnte, kommt im Rahmen dieses Verfassungsbeschwerdeverfahrens nicht in Betracht. Das gilt schon deshalb, weil die Verfassungsbeschwerde unzulässig und diese Frage daher nicht entscheidungserheblich ist. Im Übrigen dürfte Art. 27 JI-RL, auch wenn er eine Folgenabschätzung im Fall der Zero-Day-Sicherheitslücke nicht erforderte, einer weitergehenden Auslegung von § 80 PolG BW kaum entgegenstehen (vgl. Art. 1 Abs. 3 JI-RL). Selbst wenn die Verfassungsbeschwerde zulässig wäre, wäre die Auslegung von Art. 27 JI-RL für die Entscheidung des Bundesverfassungsgerichts daher nicht entscheidungserheblich. 62

cc) Die Beschwerdeführenden tragen auch nicht ausreichend dazu vor, inwiefern das Cybersicherheitsrecht Baden-Württembergs Schutzvorschriften enthält. 63

Am 17. Februar 2021 ist das Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften (GBl 2021, S. 182, im Folgenden: Cybersicherheitsgesetz <CSG>) in Kraft getreten. Das Gesetz sieht die Cybersicherheitsagentur Baden-Württemberg vor (vgl. § 1 Abs. 1, § 3 CSG). Diese soll als zentrale Koordinierungs- und Meldestelle für die Zusammenarbeit der öffentlichen Stellen in Angelegenheiten der Cybersicherheit in Baden-Württemberg fungieren (vgl. § 4 Abs. 1 CSG) und dabei insbesondere alle für die Abwehr von Gefahren für die Cybersicherheit erforderlichen Informationen, unter anderem zu Sicherheitslücken, sammeln und auswerten (vgl. § 4 Abs. 2 Nr. 1 CSG). Durch das Cybersicherheitsgesetz sollen ab Januar 2022 auch Pflichten der Landesbehörden zur Meldung von Sicherheitslücken an die Cybersicherheitsagentur begründet werden (vgl. § 4 Abs. 3 CSG) und der Cybersicherheitsagentur Befugnisse zur Abwehr von Gefahren für die Cybersicherheit eingeräumt werden (vgl. § 5 CSG). Die Cybersicherheitsagentur soll auch Warnungen, Empfehlungen und Hinweise zu Sicherheitslücken an die Öffentlichkeit oder die betroffenen Kreise – in der Regel nach vorheriger Anhörung des Herstellers – aussprechen dürfen (vgl. § 8 Abs. 1 CSG).

Auch insoweit waren Ausführungen in der Verfassungsbeschwerde nicht deswegen entbehrlich, weil das Cybersicherheitsgesetz erst nach Einlegung der Verfassungsbeschwerde und nach Ablauf der Beschwerdefrist in Kraft getreten ist (oben Rn. 57). Der im ergänzenden Schriftsatz vom 10. März 2021 enthaltene Vortrag der Beschwerdeführenden zum Cybersicherheitsgesetz ist zwar zu berücksichtigen, weil die Regelungen erst am 17. Februar 2021 in Kraft getreten sind, sodass die Beschwerdeführenden hierzu nicht innerhalb der Beschwerdefrist hätten vortragen können. Auch insoweit genügen die Ausführungen den Begründungsanforderungen jedoch nicht. Um die Möglichkeit einer Schutzpflichtverletzung zu begründen, ist eine Auseinandersetzung mit den Schutzvorkehrungen im Ganzen erforderlich; ein punktuelles Herausgreifen einer einzelnen, möglicherweise unzulänglichen Regelung reicht dafür nicht aus. Vor allem aber haben sich die Beschwerdeführenden nicht mit der Frage auseinandergesetzt, ob die relevanten Vorschriften so ausgelegt werden können, dass verfassungsrechtlich ausreichender Grundrechtsschutz gegen Angriffe Dritter auf informationstechnische Systeme besteht. 64

dd) Schließlich gehen die Beschwerdeführenden nicht auf den untergesetzlich geregelten Meldestandard ein. Unter Geltung des Vertrags über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur 65

Ausführung von Artikel 91c GG (IT-Staatsvertrag in der Fassung der Bekanntmachung vom 13. Dezember 2019, BGBl I S. 2852) hat der IT-Planungsrat am 5. Oktober 2017 ein „Verbindliches Meldeverfahren zum Informationsaustausch über IT-Sicherheitsvorfälle im VerwaltungsCERT-Verbund (VCV) – (Meldestandard)“ beschlossen (Nr. 2017/35). Damit wurde für den Informationsaustausch für Bund und Länder als IT-Sicherheitsstandard im Sinne von § 3 Abs. 1 (jetzt § 2 Abs. 1) des IT-Staatsvertrags verbindlich (vgl. § 2 Abs. 2 Satz 2 IT-Staatsvertrag) vereinbart, dass IT-Sicherheitsvorfälle, bei denen Auswirkungen auf die Länder oder den Bund nicht ausgeschlossen werden können oder die auch für andere als relevant eingeschätzt werden, zu melden sind (§ 2 Abs. 1 des Beschlusses). Die Meldung erfolgt unter anderem an das Bundesamt für Sicherheit in der Informationstechnik. Unter die Meldepflicht fallen auch neuartige Sicherheitslücken in IT-Produkten (vgl. § 2 Abs. 2 in Verbindung mit Anlage 1 des Beschlusses). Meldepflichtig sind nach § 3 des Beschlusses Bund und Länder. Insofern erscheint jedenfalls denkbar, dass das Bundesamt für Sicherheit in der Informationstechnik seine Ermessensspielräume bei der Entscheidung über den weiteren Umgang mit derartigen Kenntnissen – insbesondere bei der Erteilung von Warnungen vor Sicherheitslücken in informationstechnischen Systemen an die Öffentlichkeit oder die betroffenen Kreise nach § 7 Abs. 1 Satz 1 Nr. 1 lit. a BSIG und der Information der Hersteller – unter Berücksichtigung der grundrechtlichen Schutzpflichten ausfüllen könnte und müsste.

Inwieweit der grundrechtlichen Schutzpflicht durch untergesetzlich normierte Mitteilungspflichten genügt werden kann und ob die gesetzliche Verankerung dieser Normierung hier ausreicht, bedürfte näherer Prüfung. Weil der beschlossene Meldestandard ein Element einer Gesamtregelung des Schutzes vor der unzulässigen Nutzung von Schwachstellen durch Dritte sein könnte, hätte es auch insoweit der Darlegung durch die Beschwerdeführenden bedurft. 66

VI.

Die Verfassungsbeschwerde ist zudem unzulässig, weil sie nicht den Anforderungen der Subsidiarität im weiteren Sinne genügt. 67

1. a) Die Anforderungen der Subsidiarität beschränken sich nicht darauf, nur die zur Erreichung des unmittelbaren Prozessziels förmlich eröffneten Rechtsmittel zu ergreifen, sondern verlangen, alle Mittel zu nutzen, die der geltend gemachten Grundrechtsverletzung abhelfen können. Damit soll erreicht werden, dass das 68

Bundesverfassungsgericht nicht auf ungesicherter Tatsachen- und Rechtsgrundlage weitreichende Entscheidungen treffen muss, sondern zunächst die für die Auslegung und Anwendung des einfachen Rechts primär zuständigen Fachgerichte die Sach- und Rechtslage aufgearbeitet haben.

Der Grundsatz der Subsidiarität erfordert deshalb grundsätzlich, vor Einlegung einer Verfassungsbeschwerde alle zur Verfügung stehenden prozessualen Möglichkeiten zu ergreifen, um eine Korrektur der geltend gemachten Verfassungsverletzung zu erwirken oder eine Grundrechtsverletzung zu verhindern. Das gilt auch, wenn zweifelhaft ist, ob ein entsprechender Rechtsbehelf statthaft ist und im konkreten Fall in zulässiger Weise eingelegt werden kann. 69

Wenn sich eine Verfassungsbeschwerde unmittelbar gegen ein Gesetz wendet, kann daher auch die Erhebung einer Feststellungs- oder Unterlassungsklage zu den zuvor zu ergreifenden Rechtsbehelfen gehören. Das ist selbst dann nicht ausgeschlossen, wenn die Vorschriften abschließend gefasst sind und die fachgerichtliche Prüfung günstigstenfalls dazu führen kann, dass das angegriffene Gesetz gemäß Art. 100 Abs. 1 GG dem Bundesverfassungsgericht vorgelegt wird. Ausschlaggebend ist auch dann, ob die fachgerichtliche Klärung erforderlich ist, um zu vermeiden, dass das Bundesverfassungsgericht seine Entscheidungen auf ungesicherter Tatsachen- und Rechtsgrundlage trifft. Ein solcher Fall wird in der Regel dann gegeben sein, wenn die angegriffenen Vorschriften auslegungsbedürftige und -fähige Rechtsbegriffe enthalten, von deren Auslegung und Anwendung es maßgeblich abhängt, inwieweit Beschwerdeführende durch die angegriffenen Vorschriften tatsächlich und rechtlich beschwert sind (vgl. BVerfGE 143, 246 <321 f. Rn. 210>; 145, 20 <54 f. Rn. 85 f.>; 150, 309 <326 f. Rn. 42 ff.>). 70

Soweit die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären, bedarf es einer vorangehenden fachgerichtlichen Entscheidung hingegen nicht (vgl. BVerfGE 150, 309 <326 f. Rn. 44> m.w.N.). Außerdem ist es zur Wahrung des Grundsatzes der Subsidiarität nicht erforderlich, vor Erhebung einer Verfassungsbeschwerde gegen eine straf- oder bußgeldbewehrte Rechtsnorm zu verstoßen und sich dem Risiko einer entsprechenden Ahndung auszusetzen, um dann im Straf- oder Bußgeldverfahren die Verfassungswidrigkeit der Norm geltend machen zu können (vgl. BVerfGE 145, 20 <54 Rn. 85> m.w.N.). Darüber hinaus gelten Ausnahmen von der Pflicht zur vor- 71

herigen Anrufung der Fachgerichte, wenn die angegriffene Regelung die Beschwerdeführenden zu gewichtigen Dispositionen zwingt, die später nicht mehr korrigiert werden können, wenn die Anrufung der Fachgerichte offensichtlich sinn- und aussichtslos wäre oder sie sonst nicht zumutbar ist (vgl. BVerfGE 150, 309 <327 f. Rn. 45> m.w.N.). Dabei ist allerdings die Anrufung der Fachgerichte nicht schon dann als von vornherein aussichtslos anzusehen, wenn Rechtsprechung zugunsten der Zulässigkeit des Rechtsbehelfs für die gegebene Fallgestaltung noch nicht vorliegt (vgl. BVerfGE 145, 20 <54 Rn. 85>).

b) Diese Grundsätze beanspruchen auch im Falle der Rüge einer gesetzgeberischen Schutzpflichtverletzung Geltung. Häufig wird sich eine Lücke in den gesetzlichen Regelungen zu einer bestimmten Problematik nur dann zuverlässig feststellen lassen, wenn zuvor die Fachgerichte den zugrunde liegenden Sachverhalt und die einfachrechtliche Rechtslage auch unter Berücksichtigung verfassungsrechtlicher Vorgaben umfassend aufgearbeitet haben. Auch in den Fällen gesetzgeberischen Unterlassens wird so vermieden, dass das Bundesverfassungsgericht auf tatsächlich und einfachrechtlich ungeklärter Basis entscheiden muss. 72

2. Dem genügt die Verfassungsbeschwerde nicht. Im hier zu entscheidenden Fall stellen sich umfangreiche Fragen zur Auslegung des einfachen Rechts. Ob die Behörden bereits nach bestehendem Recht eine der grundrechtlichen Schutzpflicht genügende Abwägung vornehmen müssen, bevor sie entscheiden, eine ihnen bekannt gewordene Zero-Day-Schwachstelle nicht dem Hersteller zu melden, hängt von der Auslegung verschiedener Bestimmungen des Polizei-, des Datenschutz-, des Cybersicherheits- und des IT-Sicherheitsrechts ab (oben Rn. 53 ff.). Es handelt sich bei diesen Vorschriften überwiegend um jüngeres Fachrecht, dessen Bedeutung bislang weder durch Gerichtsentscheidungen oder andere Rechtsanwendungsakte noch durch die Fachliteratur näher erschlossen ist. Damit das Bundesverfassungsgericht nicht auf ungesicherter Grundlage Entscheidungen treffen muss, müssen daher zunächst die für die Auslegung und Anwendung des einfachen Rechts primär zuständigen Fachgerichte die Möglichkeit erhalten, die Sach- und Rechtslage zu prüfen. Die Beschwerdeführenden hätten darum versuchen müssen, etwa durch Erhebung einer verwaltungsgerichtlichen Feststellungs- oder vorbeugenden Unterlassungsklage fachgerichtlichen Rechtsschutz zu erlangen. Nach der neueren verwaltungsgerichtlichen Rechtsprechung ist nicht auszuschließen, dass fachgerichtlicher Rechtsschutz auch hinsichtlich der Frage erreichbar wäre, ob die Grundrechte der Nutzer informationstechnischer 73

Systeme (weitere) Vorkehrungen zur hinreichenden Berücksichtigung des Schutzes solcher Systeme vor Infiltrationen durch Dritte bei Entscheidungen über die Offenhaltung unerkannter Sicherheitslücken für etwaige Quellen-Telekommunikationsüberwachungen gebieten (vgl. zur Zulässigkeit einer negativen Feststellungsklage BVerwGE 157, 8 <10 f. Rn. 13 >; 157, 126 <128 f. Rn. 15>; zur vorbeugenden Unterlassungsklage BVerwG, Urteil vom 22. Oktober 2014 - 6 C 7/13 -, Rn. 15 ff.; Urteil vom 13. Dezember 2017 - 6 A 6/16 -, Rn. 14; BVerwGE 161, 76 <77 f. Rn. 12 ff.>).

Gründe dafür, dass den Beschwerdeführenden die Beschreitung des fachgerichtlichen Rechtswegs nicht zugemutet werden könnte, sind nicht ersichtlich. Insbesondere war vor Erhebung der vorliegenden Verfassungsbeschwerde bereits mehrfach das Erfordernis einer verwaltungsgerichtlichen Feststellungsklage oder Unterlassungsklage angesprochen worden (vgl. BVerfGE 143, 246 <321 f. Rn. 210>; 145, 20 <54 f. Rn. 86>; nach Ablauf der ursprünglichen Beschwerdefrist, aber vor der Einführung von § 80 PolG BW und der Verabschiedung des Cybersicherheitsgesetzes Baden-Württembergs auch BVerfGE 150, 309 <326 f. Rn. 42 ff.> – KFZ-Kennzeichenkontrolle BW-HE). 74

Harbarth Paulus Baer

Britz Ott Christ

Radtke Härtel