Bundesverfassungsgericht

Erster Senat
- Geschäftsstelle -

Bundesverfassungsgericht ♦ Postfach 1771 ♦ 76006 Karlsruhe

Herrn Rechtsanwalt
Dr. Peter Spengler
Schleiermacherstraße 2
64283 Darmstadt

RA Dr. Spengler
Eing.: 23. Okt. 2020

→ Fr. Schyra-Hyat

Aktenzeichen
1 BvR 1552/19
(bei Antwort bitte angeben)

☎ (0721)
9101-403

Datum
14.10.2020

Verfassungsbeschwerde

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

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

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

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

Ihr Zeichen: 46/18 PS

1 Anlage

Sehr geehrter Herr Rechtsanwalt Dr. Spengler,

anliegend wird ein Abdruck des Schreibens des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz vom 8. Oktober 2020 zur Kenntnisnahme übersandt.

Mit freundlichen Grüßen
Auf Anordnung

(Wolf)
Tarifbeschäftigte

Hinweis: Personenbezogene Daten, die uns im Zusammenhang mit der Durchführung von gerichtlichen Verfahren bzw. der Bearbeitung von Justizverwaltungsangelegenheiten übermittelt werden, werden von uns ausschließlich zur Wahrnehmung unserer Aufgaben bzw. zur Erfüllung unserer rechtlichen Verpflichtungen verarbeitet. Rechtsgrundlagen sind Art. 6 Abs. 1 Satz 1 lit. e DSGVO i.V.m. § 3 BDSG, Art. 6 Abs. 1 Satz 1 lit. c DSGVO und die jeweils einschlägigen Verfahrensvorschriften des BVerfGG. Unsere ausführlichen Informationen zum Datenschutz in gerichtlichen Verfahren und Justizverwaltungsangelegenheiten finden Sie auf unserer Internetseite www.bundesverfassungsgericht.de unter dem Menüpunkt „Verfahren". Auf Wunsch senden wir Ihnen diese Informationen auch in Papierform zu.

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

RA Dr. Spengler
Eing.: 23. Okt. 2020

2. Vf. 21.10.20

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit RLP
Postfach 3040 | 55020 Mainz

An das
Bundesverfassungsgericht
Erster Senat
Postfach 1771
76006 Karlsruhe

Bundesverfassungsgericht
Eing. 12.10.20 10:11
Doppel Bd.
1 Anlage 19 Doppel

Hintere Bleiche 34 | 55116 Mainz
Postfach 3040 | 55020 Mainz

Telefon +49 (0) 6131 208-2449
Telefax +49 (0) 6131 208-2497

poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

Ihr Zeichen	Ihre Nachricht vom	Geschäftszeichen	Telefondurchwahl	Datum
1 BvR 1552/19		6.00.25	2449	08.10.2020

Stellungnahme zu der Verfassungsbeschwerde mit Az. 1 BvR 1552/19

Sehr geehrter Herr Vizepräsident Prof. Dr. Harbarth,

anbei sende ich Ihnen die Stellungnahme des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz als sachkundiger Dritter (§ 27a BVerfGG, § 22 Abs. 5 GOBVerfG) zu der o.g. Verfassungsbeschwerde.

Mit freundlichen Grüßen

Prof. Dr. Dieter Kugelmann

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Stellungnahme
des Landesbeauftragten für den Datenschutz und die Informationsfreiheit
Rheinland-Pfalz
zu den Verfassungsbeschwerden

mit Az. 1 BvR 1552/19 (§ 15b und § 15c des Hessischen Gesetzes über die Sicherheit und Ordnung (HSOG) in der Fassung des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen vom 25. Juni 2018 (GVBl. S. 302))
und
mit Az. 1 BvR 2771/18 (§ 23b Abs. 2 des Polizeigesetzes Baden-Württemberg (PolG BW) in der Fassung des Gesetzes zur Änderung des Polizeigesetzes vom 28. November 2017 (GBl. BW S. 624)

als sachkundiger Dritter (§ 27a BVerfGG, § 22 Abs. 5 GOBVerfG).

I. Vorbemerkungen

Die Stellungnahme befasst sich mit den Fragestellungen, ob eine verfassungsrechtliche Notwendigkeit staatlicher Maßnahmen zum Schutz informationstechnischer Systeme gegen Dritte besteht (II.), ob solche Schutzvorschriften bestehen (III.) und erörtert die Bedeutung der VO (EU) 2016/679 sowie der RL (EU) 2016/680 in diesem Zusammenhang (IV.).

Aufgrund der abstrakten Natur der Rechtsfragen, die beide der oben genannten Verfassungsbeschwerden betreffen, gibt der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI) eine einheitliche Stellungnahme in Bezug auf beide Verfassungsbeschwerden ab. Sofern dabei die Bezugnahme auf die streitgegenständlichen Vorschriften des Hessischen Gesetzes über die Sicherheit und Ordnung (HSOG) und des Polizeigesetzes Baden-Württemberg (PolG BW) erforderlich ist, ist dies durch Nennung der entsprechenden Vorschriften ersichtlich.

II. Verfassungsrechtliche Notwendigkeit staatlicher Maßnahmen zum Schutz informationstechnischer Systeme gegen Dritte

1. Beschwerdegegenstand

Die Verfassungsbeschwerde 1 BvR 1552/19 wendet sich gegen die Vorschriften der § 15b (Quellen-Telekommunikationsüberwachung) und § 15c (Online-Durchsuchung) des Hessischen Gesetzes über die Sicherheit und Ordnung (HSOG) und beantragt, die Nichtigkeit dieser Vorschriften festzustellen.

Die Verfassungsbeschwerde 1 BvR 2771/18 wird gegen die Vorschrift des § 23b Abs. 2 Polizeigesetz Baden-Württemberg (PolG BW) geführt und rügt die Verletzung von Art. 2

Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG) als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. In der Folge beantragen die Beschwerdeführer_innen zu entscheiden, dass § 23b Abs. 2 PolG BW in Verbindung mit § 23b Abs. 1PolG BW mit Art. 2 Abs.1 i.V.m. Art. 1 Abs. 1 GG unvereinbar ist, soweit er es erlaubt, zur Durchführung von Eingriffen in informationstechnische Systeme mit technischen Mitteln auch Schwachstellen dieser Systeme auszunutzen, die den jeweiligen Herstellern nicht bekannt sind (sog. 0-Day-Verfahren) (S. 69 der Beschwerdeschrift zu Az. 1 BvR 2771/18).

Die angeführten Defizite der angegriffenen Vorschriften betreffen in beiden Verfassungsbeschwerden das Fehlen von Regelungen, die ein sog. Schwachstellenmanagement in Bezug auf den Hersteller unbekannte Sicherheitslücken ermöglichen. Dem wird zugrunde gelegt, dass die Verwendung der betreffenden Software, mit der die Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung ermöglicht werden, indem das informationstechnische System infiltriert wird, durch die Nutzung von den Herstellern unbekannten Sicherheitslücken dieser informationstechnischen Systeme erfolgt (S. 21 der Verfassungsbeschwerde mit Az. 1552/19). Dies ohne Vorkehrungen zu treffen, dass die identifizierten Sicherheitslücken, die die informationstechnischen Systeme auch für Zugriffe unbefugter Dritter angreifbar machen, geschlossen werden bzw. die Hersteller über die betreffenden Lücken informiert werden.

In diesem Zusammenhang wird gefordert, dass Regelungen in Bezug auf Beschaffenheit, Funktionalität und Anwendungskontrolle getroffen werden (S. 45 der Beschwerdeschrift zu 1 BvR 1552/19) bzw. dass ein Verwaltungsverfahren vorgesehen wird, „mit dem eine hiermit zu betrauende Behörde ihr bekannt werdende Sicherheitslücken auf ihre Bedeutung hin untersuchen und einzustufen hat, um auf dieser Grundlage über den Umgang mit der Sicherheitslücke zu entscheiden“ (sog. Schwachstellenmanagement) (S. 65 der Beschwerdeschrift zu Az. 1 BvR 2771/18).

Für den verfassungsrechtlichen Maßstab bedeutet dies, dass nicht die Eingriffstatbestände der betreffenden Maßnahmen der Online-Durchsuchung und Quellen-Telekommunikationsüberwachung Gegenstand der Prüfung sind, sondern die Vorkehrungen in Bezug auf die Infiltration der informationstechnischen Systeme, die zum Zwecke der Ausübung der betreffenden Befugnisse zu treffen sind.

2. Verfassungsrechtlicher Maßstab

Verfassungsrechtlicher Maßstab für die Einordnung der Eingriffswirkung ist hier das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Im Wesentlichen hat das Bundesverfassungsgericht in seiner Entscheidung zur Online-Durchsuchung (BVerfG, Urteil vom 27. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822) den grundrechtlichen Eingriff, der

mit der Quellen-Telekommunikationsüberwachung einhergeht, zwar unter den Anwendungsbereich des Grundrechts auf Telekommunikationsgeheimnis gem. Art. 10 GG gefasst. Dies erfolgte jedoch in Bezug auf die Eingriffswirkung der Maßnahme auf die im Rahmen der Quellen-Telekommunikationsüberwachung erfassten Kommunikationselemente und nicht in Bezug auf die Eingriffswirkung, die mit dem heimlichen Zugriff auf das betreffende IT-System einhergeht, um die Vollziehung der Maßnahme erst möglich zu machen. Bezogen auf den Sachverhalt der zugrunde liegenden Verfassungsbeschwerden weist das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme den stärkeren sachlichen Bezug auf (vgl. zur Abgrenzung Petri, DuD 2008, 443 (444)).

Die staatliche Infiltration informationstechnischer Systeme hat das Bundesverfassungsgericht in seiner Entscheidung zur Online-Durchsuchung vom 27. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07 - als Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erachtet. Der Einwand der Subsidiarität, der grds. bezüglich des Verhältnisses von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und Art. 10 GG besteht, greift insoweit nicht. Das grundrechtliche Schutzbedürfnis folgt dabei einerseits aus der Bedeutung der Nutzung der informationstechnischen Systeme für die Persönlichkeitsentfaltung des Einzelnen und andererseits aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind. Da unbefugte Zugriffe auf informationstechnische Systeme vielfach unbemerkt bleiben, ist der Einzelne darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet (vgl. BVerfG, Urteil vom 27. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 (825 Rn. 181)). Geschützt sind danach IT-Systeme, „die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu entfalten." (BVerfG, Urteil vom 27. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 (827 Rn. 203)).

Der Schutzgehalt erschöpft sich nicht in der Vertraulichkeit der auf dem IT-System befindlichen personenbezogenen Daten, sondern erfasst auch die Integrität des IT-Systems an sich. Insoweit soll der Einzelne davor geschützt werden, dass auf das IT-System in einer Weise zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können (Roßnagel/Schnabel, NJW 2008, 3534 (3535)). Durch die technische Ermöglichung solcher Zugriffe werden Angriffe wie eine Ausspähung, Überwachung oder Manipulation des Systems ermöglicht (BVerfG, Urteil vom 27. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 (827) Rn. 204). Dieser auf den Adressaten der Maßnahme bezogene Abwehranspruch hat zur Folge, dass der Verantwortliche Veränderungen, die mit der Infiltration von IT-Systemen vorgenommen wurden, rückgängig machen muss. In Bezug auf die Rechtsgrundlagen zur Online-Durchsuchung und auch zur

Quellen-TKÜ ist in der Folge regelmäßig Regelungsgegenstand, technisch sicherzustellen, dass die vorgenommenen Veränderungen bei Beendigung der Maßnahmen soweit technisch möglich automatisiert rückgängig gemacht werden (s.u. Ziffer III.). Diese Vorgaben betreffen jedoch die aktiven Veränderungen eines bestimmten informationstechnischen Systems seitens der staatlichen Stellen. Diese Veränderungen sind auf ein aktives Tun des Staates zurückzuführen, während die Verfassungsbeschwerden das Unterlassen der Schließung der Schutzlücken betreffen, das die IT-Sicherheit im Ganzen gefährde.

3. Schutzpflichten des Staates in Bezug auf informationstechnische Systeme

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme beinhaltet eine objektiv-rechtliche Funktion. Der Staat hat danach die Aufgabe die IT-Sicherheit zu gewährleisten und muss geeignete Maßnahmen ergreifen, um zu verhindern, dass das Grundrecht durch Dritte verletzt wird. Diese Funktion wird u.a. auf die Bezeichnung als ein Grundrecht auf „Gewährleistung" zurückgeführt (vgl. Petri, DuD 2008, 443 (446)). Durch den Gewährleistungsauftrag muss der Staat mit effektiven Mitteln gewährleisten, dass unzulässige Gefährdungen der Vertraulichkeit und Integrität informationstechnischer Systeme auch im Privatrechtsverkehr unterbleiben. Die Rechtsbeziehung zwischen den Grundrechtsträgern und Privaten ist in der Folge durch Rechtsetzung, Vollziehung insbesondere in regulatorischer Form und durch Rechtsprechung vom Staat zu gestalten (vgl. Gusy, DuD 2009, 33 (37)).

Diese Ausprägung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme steht im Einklang mit der Rechtsprechung des Bundesverfassungsgerichts, wonach dem allgemeinen Persönlichkeitsrecht die lückenschließende Funktion zukommt, neuartigen Gefährdungen, zu denen es aufgrund des technischen und gesellschaftlichen Fortschritts kommen kann, durch Grundrechtsschutz zu begegnen (BVerfG, Urteil vom 27. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 (827 Rn. 169)). Diese Argumentation, die zur Schaffung des Grundrechts als eine Ausprägung des Allgemeinen Persönlichkeitsrechts an sich führte, streitet insoweit auch für den Gewährleistungsgehalt in einer objektiv-rechtlichen Funktion. Die zunehmende Digitalisierung des öffentlichen und privaten Lebens fördert die Abhängigkeit der Gesellschaft, Wirtschaft, Verwaltung und Daseinsvorsorge von informationstechnischen Systemen. In der Konsequenz sind diese informationstechnischen Systeme zunehmend Angriffsziel von Cyber-Attacken und Cyberkriminalität. Dies wird insbesondere an den zahlreichen Hacker-Angriffen auf kritische Infrastrukturen ersichtlich. Sowohl letztes als auch dieses Jahr sind in Rheinland-Pfalz solche Angriffe auf kritische Infrastrukturen erfolgt. Die Gefährdungen in Bezug auf die Integrität und Vertraulichkeit informationstechnischer Systeme sind aufgrund der Komplexität durch den Einzelnen nicht zu beherrschen. Der Staat muss angemessene Maßnahmen ergreifen, um Gefährdungen präemptiv vorzubeugen.

Vorrangige Konsequenz dieser Schutzfunktion ist, dass der Staat zum Schutze der Grundrechtsträger insbesondere Rechtsverhältnisse zwischen Privaten regeln bzw. regulieren soll. In den mit den Verfassungsbeschwerden aufgegriffenen Konstellationen ist er jedoch selbst Akteur in diesen Rechtsbeziehungen. Er nutzt bestehende Sicherheitslücken von IT-Systemen, die von den Herstellern unabsichtlich nicht geschlossen wurden, zur Vollziehung seiner individuell-konkreten Maßnahmen aus und ist damit selbst Nutznießer der Gefahren, die er eigentlich abwehren müsste. Fraglich ist vor diesem Hintergrund, in welchem Verhältnis die staatliche Schutzpflicht in Bezug auf IT-Sicherheit zu Grundrechtseingriffen infolge von staatlichen Eingriffsmaßnahmen z.B. aufgrund des Unterlassens der Schließung einer Sicherheitslücke, steht und welche Auswirkungen dies auf die Ausgestaltung der staatlichen Schutzmaßnahmen hat.

Unabhängig von der grundrechtsdogmatischen Konstruktion steht der Staat jedenfalls in einem Konflikt, wenn er einerseits die IT-Sicherheit gewährleisten muss, auf der anderen Seite jedoch systemische Schwachstellen benötigt, um mit den zur Verfügung stehenden Eingriffsbefugnissen die darauf fußenden Maßnahmen durchführen zu können (vgl. auch Derin/Golla, NJW 2019, 1111 (1114 f.)) und dabei kritischer Erfolgsfaktor ist, dass die Schwachstellen zunächst offen bleiben und die Hersteller nicht über die Schwachstellen informiert werden, um sie schließen zu können, damit der Erfolg der Maßnahme nicht gefährdet wird.

4. Zwischenfazit: Konsequenzen in Bezug zu dem Erfordernis staatlicher Maßnahmen

Die Schutzpflicht des Staates aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hat zur Folge, dass die Grundrechtsträger einen Anspruch darauf haben, dass der Staat wirksame Schutzmaßnahmen ergreift, um den Schutz, der von dem Grundrecht ausgeht, zu gewährleisten. Unterbleibt dies, wird die staatliche Schutzpflicht verletzt und eine Verletzung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme würde vorliegen. Staatlichen Stellen steht bei der Erfüllung der Schutzpflicht eine weite Entscheidungsprärogative zu.

III. Bestehen staatlichen Schutzvorschriften zur Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme

Einige verfahrens- und technikbezogene Regelungen des Sicherheitsrechts können als Schutzvorschriften bewertet werden, durch die der Staat seine Schutzpflicht in Bezug auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erfüllt. Sie sind Ausdruck des Grundsatzes der Verhältnismäßigkeit.

Sowohl das Hessische Gesetz über die Sicherheit und Ordnung als auch das Baden-Württembergische Polizeigesetz sehen in ihren Vorschriften zur Quellen-Telekommunikationsüberwachung (Hessen und Baden-Württemberg) und Online-Durchsuchung (Hessen) Regelungen vor, die mit den Maßnahmen einhergehende Veränderungen des informationstechnischen Systems betreffen. In § 23b Abs. 3 S. 1 PolG BW und § 15b Abs. 2 HSOG wird geregelt, dass bei Maßnahmen der Quellen-Telekommunikationsüberwachung sicherzustellen ist, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind (§ 23b Abs. 3 S. 1 Nr. 1 PolG; § 15b Abs. 2 S. 1 Nr. 1 HSOG.) und die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden (§ 23b Abs. 3 S. 1 Nr. 2 PolG; § 15b Abs. 2 Nr. 2 HSOG). In Satz 2 wird zudem geregelt, dass das eingesetzte Mittel gegen die unbefugte Nutzung zu schützen ist.
§ 15c Abs. 3 S. 1 HSOG verweist für die Maßnahme der Online-Durchsuchung auf die Regelungen des § 15b Abs. 2 HSOG.

Grundsätzlich zielen diese Regelungen darauf ab, dass der Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auf das erforderliche Maß begrenzt (§ 23b Abs. 3 S. 1 Nr. 1 PolG BW; § 15b Abs. 2 S. 1 Nr. 1 HSOG) und insbesondere durch die Rückgängigmachung der Infiltration beendet werden soll.

Durch § 23b Abs. 3 S. 2 PolG BW; § 15b Abs. 2 S. 2 HSOG werden zudem Anforderungen an die Ausgestaltung des Mittels, also der auf das informationstechnisches System aufgespielten Software gestellt. Dieses soll ausreichende Schutzvorkehrungen vorsehen, um die Nutzung durch unbefugte Dritte auszuschließen. Diese Regelungen gewährleisten zwar in Bezug auf das von der Maßnahme betroffene informationstechnische System und das zur Infiltration eingesetzte Mittel, dass Veränderungen nur vorübergehender Art sind und das System nach Beendigung der Maßnahme sowohl vor dem Zugriff der Sicherheitsbehörden als auch unbefugter Dritter wieder geschützt ist. Über diesen individualisierten und fallbezogen konkretisierten Anspruch hinaus werden jedoch keine Anforderungen gestellt, die dazu führen, dass der Verantwortliche auch die Sicherheitslücken, die zur Nutzung der Software bestehen müssen, schließen muss. Diese Lücken hat er ja nicht selbst geschaffen, sondern „lediglich" (aus-)genutzt, sie sind deswegen nicht als „Mittel" im Sinne der Vorschriften der § 23b Abs. 3 S. 2 PolG BW und § 15b Abs. 2 S. 2 HSOG zu qualifizieren.

Sonstige Regelungen in den betreffenden Polizeigesetzen, die als Schutzvorschriften zur Gewährleistung des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme in Bezug auf ein Schwachstellenmanagement qualifiziert werden können, sind nicht ersichtlich. Insbesondere auch Regelungen zum Grundrechtsschutz durch Verfahren wie die Regelungen des Richtervorbehalts in § 23b Abs. 4 S. 1PolG BW bzw. § 15b Abs. 3

S. 2 i.V.m. § 15 Abs. 5 HSOG reichen nicht zur Kompensation des Schutzdefizits aus, da sie den vorgelagerten Rechtsschutz und die Rechtskontrolle in Bezug auf die Grundrechte des betroffenen Einzelnen zum Ziel haben und dabei keine Bewertung der Auswirkungen der Maßnahmen in Bezug auf die kollektive IT-Sicherheit vornehmen.

Als weitere Vorkehrungen, die als Konkretisierung der Schutzpflichten verstanden werden können, kommen auf einer übergeordneten Ebene die Pflichten in Betracht, die für die heimliche Verarbeitung von personenbezogenen Daten gelten. Pflichten der Protokollierung (z.B. § 64 LDSG RP; siehe Art. 25 JI-RL) und Kennzeichnung (z.B. § 62 Abs. 2 LDSG RP; vgl. Art. 9 Abs. 3 JI-RL) der Daten dürfen nicht unangemessen verkürzt werden. Die Beachtung dieser Vorschriften muss sichergestellt werden. Die Kontrollbefugnis der zuständigen Datenschutzaufsichtsbehörde muss gewährleistet sein.

Zu den etwaigen Regelungen der Datenschutz-Grundverordnung (EU) 2016/679 oder solche, die im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 geschaffen wurden, die in diese Richtung weisen könnten, wird auf den Teil IV. der Stellungnahme verwiesen.

IV. Bedeutung der VO (EU) 2016/679 sowie der RL (EU) 2016/680 in diesem Zusammenhang

1. Anwendungsbereich der Richtlinie (EU) 2016/680

Die in den Verfassungsbeschwerden aufgegriffenen Problemfelder und angegriffenen Rechtsvorschriften betreffen die Eingriffsbefugnisse der Polizeibehörden des Landes Hessen und des Landes Baden-Württemberg. Die mit der Ausübung der Befugnisse einhergehenden Datenverarbeitungen erfolgen dabei zum Zwecke der Gefahrenabwehr und Straftatenverhütung und damit im Anwendungsbereich der Richtlinie (EU) 2016/680, welche nach Art. 1 der Richtlinie (EU) 2016/680 Bestimmungen 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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit beinhaltet.

2. Schutzniveau der Grundrechtecharta der Europäischen Union

Im Zusammenhang mit dem Beschwerdegegenstand der Verfassungsbeschwerden sind die europäischen Grundrechte des Rechts auf Achtung des Privat- und Familienlebens (Art. 7 Europäische Grundrechtecharta (GRCh)) und des Schutzes personenbezogener Daten (Art. 8 GRCh) relevant. Grundsätzlich wird mit der Rspr. des Europäischen Gerichtshofs (EuGH) eine Idealkonkurrenz zwischen Art. 7 und Art. 8 der Grundrechte-Charta angenommen (Jarass, Charta der Grundrechte der EU, 3. Auflage 2016 Art. 8 Rn. 4). Wie bereits in Bezug auf den verfassungsrechtlichen Maßstab erörtert, betrifft das in den Ver-

fassungsbeschwerden aufgegriffene Spannungsverhältnis nicht den Schutz der Kommunikation, sondern den Schutz vor unbefugten Zugriffen in informationstechnischen Systemen. In diesem Zusammenhang ist entsprechend der obigen Abgrenzung im Verhältnis zwischen Art. 7 und Art. 8 GRCh, Art 8 GRCh als betroffenem Grundrecht der Vorrang einzuräumen, da hier aufgrund des Vorliegens von Datenverarbeitungen der spezifische Technikbezug des Datenschutzes zum Tragen kommt (vgl. EuGH, Urt.v.16.7.2020, Rs. C-311/18 („Schrems II"), Rn. 170).

Auch wenn das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht unmittelbar kodifiziert, sondern im Rahmen der Rechtsprechung entwickelt wurde, steht der Gewährleistungsgehalt in seiner Ausprägung nicht hinter dem des Art. 8 GRCh zurück. Insoweit bestehen keine Anhaltspunkte, dass das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in der oben diskutierten Ausprägung das Schutzniveau der Grundrechtecharta nicht mit gewährleisten kann. Das Schutzniveau der Grundrechtecharta der Europäischen Union im Rahmen eines auf Vielfalt angelegten Grundrechtsschutzes dürfte durch den Grundrechtsschutz des Grundgesetzes in der konkreten Fallkonstellation gleichermaßen gewährleistet sein (vgl. BVerfG, Urteil v. 19. Mai 2020 – 1 BvR 2835/17, Rn. 326).

3. Systemdatenschutz des europäischen Datenschutzrechts

a) Vorgaben der Datenschutz-Grundverordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680

Durch Art. 5 DS-GVO und entsprechend Art. 4 Abs. 1 Richtlinie (EU) 2016/680 werden die Wertsetzungen des Art. 8 Grundrechtecharta der Europäischen Union zum Ausdruck gebracht (vgl. Albrecht/Jotzo, Das neue Datenschutzrecht der EU, Teil 2 Rn. 1). Dies betrifft auch den Grundsatz des Systemdatenschutzes (Art. 5 Abs. 1 lit. f DS-GVO bzw. Art. 4 Abs. 1 lit. f Richtlinie (EU) 2016/680). Er umfasst neben dem Schutz der Datenverarbeitung in Bezug auf die technischen Ziele der Integrität und Vertraulichkeit auch die Ziele der Verfügbarkeit und Unversehrtheit der Daten sowie der Beschränkung des Zugangs zu und des Zugriffs auf die Daten (vgl. Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art 5 Rn. 167 DS-GVO). Im Rahmen des durch die Datenschutz-Grundverordnung und Richtlinie (EU) 2016/680 geforderten Systemdatenschutzes werden Gehalte des Grundrechts auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme aufgegriffen, insbesondere die übergeordnete Verantwortlichkeit der Verantwortlichen in Bezug auf Funktionsweisen der IT-Systeme, die im Einflussbereich des Verantwortlichen liegen und außerhalb der Steuerungsmöglichkeiten der betroffenen Personen (vgl. Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art 5 Rn. 169 DS-GVO).
Konkretisiert wird der datenschutzrechtliche Grundsatz durch Anforderungen, Verarbeitungen datenschutzgerecht zu gestalten (data protection by design (Art. 24 DS-GVO) und

data protection by default (Art. 25 DS-GVO) bzw. Art. 20 Richtlinie (EU) 2016/680) und die Sicherheit der Verarbeitung gem. Art. 32 DS-GVO bzw. gem. Art. 29 Richtlinie (EU) 2016/680 zu gewährleisten.

Im Hessischen Datenschutz- und Informationsfreiheitsgesetz (HDSIG) werden diese Anforderungen der Richtlinie (EU) 2016/680 im Schwerpunkt in § 59 HDSIG in Bezug auf die Sicherheit der Verarbeitung umgesetzt sowie in Bezug auf Anforderungen an den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung in § 66 HDSIG.

Relevant hinsichtlich der in den Verfassungsbeschwerden geltend gemachten Schutzdefiziten, die mit der Nutzung von den Herstellern unbekannten Sicherheitslücken der informationstechnischen Systeme zusammenhängen, sind dabei zuvörderst die Anforderungen zur Sicherheit der Verarbeitung. Die Vorgaben des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen betreffen weniger die Datensicherheit, sondern die Gewährleistung der Zulässigkeit der Verarbeitung durch technisch-organisatorische Maßnahmen.

b) Umsetzung der unionrechtlichen Vorgaben im Hessischen Datenschutzrecht

Nach § 59 Abs. 1 HDSIG soll der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen sollen gem. § 59 Abs. 2 S. 2 Nr. 1 HDSIG dazu führen, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden.

Diesen Vorgaben liegt der Präventionsgedanke zugrunde, wonach vorsorglich bestimmte Risiken, die in Bezug auf die Sicherheit der Verarbeitung bestehen, mit geeigneten Maßnahmen entgegen gewirkt werden sollen, die nicht nur die Sicherheit der Verarbeitung betreffen, sondern auch die Sicherheit der Systeme und Dienste, die „im Zusammenhang" mit der Verarbeitung genutzt werden (vgl. Hansen in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht Art. 32 Rn. 36 DS-GVO; Piltz in Gola, BDSG, 2. Aufl. 2018, Art. 32 Rn. 29 DS-GVO). Die Anforderungen an die IT-Sicherheit beziehen sich auf die Systeme als Ganzes und umfassen sowohl die Hard- und Software als auch die Netzwerkkomponenten. Die Anforderungen, dass diese Sicherstellung auf Dauer angelegt sein soll, erfordert die regelmäßige Evaluierung und Anpassung der getroffenen Maßnahmen der Sicherheit der Verarbeitung (vgl. Jandt in Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 32 Rn. 22 DS-GVO).

Die Gewährleistung der Vertraulichkeit umfasst dabei den Schutz vor unbefugter Preisgabe von Informationen. In dem Sinne dürfen vertrauliche Daten nur den Berechtigten zur Verfügung stehen bzw. zugänglich sein (vgl. Hansen in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht Art. 32 DS-GVO Rn. 38). Diese Vertraulichkeit soll nach dem Wortlaut neben den personenbezogenen Daten auch in Bezug auf das System bestehen. Dies betrifft auch die Integrität, die sich sowohl in Bezug auf die Unversehrtheit von Daten als auch auf die korrekte Funktionsweise von Systemen beziehen kann (vgl. Hansen in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht Art. 32 DS-GVO Rn. 40 mit Verweis auf BSI, IT-Grundschutz-Kompendium, Integrität, Glossar, 2018).

In Bezug auf die Integrität und Vertraulichkeit informationstechnischer Systeme sind insbesondere die Netzwerkschnittstellen als Einfallstor für Sicherheitsrisiken relevant, die etwa durch Schadsoftware, "Trojanische Pferde" oder Spyware in Bezug auf die Integrität der Systeme bestehen. Insofern muss der Verantwortliche im Bereich der Richtlinie (EU) 2016/680 entsprechend der Vorgaben des § 59 Abs. 2 S. 2 Nr. 1 HDSIG Schutzvorkehrungen in Bezug auf die Integrität und Vertraulichkeit von informationstechnischen Systemen und Diensten treffen.

Die Anforderungen sind ähnlich den Vorgaben in der Datenschutz-Grundverordnung und der Richtlinie (EU) 2016/680 weit gefasst und lassen dem Verantwortlichen einen Spielraum, welche Maßnahmen er zur Gewährleistung der Sicherheit der Verarbeitung erlässt. Dieser weite Ermessenspielraum ist zweckmäßig, da die Maßnahmen sich an dem Risiko, welches für die Verarbeitung und die in diesem Zusammenhang genutzten Systeme besteht, orientieren und der Ermessensspielraum es zulässt, zielgenaue Maßnahmen technischer oder organisatorischer Art vorzunehmen, die individuell auf das identifizierte Sicherheitsrisiko zugeschnitten sind.

Solche können auch in Form des geforderten Schwachstellenmanagements erfolgen, im Rahmen dessen Maßnahmen in Bezug auf die Beschaffenheit, Funktionalität und Anwendungskontrolle hinsichtlich des Mittels, welches zur staatlichen Infiltration informationstechnischer Systeme genutzt wird, bestehen. Durch die extensiv ausgestaltete Regelung des § 59 Abs. 2 S. 2 Nr. 1 HDSIG sind die Anforderungen jedoch nicht in einem Maß zwingend, das geeignet wäre das unter Ziffer II. identifizierte Schutzdefizit zu kompensieren. Dazu sind hinreichend bestimmte und konkret auf das Problem der Nutzung sog. 0-Day-Verfahren im Rahmen der Quellen-Telekommunikationsüberwachung oder Online-Durchsuchung zugeschnittene Regelungen erforderlich.

c) Umsetzung der unionsrechtlichen Vorgaben im baden-württembergischen Datenschutzrecht

In Baden-Württemberg wurden die Vorgaben der Richtlinie (EU) 2016/680 in den Fachgesetzen der Polizeibehörden noch nicht umgesetzt. Im Rahmen der Anpassung des Landesdatenschutzgesetzes (LDSG BW) an die Datenschutz-Grundverordnung wurde die Übergangsvorschrift des § 30 LDSG BW geschaffen. Nach § 30 Abs. 1 LDSG BW gilt für die Verarbeitung personenbezogener Daten durch die Polizeibehörden und den Polizeivollzugsdienst, soweit sie nicht die Verordnung (EU) 2016/679 anzuwenden haben, das Landesdatenschutzgesetz in der am 20. Juni 2018 geltenden Fassung weiter, bis die Regelungen des Landes Baden-Württemberg zur Umsetzung der Richtlinie (EU) 2016/680 für den Bereich der Polizei in Kraft treten. Insofern ist eine bereichsspezifische Umsetzung der Vorgaben des Art. 29 Richtlinie (EU) 2016/680, mit dem ein gewisses Maß an Systemdatenschutz einhergeht (s.o.), noch nicht erfolgt. Andere Schutzmaßnahmen durch die die Schutzdefizite kompensiert werden können, sind in Bezug auf den § 23b PolG BW nicht ersichtlich.

V. Schlussfolgerungen

Dem Staat obliegt von Verfassungswegen die Pflicht, den Einzelnen vor den Gefahren, die von informationstechnischen Systemen ausgehen, zu schützen. Die Funktion der Schutzpflicht, die im vorliegenden Zusammenhang in Bezug auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG besteht, gibt dem Staat hinsichtlich der Erfüllung seines Gewährleistungsauftrags dabei eine weite Einschätzungsprärogative.

Die Regelungen des Polizeigesetzes Baden-Württemberg und des Hessischen Gesetzes über die Sicherheit und Ordnung in der streitgegenständlichen Fassung stellen keine hinreichenden konkreten gesetzlichen Anforderungen an den allgemeinen Schutz informationstechnischer Systeme, die hinreichend effektiv den Grundrechtsschutz in Bezug auf die Gefahren, die von offen gehaltenen Sicherheitslücken im Wege des sog. 0-Day-Verfahrens ausgehen, gewährleisten.

Die Anforderungen des europäischen Datenschutzrechtes zielen auf einen Systemdatenschutz ab, der insbesondere die Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen soll. Dazu sind die erforderlichen Maßnahmen seitens des Verantwortlichen zu treffen. In Bezug auf die Rechtslage in Hessen wurden die entsprechenden Vorgaben des Art. 29 der hier anwendbaren Richtlinie (EU) 2016/680 in § 59 des Hessischen Datenschutz- und Informationsfreiheitsgesetz umgesetzt. Diese könnten grundsätzlich auch die von den Beschwerdeführer_innen mit der Verfassungsbeschwerde Az. 1 BvR 1552/19 geforderten Maßnahmen eines Schwachstellenmanagements sein, durch das angemessene Vorkehrungen gegen die durch den Einsatz von Staatstrojanern geförderten Fehlentwicklungen getroffen werden. Die Regelungen des § 59 Abs. 2 S. 2 Nr. 1 HDSIG sind jedoch nicht hinreichend konkret und effektiv ausgestaltet, um den erforderlichen Grundrechtsschutz zu erreichen, der in Bezug auf das Schutzdefizit im Hinblick auf die

sog. 0-Day-Verfahren erforderlich ist und von den Beschwerdeführen gefordert wird (Regelungen in Bezug auf die Beschaffenheit, Funktionalität und Anwendungskontrolle der Überwachungssoftware).

Aufgrund des bestehenden Schutzdefizits, welches zur Folge hat, dass durch Ausübung der Befugnisse gem. § 15b und § 15c HSOG das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verletzt wird, sind infolge des Verstoßes gegen das Untermaßverbot diese Vorschriften verfassungswidrig.

Das Datenschutz- und das Sicherheitsrecht des Landes Baden-Württemberg sieht keine Vorschriften vor, mit denen die Schutzpflicht des Staates, die Integrität und Vertraulichkeit informationstechnischer Systeme in Bezug auf die die sog. 0-Day-Verfahren zu gewährleisten, erfüllt wird. Da die Richtlinie (EU) 2016/680 noch nicht im Polizeirecht des Landes Baden-Württemberg umgesetzt wurde, sind auch nicht die Umsetzungsvorschriften zum Systemdatenschutz im Anwendungsbereich der Richtlinie (EU) 2016/680 heranzuziehen.

In der Folge ist die Befugnis zur Quellen-Telekommunikationsüberwachung gem. § 23b Abs. 2 PolG BW mangels Schutzvorschriften verfassungswidrig.

Mainz, den 09.10.2020

Prof. Dr. Dieter Kugelmann