Prof. Dr. Tobias Singelnstein
(…)

An das
Bundesverfassungsgericht
Schlossbezirk
76131 Karlsruhe

Bochum, 7. Dezember 2018

In dem Verfahren

1. des Rechtsanwalts Dr. Udo Kauß, (…).
2. des Rechtsanwalts Michael Moos, (…),
3. des Journalisten Peter Welchering, (…)
4. des Journalisten Hinnerk Feldwisch-Drentrup, (…)
5. des Chaos Computer Club Stuttgart e.V., c/o Hanno Wagner, Mittelfeldstraße 23, 70806 Kornwestheim, vertreten durch den Vorstand Hanno Wagner und Stefan Leibfarth, (…),
6. des Internet Service Providers ISP Service eG, Mezgerstraße 34, 70563 Stuttgart, vertreten durch den Vorstand Kurt Jaeger und Björn Schwarze, (…),
7. des Onlinehandels und Ladengeschäfts zündstoff. - S. Klemz & M. Rau GbR, Rehlingstraße 7, 79100 Freiburg, vertreten durch ihre geschäftsführenden Gesellschafter Sascha Klemz und Matthias Raus, (…).

erhebe ich namens und in Vollmacht der Beschwerdeführer*innen

Verfassungsbeschwerde

gegen

> § 23b Abs. 2 Polizeigesetz Baden-Württemberg (PolG BW) in der Fassung des Gesetzes zur Änderung des Polizeigesetzes vom 28.11.2017 (GBl. S. 624)

und rüge eine Verletzung von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG in der Ausprägung als Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme.

Gliederung des Schriftsatzes

A. Einleitung

Diese Verfassungsbeschwerde betrifft die rechtsstaatlichen Anforderungen an den Einsatz sogenannter „Staatstrojaner“ als Standardmaßnahme im Rahmen der polizeilichen Gefahrenabwehr. Die in § 23b Abs. 2 i.V.m. Abs. 1 PolG BW nunmehr vorgesehene Rechtsgrundlage für „Quellen-Telekommunikationsüberwachung“ (Quellen-TKÜ) ermöglicht es, über die Einspeisung eines Staatstrojaners in ein informationstechnisches System (IT-System) einzudringen und so unter anderem Kommunikationsdaten am Gerät abzufangen und zu überwachen, bevor diese verschlüsselt und verschickt werden. Durch das Eindringen in das IT-System wird dabei seine Integrität und Vertraulichkeit vollständig aufgehoben; dies gilt ungeachtet der Tatsache, dass dann nur bestimmte Daten – etwa „laufende Kommunikation“ – ausgeleitet werden.

Während es aufgrund der seit 2009 geltenden Rechtsgrundlagen für solche Eingriffe im Gesetz über das Bundeskriminalamt nur zu einer kleinen zweistelligen Zahl von Maßnahmen gekommen ist, die zudem entsprechend der Aufgabenzuweisung an das BKA nur den Bereich der Abwehr terroristischer Gefahren betrafen, erlauben vergleichbare Rechtsgrundlagen der StPO inzwischen den Einsatz von Staatstrojanern in mehreren 10.000 Fällen im Jahr, nämlich in allen Fällen, in denen zuvor eine klassische Telekommunikationsüberwachung gem. § 100a Abs. 1 StPO unter Einbindung der jeweiligen Provider (vgl. § 100b StPO a.F.) vorgenommen wurde. Durch eine Erweiterung dieser Befugnisse auch auf den Bereich der polizeilichen Gefahrenabwehr auf Landesebene droht sich diese Fallzahl weiter zu erhöhen.

Die Beschwerdeführer greifen die Regelung im Polizeigesetz Baden-Württemberg dabei *nicht* aus abwehrrechtlicher Perspektive an, sondern rügen die folgende Leerstelle: Das Land Baden-Württemberg ist bei der Regelung der Quel-

len-TKÜ seiner Verpflichtung nicht nachgekommen, entsprechend dem Grundrecht auf **Gewährleistung** der Integrität und Vertraulichkeit informationstechnischer Systeme einen Rechtsrahmen für den Einsatz von Staatstrojanern zu schaffen, der geeignet ist, fatale Fehlanreize für seine Behörden zu vermeiden, die die IT-Sicherheit im Geltungsbereich des Grundgesetzes und darüber hinaus insgesamt unterminieren.

Nach § 23b Abs. 2 i.V.m. Abs. 1 PolG BW sollen Gefahrenabwehrbehörden in informationstechnische Systeme „eingreifen" dürfen, um aus ihnen Daten zu erheben. Hierzu ist denklogisch ein „Fuß in der Tür" erforderlich, also das Aufbringen einer hoheitlichen Software in dem informationstechnischen System der von einer Überwachung betroffenen Personen, die Daten ausliest und an die Polizei übermittelt. Solche Software-Lösungen werden allgemein als Staatstrojaner bezeichnet.

Weder das PolG BW in der angegriffenen Fassung noch die Begründung des Gesetzesentwurfs zur Einführung der angegriffenen Normen definieren indes, wie ein Staatstrojaner auf das Zielsystem aufgebracht werden darf. Denkbar sind insbesondere folgende Wege:

- Aufspielen durch Hoheitsträger, etwa bei einer Grenzkontrolle,
- Aufspielen durch Hoheitsträger nach heimlichem Betreten der Räumlichkeiten, in denen sich das System befindet,
- Ausnutzen der Unaufmerksamkeit des berechtigten Nutzers, etwa indem man ihm einen E-Mail-Anhang mit einem (getarnten) Infektions-Programm in der Hoffnung zuspielt, dass er ihn ausführen werde,
- Aufspielen durch Ausnutzen von Sicherheitslücken des genutzten Systems, etwa indem der berechtigte Nutzer zum Aufruf einer speziell präparierten WWW-Seite animiert wird, deren bloße Ansicht aufgrund von

Sicherheitslücken zur Infektion des Zielsystems führt (sogenannte *drive by downloads*).

Es erschließt sich unmittelbar, dass die rechtliche Bewertung der Zugriffe völlig unterschiedlich ausfällt: Das Betreten von Räumlichkeiten zur Infektion von Systemen ist im Lichte von Art. 13 Abs. 1 GG ohne eine (bisher fehlende, rechtspolitisch aber mitunter bereits geforderte) spezifische Ermächtigungsgrundlage schlechthin rechtswidrig. Das Aufspielen etwa bei einer Grenzkontrolle hingegen ist als solches unbedenklich. Einen Grenzfall stellt das Zusenden einer E-Mail mit einem getarnten Staatstrojaner dar.

Die Infektion des Zielsystems durch Ausnutzen von Sicherheitslücken bietet für einen Zugriff auf Daten besondere praktische Vorteile. Solche Sicherheitslücken werden deshalb auf dem internationalen Schwarzmarkt für hohe Summen verkauft und spielen eine zentrale Rolle sowohl für Überwachungsmaßnahmen staatlicher Stellen als auch für die organisierte Kriminalität. Es ist davon auszugehen, dass sie auch bei der Umsetzung von Maßnahmen nach § 23b Abs. 2 i.V.m. Abs. 1 PolG BW von herausgehobener Bedeutung sind oder sein werden.

Die Möglichkeit für Polizeibehörden Baden-Württembergs, Quellen-TKÜ durch Ausnutzen von Sicherheitslücken durchzuführen, führt hingegen zu gravierenden Fehlanreizen: Wenn Polizeibehörden solche Lücken ausnutzen dürfen, so haben sie ein – isoliert betrachtet – durchaus nachvollziehbares Interesse daran, ein „Arsenal“ von Sicherheitslücken aufzubauen, um im Falle des Falles eine Zielperson angreifen zu können. Dieses Interesse wird sie jedoch davon abhalten, eine entdeckte oder gar auf dem Schwarzmarkt angekaufte Sicherheitslücke den jeweiligen Herstellern der IT-Systeme mitzuteilen, damit die Lücken geschlossen werden können. So entstehen Anreize für Behörden, ihnen

bekannte Sicherheitslücken gerade nicht schließen zu lassen, sondern sie lieber zu „horten“.

Tatsächlich kaufen deutsche staatliche Stellen bereits Sicherheitslücken auf dem Schwarzmarkt auf bzw. haben entsprechende Mittel im Zuge der Haushaltsberatungen bewilligt bekommen. Dies führt dazu, dass Sicherheitslücken nicht nur nicht geschlossen werden. Vielmehr wird der bestehende Schwarzmarkt noch zusätzlich angeheizt. Hohe und steigende Preise für Sicherheitslücken wiederum schaffen vermeidbare Anreize für Sicherheitsforscher, ihre Erkenntnisse nicht den Herstellern zur Verfügung zu stellen, sondern sie auf dem Schwarzmarkt zu verkaufen.

Solange aber die Lücken nicht von den Herstellern der Systeme geschlossen werden können, weil sie von ihnen keine Kenntnis erlangen, können natürlich nicht nur die Polizei Baden-Württembergs diese Lücken für den Einsatz von Staatstrojanern ausnutzen. Vielmehr kann jeder, der sie findet oder seinerseits auf dem Schwarzmarkt für Sicherheitslücken kauft, diese Lücken zur Infiltration informationstechnischer Systeme missbrauchen. Das gilt insbesondere auch für Cyber-Kriminelle, die es beispielsweise regelmäßig darauf anlegen, möglichst viele Systeme zum Teil eines sogenannten Botnetzes zu machen oder Zahlungsdaten für Online-Überweisungen von ihnen abzugreifen.

Im Ergebnis setzen staatliche Stellen bereits heute Millionen Nutzer*innen von IT-Systemen weltweit, die von einer den Behörden bekannten Lücke betroffen sind, einem fortbestehenden Risiko von Cyber-Angriffen aus, um diese Sicherheitslücken im Einzelfall selbst für Ermittlungsmaßnahmen in der hier angegriffenen Form ausnutzen zu können. Diese Kollateralschäden werden in Kauf genommen, nur um mit Blick auf die erstrebte Sanktionierung einer Einzelper-

son wegen einer vermuteten Straftat den Sachverhalt aufzuklären oder den Aufenthaltsort des Beschuldigten zu ermitteln. Das Missbrauchsrisiko, das hier durch ein Horten von Sicherheitslücken bewusst eingegangen wird, steht in keinem ausgewogenen Verhältnis zu dem verfolgten Zweck, nämlich der (möglicherweise) erleichterten Gefahrenabwehr im Einzelfall.

Die Ausnutzung von staatlicherseits geheim gehaltenen Sicherheitslücken ist durchaus keine düstere Fantasie, sondern bittere Realität. Erinnert sei an den Vorfall um „WannaCry“ vom 12. Mai 2017: Innerhalb weniger Stunden infiltrierte dieses Schadprogramm, ein sog. Kryptotrojaner, weltweit etwa 220.000 Systeme. Der Trojaner verschlüsselte die Daten auf den betroffenen Computern und bot den Nutzern zeitgleich einen Code für die Entschlüsselung an, ansonsten werde die Löschung der Daten veranlasst. In Deutschland war davon bspw. die Deutsche Bahn betroffen. Besonders schwer traf es das Gesundheitssystem in Großbritannien. Zahlreiche Rechner des National Health Service waren befallen. Patient*innen berichteten von chaotischen Zuständen. Die Daten von Krebs- und Herzpatient*innen standen nicht mehr zur Verfügung. Viele Kranke mussten in andere Kliniken umgeleitet werden.

Der WannaCry-Trojaner nutzte eine Lücke im Betriebssystem Microsoft Windows. Diese Lücke war schon Jahre zuvor von der National Security Agency, des auf Hacking spezialisierten US-Geheimdienstes, entdeckt, aber nicht an den Hersteller Microsoft gemeldet worden, damit er die Sicherheitslücke schließe. Brad Smith, Präsident von Microsoft, erhob in einer Erklärung den Vorwurf, die Geheimdienste würden diese Lücken absichtsvoll horten, statt sie sofort an die Hersteller zu melden.

Angesichts der Erfahrungen mit diesem Kryptotrojaner, dessen schnelle Verbreitung weltweit zu einem zeitweiligen Stillstand von Gesundheits- und Verkehrseinrichtungen geführt hat, bekommen die eindringlichen Worte des angerufenen Gerichts in seinem Urteil vom 27. Februar 2008 ein zusätzliches Gewicht:

> *„Je nach der eingesetzten Infiltrationstechnik kann die Infiltration auch weitere Schäden verursachen, die im Zuge der Prüfung der Angemessenheit einer staatlichen Maßnahme mit zu berücksichtigen sind. Wird dem Betroffenen etwa eine Infiltrationssoftware in Form eines vermeintlich nützlichen Programms zugespielt, lässt sich nicht ausschließen, dass er dieses Programm an Dritte weiterleitet, deren Systeme in der Folge ebenfalls geschädigt werden. Werden zur Infiltration bislang unbekannte Sicherheitslücken des Betriebssystems genutzt, kann dies einen Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme auslösen. In der Folge besteht die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sie sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben. Der Zielkonflikt könnte daher das Vertrauen der Bevölkerung beeinträchtigen, dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist.“*
>
> BVerfGE 120, 274 <325 f.>.

Eine solche Güterabwägung, die aus der isoliert auf den Ermittlungserfolg fokussierenden Sicht einer Gefahrenabwehrbehörde vielleicht noch nachvollziehbar sein mag, verbietet sich aus der Perspektive des Gesetzgebers, der das Wohl

der Allgemeinheit in den Blick zu nehmen hat. Nicht zuletzt hat sich die Landesregierung Baden-Württemberg politisch zur Förderung der IT-Sicherheit bekannt.

> Winfried Kretschmann, Ministerpräsident des Landes Baden-Württemberg, dazu am 19. September 2017 anlässlich der Initiierung der Cyberwehr BW, einer IT-Beratungsstelle: „Baden-Württemberg soll zur digitalen Leitregion werden, dazu haben wir vor dem Sommer die Digitalisierungsstrategie digital@bw vorgestellt. Eine wichtige Voraussetzung dabei ist die Cybersicherheit. Gefahren und Angriffen aus dem Netz müssen wir uns gezielt entgegenstellen, denn Cyberattacken wie Wannacry verunsichern die Bürgerinnen und Bürger und sie gefährden Geschäftsmodelle."
>
> Online abrufbar unter https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/landesregierung-initiiert-cyberwehr-baden-wuerttemberg/ (zuletzt abgerufen am 26. November 2018).

Damit sind Anreize für staatliche Behörden, die Cyber-Sicherheit in Deutschland und weltweit zu schwächen, schlechthin unvereinbar. Die Beförderung dieser immensen Sicherheitsgefahren darf nicht der Preis sein, wenn der ohnehin schon weit reichende Katalog an präventiven Eingriffsmaßnahmen noch um eine weitere ergänzt wird.

Die in § 23b Abs. 2 PolG BW geschaffenen Regelung ist deshalb mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG) erst dann vereinbar, wenn sie von einem Schwachstellen-Management begleitet wird, welches die Verwendung von bisher unbekannten Sicherheitslücken (sog. *0-days*) verbietet, solange der Hersteller des Systems nicht über die

Lücke informiert ist. Es ist sicherzustellen, dass sich alle Behörden dafür einsetzen, ihnen bekannte Sicherheitslücken durch die Hersteller so schnellstmöglich schließen zu lassen.

Daraus resultiert auch keine erhebliche Beeinträchtigung der Gefahrenabwehr. Denn eine Sicherheitslücke, die dem Hersteller bereits bekannt ist, aber beispielsweise wegen Nachlässigkeit des Systembetreibers noch nicht geschlossen wurde, kann aus der Perspektive der IT-Sicherheit durch staatliche Stellen ausgenutzt werden. Gleiches gilt für Sicherheitslücken, die nicht auf Fehlern der Hersteller beruhen, sondern auf einer individuellen fehlerhaften Einrichtung des informationstechnischen Systems.

Die Beschwerdeführer erbitten im Sinne der vorstehenden Überlegungen eine Weiterentwicklung des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme durch explizite Anerkennung seiner objektiv-rechtlichen Dimension sowie eine Aufforderung an den Gesetzgeber, ein Regime zur angemessenen Behandlung von IT-Sicherheitslücken einzuführen.

B. Sachverhalt

I. Verfahrensgegenstand

Mit ihrer Verfassungsbeschwerde rügen die Beschwerdeführer*innen, dass das Land Baden-Württemberg durch die Einführung der angegriffenen Rechtsgrundlage seine aus der objektiv-rechtlichen Dimension des Grundrechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme erwachsende Schutzpflicht verletzt hat, weil es an zwingend gebotenen Begleitregelungen zum verantwortungsvollen staatlichen Umgang mit IT-Sicherheitslücken fehlt. Dadurch hat das Land sie in ihren Grundrechten verletzt.

II. Die Beschwerdeführer*innen

1. Beschwerdeführer zu 1

Der Beschwerdeführer zu 1 ist ein deutschlandweit renommierter Rechtsanwalt mit Kanzleisitz in Freiburg. Er konzentriert sich in seiner anwaltlichen Tätigkeit insbesondere auf bürgerrechtliche Themen mit entsprechender gerichtlicher Durchsetzung. Als Vorsitzender des Landesverbandes der Humanistischen Union Baden-Württemberg wird er des Öfteren als Anwalt auf die Übernahmen von bürgerrechtlichen Mandaten angesprochen, die ihren Schwerpunkt im Datenschutzbereich haben, und denen Befürchtungen der Mandantschaft zugrunde liegen, dass insbesondere ausländische Geheimdienste in ihre IT-Systeme eindringen und sie überwachen.

Beispielsweise vertritt er den Bremer Rechtsanwalt und stellvertretenden Richter am Staatsgerichtshof der Freien Hansestadt Bremen Dr. Rolf Gössner in dessen Klage auf Feststellung der Rechtswidrigkeit seiner 38 Jahre währenden Überwachung durch den Verfassungsschutz. Das Verfahren ist aktuell beim

Bundesverwaltungsgericht anhängig, in beiden Vorinstanzen wurde die Rechtswidrigkeit gerichtlich festgestellt.

> OVG Münster, Urteil vom 13. März 2018, 16 A 906/11, DÖV 2018, 719. Siehe hierzu auch die Berichterstattung der Frankfurter Rundschau, Im Auge des Staatsschutzes. Der Rechtsstreit mit dem Menschenrechtler Rolf Gössner geht in nächste Instanz, 12. Juni 2018, online abrufbar unter http://www.fr.de/politik/menschenrechtler-im-auge-des-staatsschutzes-a-1523653 (zuletzt abgerufen am 27. November 2018).

Immer wieder vertritt er auch Mandant*innen, die eine Überwachung nicht durch inländische, sondern ausländische Dienste befürchten. So beispielsweise in einem 2014 vom Bundesverwaltungsgericht entschiedenen Fall. Sein Mandant, ein IT-Spezialist mit zehnjähriger Erfahrung im sicherheitsgeprüften Bereich, befürchtete eine Überwachung durch den amerikanischen Geheimdienst.

> Der Mandant klagte dabei erfolgreich auf Feststellung, dass die Weigerung des Bundesministeriums des Innern rechtswidrig war, den Ausdruck zu seiner Person im Nachrichtendienstlichen Informationssystem (NADIS) vollständig ohne Schwärzung vorzulegen. Siehe BVerwG, Beschluss vom 27.10.2014, BVerwG 20 F 6.14, LKV 2015, 129.

Zudem berät er auch im Asyl- und Ausländerrecht und hat dort mit Mandant*innen zu tun, die ihre Heimatländer aufgrund politischer Verfolgung verlassen haben und wiederum eine Überwachung fürchten. Darunter sind immer wieder auch türkisch-kurdische Geflüchtete, die in ihrer türkischen Heimat verfolgt werden. Viele seiner Mandant*innen haben damit ein besonderes Interesse und Bedürfnis an der Vertraulichkeit der IT-gestützten Kommunikation.

Es ist bekannt, dass ausländische Geheimdienste für die Kommunikationsüberwachung gerade den Zugriff über IT-Schwachstellen wählen. Das gilt insbesondere für US-Geheimdienste.

> Siehe dazu Patrick Beuth, Mut zur Lücke, ZEIT vom 22.08.2016, online abrufbar unter https://www.zeit.de/digital/datenschutz/2016-08/nsa-shadow-brokers-zero-days-zitis (zuletzt abgerufen am 4. Dezember 2018).
>
> Das Schadprogramm WannaCry, Sicherheitslücken, welche die National Security Agency, ein US-Geheimdienst, dieser für seine Arbeit genutzt hatte. Siehe dazu etwa https://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung (zuletzt abgerufen am 31. Juli 2018)

Der Beschwerdeführer zu 1 verwendet für seine Arbeit mehrere Computer sowie ein Smartphone. Seine E-Mail-Adresse hat der Beschwerdeführer zu 1 an verschiedenen Stellen im Internet öffentlich vermerkt, so dass sie auch einem Erstkontakt offensteht. Mit Mandant*innen kommuniziert der Beschwerdeführer zu 1 größtenteils auf elektronischem Weg, insbesondere durch E-Mails. Dabei bietet er eine PGP-Verschlüsselung an, die eine Vertraulichkeit der Kommunikation gewährleisten soll.

2. Beschwerdeführer zu 2

Der Beschwerdeführer zu 2 ist ein renommierter Fachanwalt für Strafrecht und hat ebenfalls seinen Kanzleisitz in Freiburg. Schwerpunkte seiner Arbeit liegen im Strafrechts- und Strafvollstreckungsverfahren, insbesondere in Kapitalstrafsachen sowie im Betäubungsmittelrecht und Jugend- und Ausländerstrafsachen. Häufig vertritt der Beschwerdeführer zu 2 dabei Mandant*innen aus politischen Kreisen, dazu zählen in der Vergangenheit Sympathisant*innen der RAF sowie

nach wie vor Mandant*innen aus der antifaschistischen Szene sowie Sympathisant*innen der kurdischen Arbeiterpartei PKK. Er war und ist dabei als Verteidiger in zahlreichen Verfahren vor dem OLG Stuttgart tätig, in denen in Deutschland lebende Kurden angeklagt sind, die PKK unterstützt zu haben (§ 129b StGB). Die Organisation wird unter anderem von der Türkei als Terrororganisation eingestuft und bekämpft. Vermeintliche oder tatsächliche Unterstützer*innen der PKK in Deutschland sehen sich einer Bedrohung durch den türkischen Geheimdienst ausgesetzt und sind deshalb auch in besonderem Maße auf den Schutz ihrer IT-Systeme angewiesen.

> Die Bedrohung durch den türkischen Geheimdienst ist dabei auch in Deutschland sehr real. Berichten der Zeitung die WELT zufolge ist neben einer großen Zahl von Agenten von etwa 6.000 Informanten des türkischen Geheimdienstes MIT in Deutschland auszugehen. *Thorsten Jungholt/Martin Lutz/Uwe Müller (u.a.),* Erdogans Agenten bedrohen Türken in Deutschland, die WELT vom 21. August 2016, online abrufbar unter https://www.welt.de/politik/deutschland/article157778863/Erdogans-Agenten-bedrohen-Tuerken-in-Deutschland.html (zuletzt abgerufen am 4. Dezember 2018).

Es ist davon auszugehen, dass auch der türkische Geheimdienst MIT auch Spyware benutzt, die 0-day-Schwachstellen ausnutzt.

> Ein kanadische Sicherheits- und Menschenrechtsorganisation, hat aufgedeckt, dass unter anderem auch in der T https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/ Siehe dazu auch *Simon Beuth*, Mut zur Sicherheitslücke, die ZEIT vom 22. August 2016, online abrufbar unter https://www.zeit.de/digital/datenschutz/2016-08/nsa-shadow-brokers-zero-days-zitis (zuletzt abgerufen am 4. Dezember 2018).

Viele der Mandant*innen des Beschwerdeführers zu 2 legen damit ebenfalls gesteigerten Wert auf eine besondere IT-Sicherheit, dies weil sie eine Überwachung durch inländische und ausländische Geheimdienste fürchten.

Zudem ist der Beschwerdeführer zu 2 seit 1999 politisch aktiv und als Stadtrat der Linken Liste und Fraktionsvorsitzender der Unabhängigen Liste im Gemeinderat von Freiburg. Der Beschwerdeführer zu 2 wurde seit den 1970er Jahren über einen Zeitraum von mindestens 20 Jahren vom Verfassungsschutz Baden-Württemberg überwacht. Eine Klage auf Feststellung der Rechtswidrigkeit dieser Überwachung ist beim Verwaltungsgericht Stuttgart derzeit anhängig (Az. 1 K 493/17).

Als Anwalt wie auch im Rahmen seiner politischen Tätigkeit im Stadtrat nutzt der Beschwerdeführer zu 2 mehrere Computer sowie ein Smartphone und kommuniziert mit Mandant*innen auch auf elektronischem Weg, insbesondere per E-Mail, sowie manchmal per SMS sowie mit dem verschlüsselten Messenger-Dienst Threema. Seine E-Mail-Adresse hat er auf seiner Homepage als Anwalt veröffentlich, auf der Seite der Linken Liste neben der E-Mail-Adresse auch seine Handynummer. Diese Kommunikationswege können daher von potentiellen Mandant*innen auch für den Erstkontakt genutzt werden.

3. Beschwerdeführer zu 3

Der Beschwerdeführer zu 3 ist ein renommierter investigativer Journalist und arbeitet für Radio, Fernsehen und Print, dabei unter anderem für Deutschlandradio, ZDF, verschiedene ARD-Sender und die FAZ. Er wurde 2004 gemeinsam mit Mirko Smiljanic mit dem Helmut-Sontag-Preis des Deutschen Bibliotheksverbandes e.B. (dbv) ausgezeichnet und war von 2011 bis 2014 gewähltes Mitglied des Deutschen Presserates. Neben seiner eigenen journalistischen Tä-

tigkeit ist er Lehrbeauftragter diverser deutscher und ausländischer Journalistenschulen und ist Mitglied der Jury zur Vergabe des Alternativen Medienpreises. Zusätzlich betreibt er sein eigenes Medienbüro mit Sitz in Stuttgart, in welchem Hörbücher, aufwändige Features und Hörspiele produziert werden.

Thematisch ist der Beschwerdeführer zu 2 ein anerkannter Experte für Themen im Bereich Digitalisierung und Datensicherheit und deckt dabei investigativ immer wieder Missstände auf. So hat er beispielsweise 2017 aufgeklärt, dass ein technisch fehlerhafter Umgang mit polizeilichen und geheimdienstlichen Daten dazu führte, dass einer Reihe von Journalist*innen beim G20-Gipfel rechtswidrig die Akkreditierung verweigert wurde.

> Deutschlandfunk: Kann man den Sicherheitsdaten des Bundes noch trauen? Peter Welchering im Gespräch mit Manfred Kloiber, online abrufbar unter: https://www.deutschlandfunk.de/pflegebeduerftig-kann-man-den-sicherheitsdateien-des-bundes.684.de.html?dram:article_id=391769 (zuletzt abgerufen am 23. November 2018).

Gemeinsam mit Manfred Kloiber recherchierte er im Jahr 2015 über „Schlepperbanden“, die das Internet als Vertriebskanal und Organisationsmittel verwenden und bekamen dabei von einem Informanten, der aus einem Schleusernetzwerk aussteigen wollte, umfangreiche Daten über die Arbeit der Schleuserbande im Austausch für einen Kontakt zu einem Zeugenschutzprogramm eines anderen europäischen Landes. Wären die genutzten Informationskanäle nicht sicher gewesen, hätte dies das Leben das Informanten gefährden können.

> *Peter Welchering/Manfred Kloiber*, Informantenschutz, Ethische, rechtliche und technische Praxis in Journalismus und Organisationskommunikation, Springer Wiesbaden 2017, S. 105-109.

In einem Fall hat der Beschwerdeführer zu 3 zudem konkreten Anlass zu der Vermutung, dass seine elektronische Kommunikation von türkischen Behörden

mitgelesen wurde. Und zwar moderierte er im Sommer 2017 eine Diskussionsveranstaltung zum Thema Pressefreiheit, bei dem unter anderem Can Dündar, ein türkischer Journalist im deutschen Exil, als Podiumsgast geladen war.

> *Leonie Müller*, Can Dündar: „Wir haben nur unseren Willen zum Widerstand“, Kupferblau vom 19. Juli 2017, online abrufbar unter http://www.kupferblau.de/2017/06/19/can-duendar-wir-haben-nur-unseren-willen-zum-widerstand/ (zuletzt abgerufen am 29. November 2018).

Im Vorfeld der Veranstaltung suchten den Beschwerdeführer zu 3 zwei Herren auf, die sich als türkische Regierungsmitarbeiter vorstellten und nachdrücklich darauf hinwiesen, dass diese Veranstaltung unerwünscht sei. Dabei nannten sie Details der Absprachen mit Can Dündar, die darauf schließen lassen, dass der E-Mail-Verkehr mitgelesen wurde.

Bei seiner Arbeit und auch privat nutzt der Beschwerdeführer zu 3 mehrere Computer und Mobilfunkgeräte und kommuniziert und veröffentlicht über unterschiedliche Kanäle, darunter verschiedene Messenger, mehrere Social-Media-Dienste, E-Mail und SMS. Er hat sich u.a. aus Gründen des Informant*innenschutzes mit Möglichkeiten der datensicheren Kommunikation intensiv auseinandergesetzt und kommuniziert deshalb soweit möglich verschlüsselt. Zudem nutzt er Anonymisierungsplattformen wie Tor und anonymouse.org sowie, ebenfalls über Tor laufende sogenannte „tote digitale Briefkästen“, und um sein Webverhalten zu verschleiern. Bei Tor handelt es sich um ein Netzwerk vieler Rechner weltweit, welches seinen Nutzer*innen eine anonyme Möglichkeit der Internet-Nutzung bietet.

> *Peter Welchering/Manfred Kloiber*, Informantenschutz, Ethische, rechtliche und technische Praxis in Journalismus und Organisationskommunikation, Springer Wiesbaden 2017, S. 105-109. Immer mehr Zeitungen

nutzen solche tote Briefkästen, siehe bspw. die taz, online abrufbar unter https://informant.taz.de/ (zuletzt abgerufen am 29. November 2018).

4. Beschwerdeführer zu 4

Der Beschwerdeführer ist ein anerkannter, investigativer Journalist. Er schreibt als freier Journalist vor allem für Print- und Onlinemedien, und zwar u.a. für die DPA, Spiegel Online, den Stern, die taz, den freitag, ZEIT Online oder auch US-Magazine wie STATnews oder Science. Zudem ist er Mitgründer des unabhängigen Online-Magazins MedWatch, welches 2018 den Medien #Netzwende Award gewann. Der besondere Schwerpunkt seiner Arbeit liegt im Bereich medizinische Wissenschaft, er veröffentlicht aber immer wieder auch zu anderen Themen. Seit er im Rahmen eines Austauschprogramm der Robert-Bosch-Stiftung im Jahr 2015 in China war, schreibt er insbesondere zu diversen Themen mit Bezug zu diesem Land.

Insbesondere bei Recherchen in China muss er befürchten, dass auch verschlüsselte Kommunikation überwacht wird, entweder durch Eingriff in sein eigenes oder das IT-System seiner jeweiligen Informant*innen. Im Jahr 2017 hat er mit einer journalistischen Kollegin ein einstündiges Radiofeature zur Menschenrechtslage und der (fehlenden) Kunstfreiheit in China für den Bayerischen Rundfunk erstellt, in welchem es u.a. um verfolgte Künstler*innen in China ging. Die Informant*innen äußerten dabei explizit die Sorge, dass ihre Kommunikation mit den deutschen Partner*innen überwacht würde.

Auch der chinesische Staat nutzt für Überwachungsmaßnahmen 0-day-Schwachstellen aus.

Siehe bspw. *Tom Fox Brewster*, China linked to cyber attacks on Taiwan exploiting Windows vulnerability, The Guardian vom 23. Oktober 2014, online abrufbar unter https://www.theguardian.com/technology/2014/oct/23/china-cyber-attacks-taiwan-windows-microsoft (zuletzt abgerufen am 3. Dezember 2018). Siehe auch *Glyn Moody*, China Actively Collecting Zero-Days For Use By Its Intelligence Agencies -- Just Like The West, TechDirt vom 24. September 2018, online abrufbar unter https://www.techdirt.com/articles/20180921/09121740688/china-actively-collecting-zero-days-use-intelligence-agencies-just-like-west.shtml (zuletzt abgerufen am 4. Dezember 2018).

Einem Bericht zufolge werden entdeckte Schwachstellen sogar vermutlich zunächst auf ihre Nützlichkeit für Sicherheitsbehörden überprüft, bevor sie in der Chinese National Vulnerability Database veröffentlicht werden. Die Autor*innen der Studie gehen davon aus, dass diese Sicherheitslücken durch den Geheimdienst ausgenutzt werden.

Siehe *Priscilla Moriuchi/Bill Ladd,* China Altered Public Vulnerability Data to Conceal MSS Influence, Cyber Threat Analysis 2018, online abrufbar unter https://go.recordedfuture.com/hubfs/reports/cta-2018-0309.pdf (zuletzt abgerufen am 3. Dezember 2018).

Der Beschwerdeführer zu 4 nutzt für seine Arbeit mehrere Computer und ein Smartphone. Er verschlüsselt teilweise E-Mails, kommuniziere aber hauptsächlich über verschlüsselte Messenger-Dienste wie Signal oder Threema.

5. Beschwerdeführer zu 5

Der Beschwerdeführer zu 5 trägt die Rechtsform des eingetragenen Vereins, wurde 2008 gegründet und hat aktuell etwa 40 Mitglieder. Er verfolgt den Zweck, ein Forum für seine Mitglieder zu bieten, um sich für einen kreativen und verantwortungsvollen Umgang mit Technik und dem Internet einsetzen und Datenschutz und Bürgerrechte zu stärken.

Als Teil dieses Engagements betreibt der Beschwerdeführer zu 5 seit vier Jahren einen Tor-Knoten. Die so weltweit zum Tor-Netzwerk zusammen geschlossenen Rechner bieten den Nutzer*innen kostenfrei eine anonyme Möglichkeit der Internet-Nutzung an. Diese Anonymisierung des Datenverkehrs bietet Schutz vor Überwachung. Das Tor-Netzwerk, zu dem der Beschwerdeführer zu 5 beiträgt, wird deshalb auch von Menschen und Institutionen mit erhöhtem Schutzbedürfnis genutzt, insbesondere Journalist*innen, Aktivist*innen, Dissident*innen sowie staatlichen Stellen. Das Tor-Netzwerk wird weltweit von ca. 2 Millionen Nutzer*innen verwendet. Unter anderen nutzen immer mehr Tageszeitungen tote, anonyme Briefkästen über Tor.

> Siehe hierfür die Statistik, online abrufbar unter https://metrics.torproject.org/userstats-relay-country.html (zuletzt abgerufen am 29. November 2018). Für ein Beispiel für einen toten Briefkasten siehe die Homepage Tageszeitung die taz, https://www.taz.de/!p4858/ (zuletzt abgerufen am 29. November 2018).

Der Tor-Knoten läuft in einem Rechenzentrum in Rumänien auf der eigenen Hardware des Beschwerdeführers zu 5. Das Tor-Netzwerk besteht aus vielen untereinander verbunden Knoten weltweit, um so die Wahrscheinlichkeit eines Ausfalls des Netzwerks beispielsweise durch einen Hackangriff über Schwachstellen in der Soft- und Hardware zu minimieren. Erst, wenn etliche dieser Server ausfallen, ist die Anonymisierung des Datenverkehrs gefährdet. Um die Wahrscheinlichkeit dafür zu senken, dass ein einzelner Angriff über die IT-Schwachstelle eines Betriebssystems zu viele Server gleichzeitig beschädigen kann, verwenden die Betreiber*innen auf den Servern verschiedene solcher Systeme. Der Beschwerdeführer zu 5 selbst verwendet zudem ein zusätzlich abgesichertes Betriebssystem, um den Schutz seiner Infrastruktur weiter zu erhöhen.

6. Beschwerdeführerin zu 6

Die Beschwerdeführerin zu 6 ist eine Einkaufsgenossenschaft von Internet-Service-Providern mit Sitz in Stuttgart und bietet als solche ihren Mitgliedern sowie zum Teil externen Kund*innen Dienstleistungen an. Schwerpunktmäßig sind das Carrier-Vorleistungen für die Schaltung von DSL-Leitungen und das Anlegen von Internetdomains. Die IT-Systeme, die für diese Arbeit notwendig sind, werden von ihr dabei kontinuierlich gewartet, aktualisiert und repariert, um die IT-Sicherheit für sich und ihre Kund*innen zu gewährleisten und von Herstellern erkannte Sicherheitslücken durch Updates zu schließen. Als Infrastruktur-Dienstleisterin bedeutet ein erfolgreicher Hackerangriff auf ihre Systeme, dass durch eine Hintertür auch der Datenverkehr einer Vielzahl von Kund*innen zugleich abgegriffen werden kann.

7. Beschwerdeführerin zu 7

Die Beschwerdeführerin zu 7 ist eine als Gesellschaft bürgerlichen Rechts organisiertes, in Freiburg ansässiges Handelsgeschäft für ökologisch nachhaltig und fair produzierte Mode. Das von zwei geschäftsführenden Gesellschafter betriebene Handelsgeschäft umfasst neben einem Ladengeschäft im Zentrum Freiburgs auch einen Webshop für den Online-Versand.

(…)

C. Zulässigkeit

Die Verfassungsbeschwerde ist zulässig.

I. Frist

Die Jahresfrist des § 93 Abs. 3 BVerfGG ist gewahrt. Die Verfassungsbeschwerde richtet sich gegen Regelungen, die Artikel 1 des Gesetzes zur Änderung des Polizeigesetzes vom 28. November 2017 (GBl. S. 624) eingeführt hat und die das Polizeigesetz Baden-Württemberg (PolG BW) vorher nicht kannte. Die angegriffenen Eingriffsermächtigungen sind gemäß Artikel 4 dieses Gesetzes am Tag nach der Verkündung und damit am 8. Dezember 2017 in Kraft getreten.

II. Beschwerdefähigkeit

Die Beschwerdeführer*innen sind auch beschwerdefähig im Sinne des § 90 Abs. 1 S. 1 BVerfGG. Beschwerdefähig ist demzufolge „jedermann“, soweit er fähig ist, Träger von Grundrechten zu sein. Die prozessuale Beschwerdefähigkeit knüpft dabei an die materielle Grundrechtsfähigkeit an.

> BVerfGE 115, 205 <227>.

Grundrechtsfähig sind insbesondere auch die Beschwerdeführer*innen zu 5 bis 7, bei denen es sich nicht um natürliche Personen handelt. Die Beschwerdeführerinnen zu 5 bis 7 rügen eine Verletzung des Grundrechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (dazu unter 1). Fähig, Träger*innen dieses geltend gemachten Grundrechts zu sein, sind sowohl die Beschwerdeführer*innen zu 5 und 6 als juristische Personen (dazu unter 2), als auch die Beschwerdeführerin zu 7 als Gesellschaft bürgerlichen Rechts (dazu unter 3).

1. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Die Vertraulichkeit und Integrität informationstechnischer Systeme, auf welche die Beschwerdeführer*innen in besonderem Maße angewiesen sind, ist grundrechtlich geschützt. Dieses Grundrecht der einzelnen Person leitet sich nach der Rechtsprechung des Bundesverfassungsgerichts aus dem Allgemeinen Persönlichkeitsrecht ab (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

Dazu grundlegend BVerfGE 120, 274 <302 ff.>.

Geschützt von diesem Grundrecht ist zunächst das Interesse der Nutzer*innen, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.

BVerfGE 120, 274 <314>.

2. Anwendbarkeit auf die Beschwerdeführer*innen zu 5 und 6

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von informationstechnischen Systemen steht, soweit es auf Art. 2 Abs. 1 GG gestützt ist, auch den Beschwerdeführer*innen zu 5 und 6 als inländische juristische Personen zu. Denn es ist seinem Wesen nach auch auf sie anwendbar (Art. 19

Abs. 3 GG). Damit sind auch die Beschwerdeführer*innen zu 5 und 6 grundrechts- und beschwerdefähig.

Es hängt von Schutzgehalt und Eigenart von Grundrechten ab, ob sie auch auf eine inländische juristische Person anwendbar sind.

> Siehe dazu BVerfGE 95, 220 <242>; BVerfGE 106, 28 <42>. Ausführlich und m.w.N. siehe *Remmert*, in: Maunz/Dürig, GG, 84. EL Aug. 2018, Art. 19 Abs. 3, Rn. 100.

Zwar leitet sich das IT-Grundrecht aus dem Allgemeinen Persönlichkeitsrecht ab und hat damit ebenfalls eine normative Grundlage im Prinzip der Menschenwürde (Art. 1 Abs. 1 GG). Die Gewährleistungen der Menschenwürde sind jedoch, das ist unstreitig, nur anwendbar, soweit ein Grundrecht die psychische oder physische Existenz eines Menschen voraussetzt oder an andere Merkmale und Qualitäten anknüpft, die ein Menschsein voraussetzen.

> Siehe dazu etwa BVerfGE 95, 220 <242>; 118, 168 <203>.

In Fällen, in welchen die spezifische, grundrechtlich geschützte Freiheitsausübung jedoch keinen derartigen Bezug zur Menschenwürde aufweist, ist der Schutz des Allgemeinen Persönlichkeitsrechts – und gleichermaßen auch des IT-Grundrechts – auf juristische Personen übertragbar. Denn einzelne Ausprägungen des Allgemeinen Persönlichkeitsrechts können auch korporativ betätigt werden. So hat das Bundesverfassungsgericht festgestellt, dass das Recht auf informationelle Selbstbestimmung, ebenfalls eine Ausprägung des allgemeinen Persönlichkeitsrechts, auch auf juristische Personen anwendbar ist. Das hat es damit begründet, dass juristische Personen hinsichtlich informationeller Maßnahmen des Staates ein Schutzbedürfnis haben, welches dem natürlicher Personen entspräche.

BVerfGE 118, 168 <203>.

Unterschiede können sich bei den konkreten Gewährleistungen des Grundrechts ergeben. Denn eine juristische Person, anders als eine natürliche, hat in der Regel einen durch eine bestimmte Zwecksetzung begrenzten Tätigkeitskreis.

BVerfGE 118, 168 <203>.

Die Anwendbarkeit des IT-Grundrechts auf juristische Personen ist bislang noch nicht entschieden worden. Da es sich ebenfalls um eine Ausprägung des Allgemeinen Persönlichkeitsrechts handelt, lassen sich die bisher etablierten Grundsätze aber übertragen. Soweit sich das IT-Grundrechts auch auf Art. 2 Abs. 1 GG stützt, kann auch eine juristische Person Trägerin dieses Grundrechts sein. Auch für juristische Personen besteht ein besonderes Schutzbedürfnis auf Gewährleistung der Vertraulichkeit von IT-Systemen. Die dort gespeicherten Daten lassen, sollte eine unbefugte Person Zugriff haben, weitreichende Rückschlüsse über die Arbeitsweise, Umsätze und Strategien der juristischen Person zu. Die Gefahr eines solchen Zugriffs kann auch für juristische Personen in der Ausübung ihrer grundrechtlichen Freiheiten einschüchternd wirken. Das besondere Schutzbedürfnis, welchem das IT-Grundrecht gerecht wird, knüpft damit nicht an eine Qualität an, die nur Menschen eigen ist.

Neben der eigenen Schutzbedürftigkeit weist eine juristische Person zudem ein personales Substrat auf und dient immer auch der Grundrechtsentfaltung der in ihr zusammengeschlossenen Personen.

Die Lehre vom personalen Substrat ist stetige Rechtsprechung des Bundesverfassungsgerichts. Siehe dazu BVerfGE 21, 362 <369 f.>; BVerfGE 61, 82 <101> und BVerfGE 143, 246 <313>.

Der Schutz der Rechte einer juristischen Person dient damit auch den Grundrechte der Menschen, die sich dem Dienst der Firma bedienen und die ihre Rechte an den eigenen Daten nicht effektiv schützen können, wenn diese in der Sphäre der Firma verarbeitet werden.

3. Anwendbarkeit auf die Beschwerdeführerin zu 7

Aus gleichen Gründen ist das IT-Grundrecht auch auf die Beschwerdeführerin zu 7 als Gesellschaft bürgerlichen Rechts anwendbar (Art. 19 Abs. 3 GG). Sie ist damit ebenfalls grundrechts- und beschwerdefähig.

Bei einer Gesellschaft bürgerlichen Rechts handelt es sich nicht um eine juristische Person, sondern um eine Personengesellschaft. Bei dieser schließen sich mehrere Personen für einen gemeinsamen Zweck durch einen Gesellschaftsvertrag zusammen (§§ 705 ff. BGB). Die Gesellschaft bürgerlichen Rechts kann dennoch, das ist inzwischen anerkannt, eigenständige Trägerin von Rechten und Pflichten sein. Entsprechend Art. 19 Abs. 3 GG gelten auch für sie Grundrechte, soweit sie ihrem Wesen nach auf sie anwendbar sind.

Die Beschwerdefähigkeit gem. § 90 Abs. 1 S. 1 GG knüpft an die materielle Grundrechtsfähigkeit. Die Grundrechtsfähigkeit auch der Gesellschaft bürgerlichen Rechts hat das Bundesverfassungsgericht bereits festgestellt. Seine Entscheidung erkannte die Anwendbarkeit der Eigentumsgarantie (Art. 14 Abs. 1 GG) und der Verfahrensgrundrechten (Art. 101 Abs. 1 S. 2 und Art. 102 Abs. 1 GG) und bezog sich in der Begründung auf die insoweit anerkannten einfachrechtlichen Rechte und Pflichten einer Gesellschaft bürgerlichen Rechts.

> BVerfG, Urteil vom 02.09.2002, 1 BvR 1103/02, NJW 2002, 3533 <3533>.

Das die „Außen-Gesellschaft“, soweit sie durch Teilnahme am Rechtsverkehr eigene Rechte und Pflichten begründet, rechts- und parteifähig ist, ist seit einem Urteil des BGH aus dem Jahr 2002 endgültig anerkannt.

> BGH, Urteil vom 29.01.2001, II ZR 331/00, NJW 2001, 1056; siehe dazu auch BVerfG, Urteil vom 02.09.2002, 1 BvR 1103/02, NJW 2002, 3533.

Die für juristische Personen etablierten Kriterien (siehe oben unter C.II.2) können insofern auch auf eine Gesellschaft bürgerlichen Rechts übertragen werden. Soweit es sich auf Art. 2 Abs. 1 GG stützt, ist das IT-Grundrechts seines Wesens nach gleichermaßen auf sie anwendbar. Denn auch eine Gesellschaft bürgerlichen Rechts kann einfachrechtlich zur Gewährleistung der Vertraulichkeit von Daten verpflichtet sein, etwa als sekundäre Vertragspflicht eines Versandhandel hinsichtlich der bei der Kaufabwicklung angegebenen Daten seiner Kund*innen. Soweit eine Gesellschaft bürgerlichen Rechts für die Vertraulichkeit von Daten verantwortlich ist und für ihr Geschäft damit auch darauf angewiesen ist, das gewährleisten zu können, muss sie dafür auch grundrechtlichen Schutz beanspruchen können. Nur so kann zudem ein effektiver Grundrechtsschutz derjenigen gewährleistet werden, die ihre Daten in die Sphäre der Gesellschaft geben und für ihren Schutz damit auf diese angewiesen sind.

III. Beschwerdebefugnis

Die Beschwerdeführer*innen zu 1 bis 7 sind im Sinne von § 90 Abs. 1 BVerfGG beschwerdebefugt, weil eine Verletzung ihrer Grundrechte durch die angegriffene Regelung in § 23b Abs. 2 PolG BW zumindest möglich ist und diese Regelung sie auch selbst, gegenwärtig und unmittelbar betreffen.

1. Möglichkeit der Verletzung des IT-Grundrechts

§ 23b Abs. 2 PolG BW verletzt die Beschwerdeführer*innen zu 1 bis 7 in ihrem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG). Die Beschwerdeführer sind in herausgehobener Weise auf die Vertraulichkeit ihrer IT-Systeme angewiesen, dies jeweils auch zum Schutz der Rechte anderer Menschen. Die mögliche Verletzung ihres Rechts auf Gewährleistung dieser Vertraulichkeit liegt darin, dass das Land Baden-Württemberg durch die Einführung der angegriffenen Rechtsgrundlagen in § 23b Abs. 2 PolG BW ohne eine flankierende Regelungen des Umgangs mit IT-Schwachstellen einen Anreiz dafür setzt, dass staatliche Behörden die IT-Sicherheit der Beschwerdeführer*innen zusätzlich gefährden.

Denn für Gefahrenabwehrbehörden in Baden-Württemberg ist es aufgrund dieser Regelung zukünftig von Vorteil, IT-Schwachstellen geheim zu halten, um sie somit möglichst lange für Quellen-TKÜ ausnutzen zu können, statt sie den Herstellern zu melden und ihr Beheben zu ermöglichen (dazu unter a). Der Grundrechtschutz der Gewährleistung der Vertraulichkeit von IT-Systemen beinhaltet dem hingegen die staatliche Pflicht, sich für IT-Sicherheit einzusetzen und damit schützend vor dieses Recht zu stellen (dazu unter b). Aufgabe des Staates ist es insofern, sicherzustellen, dass staatliche Stellen auf die Behebung von Schwachstellen in der IT-Sicherheit hinwirken (dazu unter c). Aufgrund ihrer jeweiligen beruflichen und privaten Tätigkeit sind die Beschwerdeführer zu 1 bis 4 in besonderem Maße darauf angewiesen, dass die Vertraulichkeit ihrer IT-Systeme gewährleistet ist und Sicherheitslücken behoben werden, und deshalb zumindest möglicherweise betroffen (dazu unter d). Das gilt gleichermaßen für Beschwerdeführer*innen zu 5 bis 7, die keine natürliche Personen sind (dazu unter e).

a) Herausgehobene Rolle von Schwachstellen-Exploits bei der Umsetzung von Quellen-TKÜ

Dabei ist auf die herausgehobene Rolle hinzuweisen, welche gerade das Ausnutzen von Schwachstellen bei der Umsetzung von Quellen-TKÜ durch die Polizei Baden-Württemberg spielt bzw. spielen wird. Diese Form des Eindringens in ein IT-System hat nämlich gegenüber den Alternativen deutliche, praktische Vorteile, da weder ein räumlicher Zugriff noch ein weiteres Fehlverhalten eines*r Nutzer*in notwendig ist. Gerade wegen dieses strategischen Vorteils werden solche Schwachstellen auf dem Schwarzmarkt hohe Summen gehandelt.

> Vgl. dazu *Kai Biermann*, Außenministerium will Internet sicherer machen, BND nicht, die ZEIT vom 9. Oktober 2017, online abrufbar unter: https://www.zeit.de/digital/datenschutz/2017-10/it-sicherheit-bnd-zero-day-aussenministerium (zuletzt abgerufen am 4. Dezember 2018).

Auf Bundesebene gab der Abteilungsleiter für Cyber- und IT-Sicherheit im Bundesministerium des Inneren und für Bauen und Heimat, Andreas Könen, zu, dass der Entwicklungs- und Beschaffungsprozess für Trojaner, welche gerade Schwachstellen ausnutzen, in Gang gesetzt wurde.

> Es handele sich derzeit, so seine Aussage aus dem Juni 2018, um höchstens 5 Prozent des Zugriffs. *Detlef Borchers*, Cyber-Sicherheitspolitik: Fünf Prozent Zero-Day-Lücken für staatliche Überwachung von Kriminellen, Heise-Online vom 6. Juni 2018, online abrufbar unter: https://www.heise.de/newsticker/meldung/Cyber-Sicherheitspolitik-Fuenf-Prozent-Zero-Day-Luecken-fuer-staatliche-Ueberwachung-von-Kriminellen-4072578.html (zuletzt abgerufen am 5. Dezember 2018).

Die vom Bundeskriminalamt entwickelten und angekauften Trojaner setzen denn ebenfalls, soweit bekannt, vollständig oder überwiegend auf das Ausnutzen von Sicherheitslücken.

> Für eine Liste der verfügbaren Trojaner siehe *Andre Meister*, Geheime Dokumente: Das Bundeskriminalamt kann jetzt drei Staatstrojaner einsetzen, Netzpolitik.org vom 26. Juni 2018, online abrufbar unter:

https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminal-amt-kann-jetzt-drei-staatstrojaner-einsetzen/ (zuletzt abgerufen am 4. Dezember 2018).

Es ist deshalb mit hoher Wahrscheinlichkeit davon auszugehen, dass auch die Polizeibehörden Baden-Württemberg Quellen-TKÜ gerade unter Ausnutzen von IT-Sicherheitslücken durchführen werden.

b) Schutzdimension des IT-Grundrechts

Neben der Abwehrdimension leiten sich aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 auch grundrechtliche Schutzpflichten für die Gewährleistung der Integrität und Vertraulichkeit von informationstechnischen Systemen ab.

Vgl. allgemein zu Schutzpflichten bzgl. des Allgemeinen Persönlichkeitsrechts *Di Fabio*, in: Maunz/Dürig, GG, Stand: 81. EL Sep. 2017, Art. 2 Rn. 135 f.

Das Grundrecht verbürgt nämlich auch den staatlichen Auftrag zur **Gewährleistung** der Vertraulichkeit und Integrität informationstechnischer Systeme. Diesen Auftrag erfüllt der Staat, indem er den Einzelnen auch vor Angriffen Dritter auf seine IT-Systeme schützt, in welcher konkreten Form auch immer: Die Beschwerdeführer verkennen nicht, dass dem Gesetzgeber im Bereich der grundrechtlichen Schutzpflichten traditionell ein weiter Gestaltungsspielraum zugebilligt wird. Dieser wird jedoch dann verlassen, wenn das Land Baden-Württemberg seiner Schutzpflicht überhaupt nicht nachkommt oder sogar, wie vorliegend, gegensätzliche Anreize setzt.

Die Vernachlässigung einer solchen grundrechtlichen Schutzpflicht kann von den Betroffenen mit der Verfassungsbeschwerde geltend gemacht werden.

BVerfGE 77, 170 <214>; 77, 381 <402 f.>; 79, 174 <201 f.>; 125, 39 <78>.

c) Aufgabe des Landes Baden-Württemberg bei der Gewährleistung der IT-Sicherheit

Für den Schutz ihrer IT-Systeme hängen die Beschwerdeführer*innen in erster Linie von Maßnahmen der Hersteller der von ihnen verwendeten Programme und IT-Systeme ab. Diese haben ein eigenes Interesse daran – und sind je nach Vertragsverhältnis ggf. dazu verpflichtet –, ihnen bekanntwerdende Sicherheitslücken zu schließen, bevor etwa kriminelle oder auch (ausländische) staatliche Akteure sie ausnutzen. In diesem Wettlauf suchen die Hersteller zwar auch selbständig nach Sicherheitslücken und loben mitunter gar Preisgelder für gefundene Lücken aus (sog. Bug-Bounty-Programme). Gleichwohl sind sie darauf angewiesen, dass Dritte sie auf bestehende Sicherheitslücken hinweisen.

Der Staat spielt jedoch eine wesentliche Rolle in der Herstellung der IT-Sicherheit. Staatliche Stellen können Kenntnis von Sicherheitslücken noch vor den Herstellern der betroffenen Programme und IT-Systeme erhalten, beispielsweise über Meldungen von Firmen oder Behörden, die von Angriffen auf ihre IT-Systeme betroffen waren. Das Land Baden-Württemberg hat genau aus diesem Grund die Cyberwehr ins Leben gerufen: Durch diese Beratungsstelle für kleine und mittlere Unternehmen, die von Hackerangriffen betroffen sind, können Informationen zu solchen Vorfällen sofort an Sicherheitsbehörden weitergeleitet werden.

Siehe hierzu die Mitteilung der Landesregierung für den Start des Pilotprojekts vom 19. September 2017, online abrufbar unter https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/landesregierung-initiiert-cyberwehr-baden-wuerttemberg/ (zuletzt abgerufen am 27. November 2018).

Die Möglichkeit zu Maßnahmen nach § 23b Abs. 2 i.V.m. Abs. 1 PolG BW begünstigen indes einen Umgang mit solchen Sicherheitslücken, der sich auf die Beschwerdeführer*innen in ganz besonderem Maße, abgeschwächt aber auch auf die restliche Bevölkerung fatal auswirkt. Denn durch die Erlaubnis, IT-Sicherheitslücken für Angriffe auf Zielpersonen in der Gefahrenabwehr zu nutzen, schafft § 23b Abs. 2 PolG BW einen starken Anreiz für die Polizei und andere staatliche Stellen, Sicherheitslücken gerade nicht den Herstellern zu melden und dadurch zu ihrer Schließung beizutragen. Denn Sicherheitslücken sind im Ankauf teuer und bieten im Zugriff die oben genannten praktischen Vorteile.

> Siehe wiederum *Kai Biermann*, Außenministerium will Internet sicherer machen, BND nicht, die ZEIT vom 9. Oktober 2017, online abrufbar unter: https://www.zeit.de/digital/datenschutz/2017-10/it-sicherheit-bnd-zero-day-aussenministerium (zuletzt abgerufen am 4. Dezember 2018).

Damit legen es die angegriffenen Normen es – jedenfalls im Zusammenspiel mit dem staatlichen Unterlassen, klare Regeln für das Melden von Sicherheitslücken aufzustellen – den Polizeibehörden Baden-Württembergs geradezu nahe, möglichst umfangreich staatliche Infiltrationsmöglichkeiten zu sammeln und geheimzuhalten, die sich für Maßnahmen nach § 23b Abs. 2 i.V.m. Abs. 2 PolG BW nutzen lassen.

Sachgerecht und naheliegend wäre deshalb etwa eine umfassende Verpflichtung aller staatlicher Stellen, insbesondere aber der mit der Durchführung von Maßnahmen nach § 23b Abs. 2 i.V.m. Abs. 1 PolG BW betrauten Stellen, ihnen bekannte, dem Hersteller aber noch unbekannte Sicherheitslücken diesem zu melden, damit für Abhilfe gesorgt werden kann. Eine solche Pflicht besteht indes nicht. Als absolute Mindestanforderung hat das Land Baden-Württemberg aber im Lichte seines Schutzauftrags davon abzusehen, eine ohnehin prekäre

IT-Sicherheitslage noch zu verschärfen, indem er durch die gesetzliche Neuregelung der § 23 Abs. 2 i.V.m. Abs. 1 PolG BW massive Anreize zum Horten und Geheimhalten von Sicherheitslücken schafft.

> Eine staatliche Pflicht zum Schutz der IT-Systeme von Privaten bejahen auch *Gersdorf*, in: BeckOK Informations- und Medienrecht, Stand: 1.05.2017, Art. 2 Rn. 29; *Roßnagel/Schnabel*, NJW 2008, 3534 (3535); *Becker*, NVwZ 2015, 1335 (1339 f.) *Sachs/Krings*, JuS 2008, 481 (486). Für eine ausführliche Herleitung der Schutz- und Förderpflicht zur Gewährleistung der IT-Sicherheit *Heckmann*, in: FS Käfer, 2009, S. 129 (133 ff.). Zu § 23b PolG BW siehe auch die Stellungnahme des Anwaltsverbands Baden-Württemberg im DAV e.V. zum Gesetzesentwurf vom 08.08.2017, S. 13-16, online abrufbar unter http://www.av-bw.de/fileadmin/daten/interessenvertretung/Stellungnahmen/Polizeigesetz/08_08_2017_AVBW_StN_PolG_Novelle_Spaehsoftware.pdf (zuletzt abgerufen am 27. November 2018).

d) Besonderes Schutzbedürfnis der Beschwerdeführer zu 1 bis 4

Die Beschwerdeführer zu 1 bis 4 sind darauf angewiesen, dass – infolge der Fehlbarkeit menschlichen Handelns als solche unvermeidbare – Sicherheitslücken ihrer IT-Systeme schnellstmöglich geschlossen werden. Denn je länger eine Sicherheitslücke besteht, desto höher die Wahrscheinlichkeit, dass sie durch interessierte Kreise gefunden und für Angriffe auf die IT-Systeme der Beschwerdeführer missbraucht wird.

Die Beschwerdeführer zu 1 und 2 bedürfen eines besonderen Schutzniveaus von IT-Systemen und IT-gestützter Kommunikation, um als Rechtsanwälte mit einem bestimmten Kreis von Mandant*innen die Vertraulichkeit der geschützten Kommunikation sicherstellen zu können. Dabei müssen sie sowohl auf ein hohes Schutzniveau der eigenen IT-Systeme als auch auf ein solches Schutzniveau

der IT-Systeme ihrer Mandanten vertrauen können. Denn nur, wenn die jeweiligen IT-Systeme und die IT-gestützte Kommunikation sicher vor fremdem Zugriff sind, können sie sicherstellen, dass die in ihrem IT-System gespeicherten, die Mandatsarbeit betreffenden Daten vor fremdem Zugriff geschützt sind und andererseits die Kommunikation mit ihren Mandant*innen vertraulich ist. Und nur bei hinreichend gewährleisteter IT-Sicherheit können sie ihren Mandant*innen auch ein Vertrauen auf die Vertraulichkeit der Mandatsarbeit vermitteln. Gerade Schwachstellen, über welchen ein Zugriff durch Dritte nicht verhindert und kaum bemerkt werden kann, bieten dafür ein Risiko.

Die Vertraulichkeit der Kommunikation ist für jede*n Anwält*in von großer Bedeutung. Bei den Beschwerdeführern zu 1 und 2 kommt jedoch darüber hinaus hinzu, dass ein Teil ihrer Mandant*innen und damit auch sie selbst von einer deutlich erhöhten Wahrscheinlichkeit ausgehen müssen, dass ihre IT-Systeme angegriffen werden. Unter ihren Mandant*innen gehören einige politischen Kreisen an, in welchen immer wieder Individuen von ausländischen staatlichen Stellen oder politischen Organisationen überwacht werden. Dazu zählen sowohl Sympathisant*innen der PKK als auch Aktivist*innen aus der antifaschistischen oder kommunistischen Szene. Andere Mandant*innen befürchten eine Überwachung ausländischer Geheimdienste aufgrund ihrer beruflichen Tätigkeit oder einer politischen Verfolgung im Heimatland. Aufgrund dieser Mandatsarbeit müssen die Beschwerdeführer ihren Mandant*innen ein besonderes Maß an Vertraulichkeit zusichern können, und müssen sie zudem selbst befürchten, Ziel von Angriffen auf ihre IT-Systeme zu werden. Zusätzlich haben die Beschwerdeführer zu 1 und 2 auch ein privates Interesse an Datensicherheit, da sie legitimierweise eine eigene Überwachung durch kriminelle oder ausländische staatliche Akteure nicht wünschen.

Die Beschwerdeführer zu 3 und 4 sind als investigativ arbeitende Journalisten ebenfalls in besonderem Maße auf einen hohen Schutz von IT-Systemen angewiesen, um ihre Quellen und auch sich selbst zu schützen. Informat*innen, beispielsweise Whistleblower, gehen ein hohes Risiko ein, wenn sie Informationen an eine*n Journalist*in weitergeben, um so bestehende Missstände aufzudecken. Um sie und auch sich selbst keiner Gefahr auszusetzen, sind die Beschwerdeführer zu 3 und 4 darauf angewiesen, dass organisierte Kriminalität, aber auch ausländische Sicherheitsbehörden nicht auf ihre IT-Systeme oder die IT-Systeme ihrer Informant*innen zugreifen können. Dafür ist es wichtig, dass die genutzten IT-Systeme vor fremdem Zugriff bestmöglich geschützt sind. Gerade das Schließen von Sicherheitslücken ist dafür wesentlich.

> *Peter Welchering/Manfred Kloiber*, Informantenschutz, Ethische, rechtliche und technische Praxis in Journalismus und Organisationskommunikation, Springer Wiesbaden 2017, S. V-VII, 105-116.

Zudem haben auch die Beschwerdeführer zu 4 und 5 ein legitimes, privates Interesse daran, nicht von ausländischen Diensten oder kriminellen Organisationen überwacht zu werden.

e) Besonderes Schutzbedürfnis der Beschwerdeführer*innen zu 5 bis 7

Eine Verletzung des Rechts der Beschwerdeführer*innen zu 5 bis 7 auf Gewährleistung der Vertraulichkeit und Integrität von IT-Systemen durch einen risikoträchtigen staatlichen Umgang mit unbekannten Sicherheitslücken ist aus gleichen Erwägungen zumindest möglich. Denn auch als juristische Personen bzw. Personengesellschaften können sie, wie bereits dargestellt, einen Gewährleitung ihrer IT-Sicherheit nach Art. 2 Abs. 1 GG grundrechtlich beanspruchen. Auch sind die Beschwerdeführer*innen in besonderem Maße auf einen Schutz ihrer IT-Systeme angewiesen.

Die Beschwerdeführerin zu 5 ist damit beauftragt, die IT-Systeme, die für ihre Dienstleistungen notwendig sind, zu aktualisieren und zu reparieren, um so ihre Sicherheit zu gewährleisten. Ein Trojaner, welcher in ihr IT-System eindringt, kann zum einen Daten über ihr Geschäftsmodell, Arbeitsweise und Strategien auslesen und damit weitreichende Einblicke in ihre Tätigkeit gewinnen. Zum anderen kann ein Angriff auf ihr IT-System und die von ihr geschaffene Infrastruktur aber auch einen erleichterten Zugriff auf die IT-Systeme ihrer Kund*innen ermöglichen und damit auf etliche weitere IT-Systeme durchschlagen. Im Fall der von ihr geschalteten Leitungen heißt das, das ein unbefugter Dritter Leitungen ändern, schalten oder auch Störtermine triggern und betrügerische Techniker zu einem Termin senden kann. Im Hinblick auf die von ihr eröffneten Domains könnten diese bei einem Zugriff verloren gehen, verändert werden oder auch E-Mails umgesteuert werden, ohne dass dies ohne Weiteres nachvollziehbar ist. Die Sicherheit ihres IT-Systems sowie des IT-Systems ihrer Kund*innen zu gewährleisten ist damit eine grundrechtlich geschützte Kerntätigkeit der Beschwerdeführerin zu 5.

Der Beschwerdeführer zu 6 ist kein Wirtschaftsunternehmen, sondern ist als Verein dem ideellen Ziel gewidmet, Datensicherheit zu fördern und informationstechnologische Systeme verantwortungsvoll zu nutzen. In dem von ihm betriebenen Tor-Relay ermöglicht er Menschen, die ein besonderes Schutzbedürfnis haben, eine besonders gesicherte Kommunikation. Dem Schutz dieser Menschen ist der Beschwerdeführer zu 6 entsprechend seiner Satzung und entsprechend dem besonderen Interesse seiner Mitglieder besonders verpflichtet und deshalb besonders darum bemüht, diese Infrastruktur gegenüber möglichen Angriffen sicher zu gestalten. Ein Eindringen in dieses geschützte System hätte tiefgreifende Konsequenzen für die Nutzer*innen des Tor-Relays. Die Sicherheit des Tor-Relays als IT-System ist deshalb für den Beschwerdeführer zu 6 ein zentrales Anliegen. Es entspricht damit sowohl einer eigenen Schutzbedürf-

tigkeit als auch, entsprechend der Lehre des personalen Substrats, der Grundrechtsverwirklichung seiner Mitglieder und der sein Tor nutzenden Personen, ihm den Schutz des Grundrechts auf Gewährleistung und Vertraulichkeit informationstechnischer Systeme zuzusprechen.

Die Beschwerdeführerin zu 7 trägt als Online-Versandhandel im Rahmen ihrer Geschäftstätigkeit die Verantwortung für die Vertraulichkeit der Daten ihrer Kund*innen, insbesondere Namen, Anschriften und Zahlungsdaten sowie Informationen zu Bestellungen. An dieser Verantwortung ändert sich nichts dadurch, dass sie im Innenverhältnis deren Verwaltung auf einen Dienstleister überträgt. Im Sinne eines effektiven Rechtschutzes muss sie hinsichtlich der von ihr zu verantwortenden Vertraulichkeit der Daten auch eigenen grundrechtlichen Schutz beanspruchen können. Das gilt weiter auch deshalb, weil die Gesellschaft bürgerlichen Rechts, gleich einer juristischen Person, der Grundrechtsverwirklichung der dahinterstehenden Menschen zu dienen bestimmt ist. Soweit ihre Kund*innen Daten in ihre Sphäre geben und für ihren Schutz damit auf die Beschwerdeführerin zu 7 angewiesen sind, muss die Vertraulichkeit dieser Daten auch innerhalb des IT-Systems der Beschwerdeführerin zu 7 einen grundrechtlichen Schutz beanspruchen können. Dafür ist sie aber, gleich einer natürlichen Person, auf die Sicherheit ihrer IT-Systeme angewiesen.

Die Gefahr wegen der Daten von Kund*innen Opfer eines Hackerangriffs zu werden ist dabei durchaus real. Ende November 2018 wurde dafür beispielhaft einer der größten Hackerskandale der Geschichte öffentlich. Bei Starwood, einer Tochter der Hotelkette Mariott, wurden durch einen erfolgreichen Angriff die Daten einer halben Milliarde Kund*innen entwendet.

> Vgl. hierzu Hacker stehlen Daten von 500.000.000 Hotelgästen, FAZ vom 30. November 2018, online abrufbar unter https://www.faz.net/aktuell/wirtschaft/diginomics/hacker-stehlen-daten-von-einer-halben-milliarde-hotelgaeste-15917777.html (zuletzt abgerufen am 5. Dezember

2018). Siehe auch *Martin Holland,* Marriott: Daten von 500 Millionen Hotelgästen abgegriffen, online abrufbar unter https://www.heise.de/security/meldung/Marriott-Daten-von-500-Millionen-Hotelgaesten-abgegriffen-4236576.html (zuletzt abgerufen am 5. Dezember 2018).

Die Gefahr solcher Angriffe beschränkt sich dabei keineswegs auf große Unternehmen, sondern betrifft insbesondere auch kleine und mittlere Unternehmen in Baden-Württemberg. Auf ebendiese Gefahr für mittelständische Unternehmen weist auch die Baden-Württembergische Landesregierung selbst hin.

Pressemitteilung vom 19. September 2017, Landesregierung initiiert „Cyber-Wehr Baden-Württemberg", online abrufbar unter https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/landesregierung-initiiert-cyberwehr-baden-wuerttemberg/ (zuletzt abgerufen am 5. Dezember 2018).

2. Betroffenheit hinsichtlich des IT-Grundrechts

Die Beschwerdeführer*innen sind sowohl unmittelbar, wie auch selbst und gegenwärtig von der angegriffenen Regelung betroffen (§ 90 Abs. 1 BVerfGG).

§ 23b Abs. 2 i.V.m. Abs. 1 PolG BW betrifft die Beschwerdeführer*innen zu 1 bis 7 unmittelbar in ihren Grundrechten aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG, weil es zu ihrer Beschwer keines weiteren gegen sie gerichteten Akts bedarf. Vielmehr folgt ihre Betroffenheit gerade aus der durch staatliche Stellen erhöhten Gefahr für ihre IT-Systeme, die daraus resultiert, dass die Polizei Baden-Württembergs wegen § 23b Abs. 2 PolG BW ihnen bekanntwerdende Sicherheitslücken unter Verletzung ihrer staatlichen Schutzpflicht gegenüber den Beschwerdeführer*innen nicht an die Hersteller der betroffenen Programme und IT-Systeme meldet.

Wäre für die Unmittelbarkeit der Grundrechtsverletzung demgegenüber daran anzuknüpfen, dass baden-württembergische Behörden eine bestimmte Schwachstelle geheim halten, um sie für Maßnahmen nach § 23b Abs. 2 i.V.m. Abs. 1 PolG BW auszunutzen und genau diese durch Dritte für einen Hackerangriff auf ein IT-System der Beschwerdeführer*innen ausgenutzt würde, dann wäre der gerichtliche Rechtschutz unmöglich, da die Beschwerdeführer*innen von diesen Tatsachen, insbesondere den konkreten den Behörden bekannten Schwachstellen, keine Kenntnis erlangen würden.

> Vergleiche hierzu im Fall des sogenannten „Großen Lauschangriffs“, BVerfGE 109, 279 <306>; 133, 277 <311 f.>.

Die Beschwerdeführer*innen sind auch selbst und gegenwärtig von dem Gesetz betroffen, weil sie IT-Systeme nutzen und auf ihre Integrität und Vertraulichkeit in besonderem Maße angewiesen sind. Hinsichtlich der Bedrohung durch Hackerangriffe speziell zu ihren Lasten sei auf die obigen Ausführungen zur besonderen Sensibilität ihrer Arbeit und politischen Tätigkeit verwiesen.

IV. Rechtsschutzbedürfnis

Gegen formelle Gesetze ist ein Rechtsweg nicht gegeben, weshalb § 90 Abs. 2 Satz 1 BVerfGG der Verfassungsbeschwerde nicht entgegensteht.

D. Begründetheit der Verfassungsbeschwerde

Die Ausgestaltung der Quellen-TKÜ in § 23b Abs. 2 PolG BW verletzt die Beschwerdeführer*innen zu 1 bis 7 in ihrem Grundrechten auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 2 Abs. 1 GG, weil das Land Baden-Württemberg die genannten Befugnisse nicht mit einem effektiven Schwachstellen-Management verbunden hat, welches insbesondere die Verwendung von Sicherheitslücken verhindert, die dem Hersteller des betreffenden Systems noch nicht bekannt sind (sog. Zero-Day-Exploits oder kurz: 0-days).

I. Maßstab

1. Das sog. IT-Grundrecht

Die Informationstechnik hatte für die Lebensgestaltung des Einzelnen schon zur Zeit der ersten Entscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung eine hohe Relevanz.

> BVerfGE 120, 274 ff.

Mit dieser Bedeutung gehen nach der Rechtsprechung des angerufenen Gerichts „besondere Persönlichkeitsgefährdungen“ und „ein grundrechtlich erhebliches Schutzbedürfnis“ einher.

> BVerfGE 120, 274 <306>.

Für dieses besondere Schutzbedürfnis entwickelte das angerufene Gericht ein besonderes Grundrecht, nämlich das **Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme** (im Folgenden auch: IT-Grundrecht). Der Schutzbereich dieses Grundrechts ist eröffnet,

wenn eine Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten, 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 erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden.

BVerfGE 120, 274 <314>.

Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme schützt zunächst das Interesse der Nutzer*innen, dass die von einem (vom Schutzbereich erfassten) informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden könnten; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen. Das Grundrecht schützt dabei insbesondere vor einem heimlichen Zugriff, durch den die auf dem System vorhandenen Daten ganz oder zu wesentlichen Teilen ausgespäht werden können.

BVerfGE 120, 274 <314>.

2. Anwendbarkeit auf inländische juristische Personen

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von informationstechnischen Systemen gilt, soweit es sich auf Art. 2 Abs. 1 GG stützt, auch für inländische juristische Personen. Denn es ist seinem Wesen nach auf

juristische Personen anwendbar (Art. 19 Abs. 3 GG). Damit können auch die Beschwerdeführer*innen zu 5 und 6 sich auf seinen Schutz berufen.

Ob Grundrechte auch auf inländische juristische Personen anwendbar sind, hängt von ihrem Schutzgehalt und Eigenart ab. Daran scheitert es nach der Rechtsprechung des Bundesverfassungsgerichts, wenn ein Grundrecht „an Eigenschaften, Äußerungsformen oder Beziehungen anknüpft, die nur natürlichen Personen wesenseigen sind."

> Siehe dazu BVerfGE 95, 220 <242>; BVerfGE 106, 28 <42>. Ausführlich und m.w.N. siehe Remmert, in: Maunz/Dürig, GG, 84. EL Aug. 2018, Art. 19 Abs. 3, Rn. 100.

Die Gewährleistungen der Menschenwürde sind deshalb unstreitig nur anwendbar, soweit ein Grundrecht die psychische oder physische Existenz eines Menschen voraussetzt oder an andere Merkmale und Qualitäten anknüpft, die ein Menschsein voraussetzen.

> Siehe dazu etwa BVerfGE 95, 220 <242>; 118, 168 <203>.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus dem Allgemeinen Persönlichkeitsrecht und damit grundsätzlich aus sowohl aus der Allgemeinen Handlungsfreiheit als auch der Menschenwürde ab. Für das IT-Grundrecht wurde die Frage der Anwendung auf juristische Personen soweit ersichtlich noch nicht ausdrücklich entschieden. Insofern können aber die an anderer Stelle für das allgemeine Persönlichkeitsrecht entwickelten Grundsätze übertragen werden.

Die Frage, ob das Allgemeine Persönlichkeitsrecht auf juristische Personen anwendbar ist, lässt sich nicht abstrakt beantworten. Vielmehr muss die spezifisch geltend gemachte Ausprägung dahingehend gewürdigt werden, ob sie auch kor-

porativ ausgeübt werden kann. Das ist dann der Fall, wenn das Grundrecht einem Schutzbedürfnis Rechnung trägt, welches nicht nur natürliche, sondern auch juristische Personen betrifft. Mit dieser Begründung hat das Bundesverfassungsgericht etwa festgestellt, dass auch juristische Personen ein Recht auf informationelle Selbstbestimmung haben, weil auch sie durch informationelle Maßnahmen des Staates in ihren grundrechtlichen Freiheiten spezifisch beeinträchtigt werden.

> BVerfGE 118, 168 <203>.

Es leitet dabei das Recht auf informationelle Selbstbestimmung dann nur aus Art. 2 Abs. 1 GG ab. Unterschiede können sich dementsprechend bei den konkreten Gewährleistungen des Grundrechts ergeben. Denn eine juristische Person, anders als eine natürliche, hat in der Regel einen durch eine bestimmte Zwecksetzung begrenzten Tätigkeitskreis.

> BVerfGE 118, 168 <203>.

Mit dieser Begründung und Maßgabe wird das Allgemeine Persönlichkeitsrecht in der zivilgerichtlichen Rechtsprechung und Literatur ganz überwiegend für auf inländische juristische Personen anwendbar erachtet.

> Siehe hierzu auch die zivilgerichtliche Rechtsprechung BGHZ 78, 24 <25>, m.w.N.; BGHZ 81, 75 <78>; BGH, Urteil vom 3. Juni 1986, NJW 1986, 2951 f.; BGH, Urteil vom 3. Juni 1975, JZ 1975, 637 ff. So auch *DiFabio*, in: Maunz/Dürig, GG, 84. EL Aug. 2018, Art. 2 Abs. 1, Rn. 224; Murswiek/Rixen, in: GG, 8. Auflage 2018, Art. 2 Rn. 76-78.

Diese Herangehensweise lässt sich auch auf das IT-Grundrecht als Ausprägung des Allgemeinen Persönlichkeitsrechts übertragen. Soweit sich das IT-Grundrecht auf Art. 2 Abs. 1 GG stützt, kann auch eine juristische Person Trägerin

des Grundrechts sein. Auch für juristische Personen besteht ein besonderes Schutzbedürfnis hinsichtlich des Schutzes ihrer IT-Systeme. Dies kann sich darauf gründen, dass innerhalb eines IT-Systems gespeicherte Daten weitreichende Rückschlüsse über die Arbeitsweise, Umsätze und Strategien der juristischen Person zulassen. Je nach Tätigkeit und Zweck der juristischen Person kann es sich aber auch gerade um eine IT-Infrastruktur handeln, deren Sicherheit neben der juristischen Person selbst noch zahlreiche weitere Nutzer*innen betrifft. Die Sicherheit dieses IT-Systems ist in diesen Fällen gewissermaßen die Kernaufgabe dieser juristischen Person.

Dabei liegt in der Natur der Sache, dass die spezifische Ausprägung des IT-Grundrechts, wenn es auf eine juristische Person angewendet wird, anders gelagert ist als dies in manchen Fällen natürlicher Personen der Fall sein mag. So liegt es nahe, dass in vielen Fällen die Erwägungen wirtschaftlicher Natur sind.

> So für das Allgemeine Persönlichkeitsrecht *DiFabio*, in: Maunz/Dürig, GG, 84. EL Aug. 2018, Art. 2 Abs. 1, Rn. 224.

Es kann es sich dabei aber auch um ideelle Zwecke handeln, wenn die juristische Person zu einem gemeinnützigen Zweck gegründet wurde. Dies gilt insbesondere, da eine juristische Person nach der stetigen Rechtsprechung des Bundesverfassungsgerichts ein personales Substrat aufweist und damit der Grundrechtsentfaltung der in ihr zusammengeschlossenen Personen dient.

> Die Lehre vom personalen Substrat ist stetige Rechtsprechung des Bundesverfassungsgerichts. Siehe dazu BVerfGE 21, 362 <369 f.>; BVerfGE 61, 82 <101> und BVerfGE 143, 246 <313>.

Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme knüpft damit an einem spezifischen Schutzbedürfnis

an, welches auch juristische Personen betrifft und welches nicht von den übrigen Grundrechten abgedeckt wird. Insbesondere wird dies nicht von der informationellen Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) erfasst.

3. Anwendbarkeit auf die Gesellschaft bürgerlichen Rechts

Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist, soweit es sich aus Art. 2 Abs. 1 GG ableitet, auch auf eine Gesellschaft bürgerlichen Rechts anwendbar. Zwar handelt es sich bei der Gesellschaft bürgerlichen Rechts nicht um eine juristische Person, sondern um eine Personengesellschaft, bei der sich mehrere Personen für einen gemeinsamen Zweck durch einen Gesellschaftsvertrag zusammenschließen (§§ 705 ff. BGB). Die Gesellschaft bürgerlichen Rechts kann dennoch, das ist inzwischen anerkannt, eigenständige Trägerin von Rechten und Pflichten sein. Entsprechend Art. 19 Abs. 3 GG gelten deshalb auch für sie Grundrechte, soweit sie ihrem Wesen nach auf sie anwendbar sind.

Dass die Gesellschaft bürgerlichen Rechts auch Trägerin von Grundrechten sein kann, hat das Bundesverfassungsgericht bereits festgestellt. In seiner Entscheidung argumentiere es dabei, dass ein grundrechtlicher Schutz dort notwendig sei, wo die Gesellschaft bürgerlichen Rechts Trägerin einfacher Rechte sei. So begründete es seine Entscheidung zur Eigentumsgarantie (Art. 14 Abs. 1 GG) damit, dass die Gesellschaft bürgerlichen Rechts als Inhaberin von Eigentumsrechten für diese Rechte auch grundrechtlichen Schutz beanspruchen könne. Auch die Verfahrensgrundrechten (Art. 101 Abs. 1 S. 2 und Art. 102 Abs. 1 GG) hat das Bundesverfassungsgericht in gleicher Entscheidung anerkannt und hierzu darauf verwiesen, dass die Parteifähigkeit der Gesellschaft bürgerlichen Rechts im Zivilprozessrecht anerkannt sei.

BVerfG, Urteil vom 02.09.2002, 1 BvR 1103/02, NJW 2002, 3533 <3533>.

Die einfachrechtliche Rechtsfähigkeit der „Außen-Gesellschaft“, soweit sie durch Teilnahme am Rechtsverkehr eigene Rechte und Pflichten begründet, ist inzwischen aber anerkannt.

BGH, Urteil vom 29.01.2001, II ZR 331/00, NJW 2001, 1056; siehe dazu auch BVerfG, Urteil vom 02.09.2002, 1 BvR 1103/02, NJW 2002, 3533.

Entsprechend diesen sowie den für juristische Personen hinsichtlich des Allgemeinen Persönlichkeitsrecht etablierten Kriterien (siehe oben unter D.I.2) kann auch eine Gesellschaft bürgerlichen Rechts Trägerin des IT-Grundrechts sein. Soweit es sich auf Art. 2 Abs. 1 GG stützt ist es nämlich seines Wesens nach auch auf sie anwendbar.

Denn zunächst kann die Gesellschaft bürgerlichen Rechts einfachrechtlich auch zum Schutz vertraulicher Daten verpflichtet sein. Soweit eine Gesellschaft bürgerlichen Rechts gegenüber Dritten verpflichtet ist, deren Daten vertraulich zu bewahren, muss ihr damit nach den Grundsätzen des Bundesverfassungsgerichts für einen effektiven Grundrechtschutz das Recht auf Gewährleistung ihrer IT-Systeme in Anspruch nehmen können. Und zudem entspricht das auch, vergleichbar einer juristischen Person, ihrem in der Grundrechtsentfaltung der hinter ihr stehenden Menschen.

4. Staatliche Schutzpflichten

Nach ständiger Rechtsprechung des Bundesverfassungsgerichts enthalten die grundrechtlichen Verbürgungen indes nicht lediglich subjektive Abwehrrechte des Einzelnen gegen die öffentliche Gewalt, sondern sind zugleich objektiv-

rechtliche Wertentscheidungen der Verfassung, die für alle Bereiche der Rechtsordnung gelten und Richtlinien für Gesetzgebung, Verwaltung und Rechtsprechung geben.

BVerfGE 7, 198 <205>; 35, 79 <114>; 39, 1 <41 f.>; 49, 89 <141 f.>.

Dies wird am deutlichsten in Art. 1 Abs. 1 Satz 2 GG ausgesprochen, wonach es Verpflichtung aller staatlichen Gewalt ist, die Würde des Menschen zu achten und zu schützen. Daraus können sich verfassungsrechtliche Schutzpflichten ergeben, die es gebieten, rechtliche Regelungen so auszugestalten, dass auch die Gefahr von Grundrechtsverletzungen eingedämmt bleibt.

BVerfGE 49, 89 <142>; 92, 26 <46>; 125, 39 <78>.

Ob, wann und mit welchem Inhalt eine solche Ausgestaltung von Verfassungs wegen geboten ist, hängt von der Art, der Nähe und dem Ausmaß möglicher Gefahren, der Art und dem Rang des verfassungsrechtlich geschützten Rechtsguts sowie von den schon vorhandenen Regelungen ab.

BVerfGE 49, 89 <142>.

Im Zusammenhang mit den Gefahren der friedlichen Nutzung der Kernenergie hat das Bundesverfassungsgericht ausgeführt, dass der Gesetzgeber zur Abschätzung künftiger Schäden durch die Errichtung oder den Betrieb einer Anlage oder durch ein technisches Verfahren weitgehend auf Schlüsse aus der Beobachtung vergangener tatsächlicher Geschehnisse auf die relative Häufigkeit des Eintritts und den gleichartigen Verlauf gleichartiger Geschehnisse in der Zukunft angewiesen ist. Fehlt eine hinreichende Erfahrungsgrundlage hierfür, muss er sich auf Schlüsse aus simulierten Verläufen beschränken. Der Gesetzgeber muss allerdings keine Regelungen schaffen, die mit absoluter Sicherheit Grundrechtsgefährdungen ausschließen.

BVerfGE 49, 89 <142>.

Das Bundesverfassungsgericht kann deswegen die Verletzung einer Schutzpflicht nur feststellen, wenn die öffentliche Gewalt Schutzvorkehrungen entweder überhaupt nicht getroffen hat oder die getroffenen Regelungen und Maßnahmen gänzlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder erheblich dahinter zurückbleiben.

BVerfGE 77, 17 <214 f.>; 88, 203 <251 ff.>; 92, 26 <46>; 125, 39 <78 f.>; 143, 313 <337 f.>.

Das angerufene Gericht hat bereits zu Art. 10 Abs. 1 GG erklärt, dass er nicht nur vor der Kenntnisnahme des Inhalts und der näheren Umstände der Telekommunikation durch den Staat schütze, sondern auch einen Auftrag an den Staat enthalte, Schutz auch insoweit vorzusehen, als private Dritte sich Zugriff auf die Kommunikation verschaffen.

BVerfGE 106, 28, <37>.

Auch zum Allgemeinen Persönlichkeitsrecht hat das Bundesverfassungsgericht eine Schutzpflicht des Staates anerkannt.

BVerfGE 63, 131 <142>; 73, 118 <201>; 96, 56 <64>; 100, 271 <284>; vgl. zu Schutzpflichten bzgl. des Allgemeinen Persönlichkeitsrechts auch *Di Fabio*, in: Maunz/Dürig, GG, Stand: 81. EL Sep. 2017, Art. 2 Rn. 135 f. (zur Pflicht zum Schutz der informationellen Selbstbestimmung: Rn. 189).

5. Staatliche Pflicht zum Schutz informationstechnischer Systeme vor Integritäts- und Vertraulichkeitsverletzungen

Dass das Bundesverfassungsgericht auch dem IT-Grundrecht eine objektivrechtliche Dimension zuerkennt, hat das Gericht bereits sprachlich durch den Auftrag zur *Gewährleistung* der Vertraulichkeit und Integrität informationstechnischer Systeme zum Ausdruck gebracht.

Hoffmann-Riem hat dies mit Bezug auf das IT-Grundrecht unmittelbar im Anschluss an die Entscheidung des angerufenen Gerichts wie folgt formuliert:

> „Vom grundrechtlichen Schutz umfasst ist die Abwehr (nicht gerechtfertigter) staatlicher Eingriffe. Es geht aber auch um die Gewährung von Schutz, sei es durch Erfüllung der in Grundrechten enthaltenen subjektiven Schutzansprüche und gegebenenfalls entsprechender Schutzpflichten, sei es in Ausgestaltung der objektiv-rechtlichen Vorgaben der Grundrechte. Schutzdimensionen außerhalb des rein abwehrrechtlichen Schutzes der Grundrechte treten umso eher in das Zentrum grundrechtlicher Garantien, je mehr die realen Voraussetzungen der Freiheitausübung der Bürger einerseits durch den Staat, andererseits aber auch durch Private oder im Zuge von Kooperationsakten zwischen Staat und Privaten geschaffen und erhalten werden müssen, aber gegebenenfalls auch von ihnen in Frage gestellt werden. Deshalb wird immer bedeutsamer, dass das BVerfG schon seit längerem vermehrt auf die objektiv-rechtliche Dimension des Grundrechtsschutzes zurückgegriffen hat. (...) Soweit es um die Aktivierung anderer, also auch der objektiv-rechtlichen Grundrechtsfunktionen geht, bedarf es (...) regelhaft entsprechender Ausgestaltungen."
>
> JZ 2008, 1009, 1013 f.

Diesen Auftrag erfüllt der Staat, indem er den Einzelnen im Rahmen seiner Möglichkeiten vor Angriffen Dritter auf seine IT-Systeme schützt, nämlich durch eine entsprechende Ausgestaltung der Rechtsordnung.

> Eine objektiv-rechtliche Dimension bzw. staatliche Schutzpflicht bejahen *Sachs/Krings*, JuS 2008, 481 (486); *Kutscha*, NJW 2008, 1042 (1044); *Roßnagel/Schnabel*, NJW 2008, 3534 (3535); *Hoffmann-Riem*, JZ 2008, 1009 (1014 und bei Fn. 44); *Hoffmann-Riem*, JZ 2014, 53); *Becker*, NVwZ 2015, 1335 (1339 f.); *Gersdorf*, in: BeckOK Informations- und Medienrecht, Stand: 1.05.2017, Art. 2 Rn. 29. Für eine ausführliche Herleitung der Schutz- und Förderpflicht zur Gewährleistung der IT-Sicherheit *Heckmann*, in: FS Käfer, 2009, S. 129 (133 ff.).

Diese objektiv-rechtliche Dimension folgt auch aus der enormen Bedeutung, die informationstechnische Systeme in der heutigen Gesellschaft haben. Die Relevanz informationstechnischer Systeme, die das Bundesverfassungsgericht im Jahr 2008 zur Anerkennung einer neuen Ausprägung des Allgemeinen Persönlichkeitsrechts führte, ist in den vergangenen zehn Jahren noch gewachsen – insbesondere durch die nahezu lückenlose Verwendung sog. Smartphones, aber auch durch den noch einmal gestiegenen Verbreitungs- und Vernetzungsgrad der bereits 2008 existierenden IT-Systeme. Informationstechnische Systeme sind dadurch auch zentral geworden für die Wahrnehmung und Ausübung anderer Grundrechte wie der Wissenschafts-, Meinungs-, Presse-, Versammlungs-, Vereinigungs- und Berufsfreiheit.

> Vgl. *Heckmann*, in: FS Käfer, 2009, S. 129 (135), der deshalb von der Sicherheit von IT-Systemen als einer „Querschnittsbedingung für die Grundrechtsausübung“ spricht.

Die Bedeutung der IT-Systeme für den Einzelnen, für die Wirtschaft und die Gesellschaft im Ganzen führt dazu, dass sich der Gehalt des Grundrechts auf

Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme nicht in einem Gebot an den Staat erschöpfen kann, nicht in die IT-Systeme der Bürger*innen einzudringen oder sie auszuspähen oder zu manipulieren (von eng zu regelnden Ausnahmen abgesehen). So wie der Staat die physische Infrastruktur zu sichern hat und den Umgang mit Waffen durch Polizei und Militär oder mit Kernbrennstoffen durch die Betreiber von Atomkraftwerken strengen Regeln unterwirft, so muss er auch für die virtuelle Infrastruktur Schutzvorkehrungen treffen und für den (eigenen) Umgang mit virtuellen Waffen – denn nichts anderes sind (Staats-)Trojaner zur Ausnutzung von Sicherheitslücken in IT-Systemen – überzeugende Regelungen treffen, die tatsächlich geeignet sind, die Lückenhaftigkeit und damit Verletzlichkeit von IT-Systemen zu verringern.

Dabei ist auch zu berücksichtigen, dass die Erweiterung der staatlichen Befugnisse in den virtuellen Raum gerade damit begründet wird, dass vormals physisch beobachtbare Ereignisse nunmehr gleichermaßen im Cyberspace stattfinden. Diese Erkenntnis kann aber nicht lediglich eine Erweiterung staatlicher Befugnisse begründen, um virtuelle Räume besser überwachen zu können, sondern geht Hand in Hand mit zugehörigen staatlichen Pflichten. Es zeichnet den Rechtsstaat aus, dass er neuen, ihm gefahrgeneigt oder gar als „rechtsfreie Räume“ erscheinenden Strukturen umsichtig begegnet. Zu dieser Umsicht gehört auch die Vermeidung von Kollateralschäden durch einen verantwortungsvollen Umgang mit Schwachstellen in IT-Systemen, die den Herstellern noch nicht bekannt sind.

II. Verletzung staatlicher Schutzpflicht durch fehlendes Schwachstellen-Management beim Einsatz von Staatstrojanern

Die Ausnutzung von Sicherheitslücken bzw. von Schwachstellen in IT-Systemen kann gravierende Folgen haben (dazu unter 1). Aus der staatlichen Pflicht zum Schutz der Integrität und Vertraulichkeit informationstechnischer Systeme folgt, dass der Staat zumindest **irgendwelche** mutmaßlich wirksamen Schutzmaßnahmen ergreifen muss (dazu unter 2). Daraus wiederum ergibt sich, dass jedenfalls ein Schwachstellenmanagement einzurichten ist, das die Ausnutzung von Sicherheitslücken verhindert, die dem Hersteller der betroffenen Soft- oder Hardware oder eines Online-Dienstes noch unbekannt sind (dazu unter 3). Dem genügt das Land Baden-Württemberg bisher nicht (dazu unter 4).

1. Arten und Auswirkungen von Sicherheitslücken/Schwachstellen in IT-Systemen

Sicherheitslücken oder Schwachstellen (die Begriffe werden im Folgenden synonym verwendet) sind nach einer Definition der US-amerikanischen nationalen Telekommunikations- und Informationsbehörde „Schwächen einer Software, Hardware oder eines Online-Dienstes, die ausgenutzt werden können, um die Vertraulichkeit, Integrität oder Verfügbarkeit eines Systems oder die auf ihm gespeicherten Daten zu verletzen.“

> Im Original: „Vulnerabilities are weaknesses of software, hardware, or online services that can be used to damage the confidentiality, integrity, or availability of those systems or the data they store.“
>
> United States National Telecommunications and Information Administration (NTIA) Awareness and Adoption Group, Vulnerability Disclosure Attitudes and Actions, Research Report, 2016. Online abrufbar un-

ter: https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf (zuletzt abgerufen am 5. Dezember 2018).

§ 2 Abs. 6 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik („BSIG“) definiert Sicherheitslücken als „Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen System beeinflussen können.“

Innerhalb dieser Definition werden Schwachstellen danach unterschieden, ob sie dem Hersteller bereits bekannt (dann „n-days“, im Sinne von: dem Hersteller bereits seit n Tagen bekannt) oder noch unbekannt sind (dann „0-days“, sprich: Zero-days oder Oh-days, dem Hersteller null Tage bekannt).

Aus der Perspektive der IT-Sicherheit von Systemen, die mit der fehlerhaften Software arbeiten, unterscheiden sich n-days und 0-days fundamental:

Für 0-days stehen in aller Regel noch keine technischen Lösungen – sogenannte „fixes“ oder „patches“ – bereit, abgesehen von dem seltenen Fall, dass der Hersteller die Software auch in Unkenntnis der Sicherheitslücke zufällig so ändert, dass die Lücke gleichsam „nebenbei“ geschlossen wird.

Für n-days hingegen können seitens des Herstellers des betroffenen Systems grundsätzlich bereits Gegenmittel entwickelt worden sein. Gleichwohl zeigt sich auch hier ein sehr diverses Bild: Die Software mancher IT-Systeme lässt sich gar nicht updaten, dies ist etwa im Bereich internetfähiger Kleingeräte wie Webcams oder WLAN-Router verbreitet. Hier konvergieren also 0-days und n-days in ihren praktischen Auswirkungen; allein eine Information aller Nutzer

und eine Abkoppelung der Geräte vom Internet können hier Angriffe vereiteln. Für andere Systeme – etwa Smartphones, Laptops und Desktop-Computer – gibt es zwar prinzipiell die Möglichkeit, sowohl das Betriebssystem als auch die installierte Anwendungssoftware zu aktualisieren. Diese Möglichkeit nutzen aber sowohl die Hersteller als auch die Nutzer*innen der Systeme in sehr unterschiedlicher Weise: Seitens der Hersteller werden insbesondere ältere Systeme oft nicht mehr mit Updates versorgt. „Ältere" ist hier allerdings ein sehr relativer Begriff – während beispielsweise iPhones noch einige Jahre nach dem Verkaufsschluss mit Updates des Betriebssystems iOS versorgt werden, endet die Update-Versorgung bei Android-Smartphones teilweise bereits mit dem Ende des Vertriebs eines Modells oder jedenfalls wenige Monate danach. Selbst wenn für ein bestimmtes Gerät oder eine Anwendungssoftware ein Update verfügbar ist, ist aber keineswegs gewährleistet, dass es auch jedes betroffene System (rechtzeitig) erreicht: Teilweise arbeiten Nutzer*innen jahrelang mit veralteten Versionen von Betriebssystem und Anwendungen, weil sie sich über Updates und Sicherheitslücken keine Gedanken machen oder sich von der Komplexität eines Update-Vorgangs überfordert fühlen.

Sicherheitslücken stellen dabei in alltäglichen IT-Systemen keine Ausnahme, sondern den Normalfall dar. Das Bundesamt für Sicherheit in der Informationstechnik („BSI") geht davon aus, dass

> „bei jedem hinreichend komplexen Softwareprodukt von der Existenz kritischer Schwachstellen auszugehen ist. (…) Da nur ein Teil der gefundenen Fehler beseitigt oder veröffentlicht wird, ist eine Gefährdung durch nicht öffentlich bekannte Schwachstellen, für die es noch keine Sicherheits-Updates gibt, immer latent vorhanden. Daher sollte davon ausgegangen werden, dass die eingesetzte Software immer Schwachstellen enthält, die auch ausgenutzt werden (…)."

BSI, Die Lage der IT-Sicherheit in Deutschland 2017, online abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4 (zuletzt abgerufen am 31. Juli 2018), S. 18.

Geraten n-days, für die noch keine technischen Lösungen bestehen oder verbreitet wurden, oder 0-days in die falschen Hände, kann das gravierende Folgen haben. Die Entwicklung von Schadsoftware dauert im Median 22 Tage.

RAND Corporation, Zero Days, Thousands of Nights , online abrufbar unter https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf (zuletzt abgerufen am 31. Juli 2018), S. 57.

Werden die IT-Systeme von Infrastruktureinrichtungen oder Krankenhäusern geschädigt, sind auch Todesfälle nicht ausgeschlossen. Das ist kein weitgehend hypothetisches Szenario, das als Restrisiko der sicherheitsbehördlichen Aufklärung außer Acht gelassen werden könnte. Solche Folgen von Angriffen auf IT-Systeme liegen vielmehr ausgesprochen nahe und sind teilweise bereits eingetreten. So hat erst im Mai 2017 das Schadprogramm „WannaCry“ weltweit Schäden verursacht, indem es die IT-Systeme von Behörden und Unternehmen, insbesondere auch von britischen Krankenhäusern lahmlegte und nur gegen Lösegeldzahlung wieder freigab.

Vgl. etwa https://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung (zuletzt abgerufen am 31. Juli 2018) sowie bereits oben A.

„WannaCry“ ist kein Einzelfall. Das BSI hat in seinem Lagebericht eine ganze Reihe an Fällen dargestellt, darunter einen, bei dem durch Ausnutzung einer

Sicherheitslücke in der E-Commerce-Software *Magento* die Zahlungsinformationen der Kund*innen von mindestens 1.000 deutschen Online-Shops an die Täter*innen weitergleitet wurden.

> BSI, Die Lage der IT-Sicherheit in Deutschland 2017, online abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4 (zuletzt abgerufen am 31. Juli 2018), S. 20.

Andere Unternehmen werden Opfer von Wirtschaftsspionage oder fremden Regierungen, häufig ohne ihr Wissen. Viele Angriffe unter Ausnutzung von Sicherheitslücken werden nicht öffentlich bekannt, weil Unternehmen nicht mit mangelnder IT-Sicherheit in Verbindung gebracht werden möchten. Aus diesem Grunde kommt zu den ohnehin hohen Fallzahlen eine hohe Dunkelziffer hinzu. Das Versicherungsunternehmen Lloyd‘s schätzt, dass künftige massenweise Angriffe auf IT-Systeme Schäden von bis zu 53 Mrd. US-Dollar verursachen könnten.

> Lloyd’s-Bericht vom 17. Juli 2017, online abrufbar unter: https://www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report (zuletzt abgerufen am 5. August 2018).

2. Staatliche Schutzpflicht aus dem IT-Grundrecht in Bezug auf Sicherheitslücken

Vor diesem Hintergrund ist der Staat nicht gehalten, die Beschwerdeführer*innen und andere Personen im Geltungsbereich des Grundgesetzes vor jeder Beeinträchtigung ihrer IT-Systeme zu schützen: Vom Staat ist nichts objektiv Unmögliches zu verlangen. Er muss auch nicht schlechterdings alles in seiner Macht Stehende zu ihrem Schutz unternehmen, etwa indem er Gegenmaßnahmen für alle ihm bekannten Gefahren selbst entwickelt und bereitstellt oder gar

ihm noch unbekannte Gefahren selbst ermittelt und so Sicherheitslücken anstelle der Anbieter der betroffenen IT-Systeme schließt. Denn das brächte ihn schnell an technische, regulatorische und fiskalische und scheiterte letztlich auch am Fehlen virtueller Grenzen.

Das bedeutet aber nicht, dass der Staat im Angesicht von Gefahren für die IT-Systeme der Beschwerdeführer*innen sowie anderer Personen im Geltungsbereich des Grundgesetzes untätig bleiben oder gar seinerseits die IT-Sicherheitslage weiter verschärfen darf. Denn die aus dem IT-Grundrecht abgeleitete staatliche Schutzpflicht für die Integrität informationstechnischer Systeme (vgl. dazu oben) erfordert jedenfalls, dass der Staat sich dieser Herausforderung erkennbar annimmt und in einer Weise tätig wird, die aus der Perspektive der IT-Sicherheit noch als sachdienlich und hinreichend wirksam angesehen werden kann. In der Terminologie des allgemeinen Verwaltungsrechts formuliert: Das Ermessen des Staates hinsichtlich der Frage des Ob eines Tätigwerdens zugunsten der IT-Sicherheit ist angesichts der dramatischen Bedrohung durch IT-Sicherheitslücken auf Null reduziert. Ein Tätigwerden des Staates, das der IT-Sicherheit zuwiderläuft, ist demnach schlechthin nicht mit der aus dem IT-Grundrecht resultierenden staatlichen Schutzpflicht vereinbar. Ein positives Tätigwerden ist daran zu messen, ob die (traditionell weit verstandenen) legislatorischen Spielräume eingehalten worden sind.

Fraglich kann demnach nur sein, welchen Mindestumfang staatliche Maßnahmen zur Gewährleistung der IT-Sicherheit haben müssen. Um diesen **Mindest**umfang zu bestimmen, sind zunächst alle **möglichen** Maßnahmen zum Schutz von IT-Systemen vor Gefahren durch unbekannte Sicherheitslücken zu betrachten: Der Staat kann einerseits entscheiden, ob er zur Gewährleistung der Sicherheit von IT-Systemen Sicherheitslücken selbst aktiv ermittelt oder ob er nur Kenntnis von ihnen erlangt. Er kann andererseits entscheiden, ob er nach Ermittlung oder Kenntniserlangung selbst Gegenmaßnahmen einleitet oder ob er lediglich Dritte zu Gegenmaßnahmen befähigt.

Zu diesen beiden Dimensionen kommt eine dritte hinzu, nämlich das **Wann** der Maßnahmen zur Schließung einer Sicherheitslücke. Dass der Staat **nie** Maßnahmen ergreift, ist – wie bereits dargestellt – bei grundsätzlicher Anerkennung einer staatlichen Schutzpflicht keine Option.

Aufgrund dieser Überlegungen wird deutlich, dass die geringste Anforderung an staatliches Tätigwerden angesichts von IT-Sicherheitsbedrohungen durch 0-days darin besteht, sie Dritten – typischerweise dem Hersteller – zu melden und so auf Abhilfe zu drängen. Ein Weniger an staatlichem Schutz vor den Gefahren von unbekannten Sicherheitslücken ist kaum denkbar: nämlich die aktive Befähigung Dritter zu Gegenmaßnahmen, nachdem der Staat Kenntnis von Sicherheitslücken erlangt hat, sowie eine nachvollziehbare Entscheidung über den Zeitpunkt staatlichen Tätigwerdens. Zur Befähigung Dritter zu Gegenmaßnahmen gehört auch, dass der Staat bis zum Wirksamwerden der Gegenmaßnahmen nicht selbst die Gefahr eines Schadens erhöht. Genau dies tut er indes, wenn er etwa die Informationen über Sicherheitslücken geheim hält, um sie seinerseits ausnutzen zu können.

3. Mindestanforderungen an ein staatliches Schwachstellen-Management beim Einsatz von Staatstrojanern

Um Staatstrojaner einzusetzen, müssen staatliche Behörden Sicherheitslücken kaufen. Derzeit verfügen sie noch nicht über die Fähigkeiten, selbst Sicherheitslücken aufzudecken. Das bestätigte der Präsident der Zentralen Stelle für Informationstechnik im Sicherheitsbereich („ZITiS“), einer neuen Einrichtung des Bundes, die die Ermittlungs- und andere Behörden bei der Identifikation und Ausnutzung von Schwachstellen unterstützen soll:

> Heise im Februar 2018, online abrufbar unter: https://www.heise.de/newsticker/meldung/Schlagabtausch-zu-ZITiS-

IT-Sicherheitsluecken-schliessen-oder-ausnutzen-3976587.html (zuletzt abgerufen am 3. August 2018).

Auf Bundesebene hat die Regierung explizit nicht ausgeschlossen, 0-days – also Schwachstellen, die dem Hersteller noch unbekannt sind –, für Quellen-TKÜ und Online-Durchsuchung einzusetzen:

> „Ob und inwieweit im Spannungsfeld technischer Erfordernisse, rechtlicher Vorgaben, sicherheits- und rechtspolitischer Erwägungen sowie taktischer Einsatzrahmenbedingungen zukünftig eine Nutzung sog. ‚Zero-Day-Exploits' für die Durchführung von Maßnahmen der Quellen-TKÜ und Online-Durchsuchung durch Sicherheitsbehörden in Betracht kommt, ist durch die zuständigen Stellen der Bundesregierung in Abstimmung mit den zu beteiligenden nationalen und ggf. internationalen Stellen und Gremien zu prüfen."
>
> Antwort der Bundesregierung auf Fragen 26 bis 31 einer Kleinen Anfrage, BT-Drs. 18/13413; Antworten auf diese Fragen sind eingestuft, aber online zugänglich unter https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/#Antwort-Drucksache-18-13566-NfD (zuletzt abgerufen am 3. August 2018).

Seitens der Landesregierung Baden-Württembergs sind zur Frage des Umgangs mit 0-days keine Äußerungen bekannt. Auch die Gesetzesbegründung schweigt zu dieser Frage. Dabei ist aus dem Ergebnis der Anhörung ersichtlich, das in der Stellungnahme des Anwaltsverbandes Baden-Württemberg e.V. § 23b Abs. 2 PolG grundlegend und insbesondere auch dahingehend kritisiert wurde, dass der Staat Sicherheitslücken ausnutzen könne, deren Existenz er eigentlich verhindern sollte. Mit diesem Einwand setzt sich die Erwiderung der Landesregierung nicht auseinander.

Landtag von Baden-Württemberg, Gesetzentwurf der Landesregierung. Gesetz zur Änderung des Polizeigesetzes und des Gesetzes über die Ladenöffnung in Baden-Württemberg, Drs. 16/2741, zur Begründung siehe S. 20-22, hinsichtlich des Ergebnisses der Anhörung und der Erwiderung der Landesregierung siehe S. 57-63, insb. S. 60. Online abrufbar unter https://www.landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP16/Drucksachen/2000/16_2741_D.pdf (zuletzt abgerufen am 26. November 2018).

Wenn der Gesetzgeber den Einsatz sog. Staatstrojaner zur Quellen-TKÜ für erforderlich hält, also regelmäßig Kenntnis von Sicherheitslücken in IT-Systemen erlangt bzw. sich diese Kenntnis sogar aktiv verschafft, so hat er zwingend zu gewährleisten, dass die betroffenen Systemhersteller den Behörden bekanntwerdende Sicherheitslücken schnellstmöglich beseitigen können. Denn das Zurückhalten von Sicherheitslücken, die den Herstellern der betreffenden Systeme noch nicht bekannt sind, ist bei Gegenüberstellung der betroffenen Rechtsgüter schlechthin unzulässig:

Für das Zurückhalten von Sicherheitslücken könnte das Interesse an der Abwehr von Gefahren für die öffentliche Sicherheit sprechen, also das Interesse, durch Ausnutzung der unbekannten Sicherheitslücke Maßnahmen gem. § 23b Abs. 2 PolG BW durchführen zu können, die sodann möglicherweise zur Verhinderung einer der in § 23b Abs. 1 PolG BW genannten Straftaten beitragen können. Indes spricht nichts dafür, dass es für die Infiltration des intendierten Zielsystems zwingend gerade einen 0-day, also eine auch dem Hersteller noch unbekannte Sicherheitslücke braucht. Wie oben im Einzelnen ausgeführt wurde, lassen sich in den meisten Fällen auch den Herstellern bekannte Lücken ausnutzen – etwa weil der Hersteller für das konkrete Zielsystem noch kein Update bereitgestellt oder die Zielperson dieses nicht eingespielt hat. Aus der Perspektive der Gefahrenabwehr bedeutet also die Nutzung von 0-days allenfalls

einen gewissen Komfort-Gewinn, weil dies die Suche nach einem Infiltrationsvektor zur Infektion des Zielsystems mit einem Trojaner gelegentlich verkürzen mag.

Aus der Perspektive der IT-Sicherheit der Allgemeinheit indes ist der Unterschied zwischen der Erlaubnis zur Nutzung von 0-days und n-days fundamental: Während ersteres die oben im Detail hergeleiteten fatalen Anreize schafft, 0-days geheimzuhalten, ist die Nutzung von n-days aus der Perspektive der IT-Sicherheit der Allgemeinheit unproblematisch: Die Lücke ist dem Hersteller ja bereits bekannt. Ob andere IT-Systeme mit einem Update versorgt werden liegt damit in der Sphäre des Herstellers sowie der Nutzer*innen.

Vor diesem Hintergrund – geringe Vorteile des 0-day-Einsatzes, aber erhebliche Beeinträchtigung der IT-Sicherheit bis hin zur Gefährdung von Leib und Leben (etwa von Krankenhauspatient*innen, wenn lebenswichtige IT-Systeme gehackt werden), weil eine Stelle des Bundes eine Sicherheitslücke geheim gehalten hat – ist eine Rechtslage, die den Einsatz von 0-days erlaubt, schlechthin unvereinbar mit der aus dem IT-Grundrecht resultierenden staatlichen Schutzpflicht.

Selbst wenn man diesen zwingenden Schluss nicht ziehen wollte, so müsste der Gesetzgeber mindestens ein – angesichts der Grundrechtsrelevanz jedenfalls in seinen Grundzügen und in seiner Ausrichtung auf die Förderung der IT-Sicherheit der Allgemeinheit zwingend durch formelles Gesetz einzuführendes – Verwaltungsverfahren vorsehen, 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. Verfassungswidrig erscheint jedenfalls der derzeitige

Rechtszustand, in dem die Polizei des Landes Baden-Württemberg und alle anderen Stellen des Landes ohne irgendeine gesetzliche Grundlage nach Gutdünken entscheiden, wie sie mit Sicherheitslücken verfahren und welche sie ggf. für hoheitliche Eingriffe verwenden bzw. geheimhalten wollen.

Materiell könnten der Bedeutung der Lücke für einen potentiellen späteren Einsatz als „Staatstrojaner“ beispielsweise folgende Punkte gegenübergestellt werden:

- Verbreitung der Sicherheitslücke,
    - quantitativ: Zahl der betroffenen Nutzer*innen
    - qualitativ: Art der betroffenen Nutzer*innen
- Gewicht der Sicherheitslücke,
    - zur Ausnutzung erforderlicher Aufwand
    - aus Ausnutzung resultierender Schaden
- Wahrscheinlichkeit, dass Betroffene die Ausnutzung der Lücke bemerken und im Einzelfall Gegenmaßnahmen einleiten,
- Wahrscheinlichkeit einer technischen Lösung für die Lücke,
- Wahrscheinlichkeit einer Verbreitung der technischen Lösung,
- Möglichkeiten zur Linderung der Folgen bei (zeitweiser) Geheimhaltung der Lücke,
- Wahrscheinlichkeit, dass Dritte die Lücke finden.

Vgl. hierzu *Sven Herpig*, Schwachstellen-Management für mehr Sicherheit. Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte. Stiftung Neue Verantwortung Berlin 2018, online abrufbar unter https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellen-management.pdf (zuletzt abgerufen am 29. November 2018).

Außerdem muss der Staat Vorkehrungen dagegen treffen, dass seine Kenntnis von Sicherheitslücken bzw. seine Mittel zu ihrer Ausnutzung von Dritten erbeutet werden. Es ist derzeit nicht erkennbar, dass deutsche Ermittlungsbehörden die bei ihnen vorhandenen Informationen oder Einsatzmittel bedeutend besser schützen können als die US-amerikanische National Security Agency im Falle „WannaCry“: Die Sicherheitslücken, die die hinter „WannaCry“ stehenden Kriminellen ausnutzten, waren zuvor der NSA gestohlen worden. Ein Schwachstellen-Management muss aber erst recht gewährleisten, dass aus dem staatlichen Horten von Sicherheitslücken und den Mitteln zu ihrer Ausnutzung keine **zusätzliche** Gefahr für die öffentliche IT-Sicherheit entsteht.

4. Bisherige Gesetze des Landes Baden-Württemberg erfüllen nicht die Mindestanforderungen an ein wirksames Schwachstellen-Management

Bislang gibt es keinen Prozess zur Bewertung von Schwachstellen, die Behörden des Landes Baden-Württemberg zu Quellen-TKÜ nutzen wollen, sowie keine Verfahren und Kriterien, nach denen über eine Meldung der Schwachstelle an die Hersteller entschieden werden kann. Auch auf Bundesebene sind hinsichtlich der auch Bundesbehörden betreffenden Befugnisse für Online-Durchsuchung und Quellen-TKÜ keine derartigen Prozesse bekannt.

> Vgl. Bericht von einer Veranstaltung im Februar 2018 mit dem ZITiS-Präsidenten, online unter: https://www.heise.de/newsticker/meldung/Schlagabtausch-zu-ZITiS-IT-Sicherheitsluecken-schliessen-oder-ausnutzen-3976587.html (zuletzt abgerufen am 3. August 2018).

III. Verletzung subjektiver Rechte der Beschwerdeführer*innen zu 1 bis 7

Die Beschwerdeführer*innen zu 1 bis 7 sind – wie vorgetragen – einerseits einer besonderen Gefahr von Hackerangriffen ausgesetzt. Dabei besteht insbesondere die besondere Wahrscheinlichkeit, dass dazu gerade 0-day-Sicherheitslücken ausgenutzt werden. Andererseits würden erfolgreiche Hackerangriffe bei ihnen jeweils auch andere Personen möglicherweise empfindlichst treffen. Es liegt nahe, dass diese Gefahr auch durch Sicherheitslücken droht, die Behörden des Landes Baden-Württemberg zu Maßnahmen nach § 23b Abs. 2 i.V.m. Abs. 1 PolG BW nutzen oder nutzen werden und dafür unter Verletzung ihrer Schutzpflicht geheim halten. Näherer Vortrag hierzu ist den Beschwerdeführer*innen naturgemäß nicht möglich, weil sie keine Kenntnis der konkreten geheim gehaltenen Sicherheitslücken haben.

E. Anträge

Die Beschwerdeführer*innen beantragen zu entscheiden:

> § 23b Abs. 2 in Verbindung mit § 23b Abs. 1 PolG BW ist mit Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG unvereinbar, soweit er es erlaubt, zur Durchführung von Eingriffen in informationstechnische Systeme mit technischen Mitteln auch Schwachstellen dieser Systeme auszunutzen, die den jeweiligen Herstellern noch nicht bekannt sind (sog. *0-days*).