Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)844 A

JOHANNES GUTENBERG UNIVERSITÄT MAINZ

JOHANNES GUTENBERG-UNIVERSITÄT MAINZ - 55099 Mainz

FACHBEREICH 03
JURA
Lehrstuhl für Öffentliches Recht und Informationsrecht, insbesondere Datenschutzrecht

Universitätsprofessor
Dr. Matthias Bäcker

Johannes Gutenberg-Universität Mainz
Jakob-Welder-Weg 9
55128 Mainz

Tel. +49 6131 39 28173
Fax +49 6131 39 28172

matthias.baecker@uni-mainz.de
www.baecker.jura.uni-mainz.de/

Stellungnahme

zu dem Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts

(BT-Drs. 19/24785)

Gliederung

Ergebnisse

1. Die generelle Ausweitung des Bestrebungsbegriffs auf Einzelpersonen überdehnt die Aufgabe des Verfassungsschutzes und führt zu (zusätzlichen) verfassungsrechtlichen Mängeln einiger Eingriffsermächtigungen des Verfassungsschutzrechts.
2. Das nachrichtendienstliche Informationssystem ist (nach wie vor) unzureichend geregelt. Die teilnehmenden Behörden sind ermächtigt, umfangreiche und sensible Datenbestände mit Bezug auch zu unverdächtigen Personen anzulegen und nahezu anlasslos weiterzuverarbeiten. Dies trägt der hohen Eingriffsintensität eines so umfassenden Datenverbunds nicht Rechnung.
3. Die Ermächtigung zu Quellen-Telekommunikationsüberwachungen muss mit Schutzvorkehrungen verbunden werden, die eine Ausnutzung noch unbekannter IT-Sicherheitslücken (Zero-Days) zur Infiltration des Zielsystems ausschließen oder zumindest einem strengen Risikomanagement unterwerfen.
4. Die Erstreckung der Quellen-Telekommunikationsüberwachung auf lokal gespeicherte frühere Kommunikationsinhalte geht fehl. Hierbei handelt es sich um eine Online-Durchsuchung, an die strengere Anforderungen zu stellen sind.
5. Die Ermächtigung zu Quellen-Telekommunikationsüberwachungen führt die zahlreichen verfassungsrechtlichen Mängel des Artikel 10-Gesetzes fort und vertieft sie.

4 I. Einzelpersonen als Bestrebungen

Die in § 4 Abs. 1 Sätze 3 und 4 BVerfSchG-E vorgesehene generelle Erstreckung des Begriffs der verfassungsschutzrelevanten Bestrebung auf Einzelpersonen überdehnt die Aufgabe des Verfassungsschutzes und führt zu (zusätzlichen) verfassungsrechtlichen Zweifeln an einem Teil der Eingriffsermächtigungen des Gesetzes.

Die Ausweitung des Beobachtungsauftrags überdehnt die Aufgabe des Verfassungsschutzes, weil sie die Verfassungsschutzbehörden potenziell mit einer weitreichenden Ausforschung des *Forum Internum* von Menschen betraut. Die von einer Einzelperson ausgehende Bestrebung wird gemäß § 4 Abs. 1 Satz 4 BVerfSchG-E anhand der Zielrichtung des Verhaltens dieser Person bestimmt. Damit knüpft der Beobachtungsauftrag primär an die inneren Befindlichkeiten der Person an, die ihrem Verhalten zumeist erst seinen verfassungsfeindlichen Sinn vermitteln.[1] Anders als bei Personenzusammenschlüssen, deren Angehörige zwangsläufig zumindest miteinander kommunizieren und damit ihre Ziele nach außen manifestieren müssen, lädt die vorgesehene Regelung geradezu zu einer Beobachtungspraxis ein, die statt von objektiv verfassungsschutzrelevanten Handlungen von (vermuteten) persönlichen Eigenschaften oder sozialen Einbindungen der betroffenen Person ausgeht.

Ein Bedürfnis hierfür ist nicht erkennbar. Eine rechtsstaatlich handelnde Verfassungsschutzbehörde hat kein Interesse daran, Einzelpersonen allein wegen ihrer mutmaßlichen Gesinnung zu beobachten. Die Gesetzesbegründung beruft sich zwar zum einen auf eruptive Radikalisierungsverläufe von Einzelpersonen, die zu militanten Aktionen führen können, zum anderen auf die auch von Einzelpersonen aktivierbare Eigendynamik sozialer Medien.[2] Beide Szenarien erfordern jedoch keine so weitreichende Ausweitung des Beobachtungsauftrags. Gewaltgeneigte Einzelpersonen werden bereits heute durch § 4 Abs. 1 Satz 6 BVerfSchG vom Bestrebungsbegriff erfasst. Da der Beobachtungsauftrag des Verfassungsschutzes generell bereits im Vorfeld konkreter Gefahren einsetzt, lassen sich fortgeschrittene Instrumente der personenbezogenen Risikobewertung, auf die sich die Gesetzesbegründung bezieht, in die gebotene Bewertung des Gewaltpotenzials einer Person zwanglos integrieren. Wo sich ein solches Potenzial auch mit solchen Instrumenten nicht erkennen lässt, verbleibt vor allem eine faktische Beobachtungslücke, die sich durch eine Ausdehnung des gesetzlichen Beobachtungsauftrags nicht schließen lässt. Soweit eine Beobachtung an die agitierende oder einschüchternde öffentliche Kommunikation von selbst nicht gewaltbereiten Personen anknüpfen soll, könnte eine auf das spezifische Gefährdungspotenzial solcher Personen und ihres Kommunikationsverhaltens zugeschnittene Regelung geschaffen werden, ohne den Beobachtungsauftrag hinsichtlich von Einzelpersonen

---

[1] Wenn Verhaltensweisen von Einzelpersonen auf die Verwirklichung bestimmter Ziele „gerichtet sein“ müssen, geht aus dem Normtext klar hervor, dass es zumindest auch auf die Intentionen der Person ankommt, vgl. allgemein zu der Diskussion um subjektive Erfordernisse im Rahmen von § 4 Abs. 1 BVerfSchG einerseits Warg, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, V § 1 Rn. 38 f., andererseits Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 4 BVerfSchG Rn. 39 ff., beide m.w.N. auch zur – uneinheitlichen – Rechtsprechung.

[2] BT-Drs. 19/24785, S. 17.

5 uferlos auszuweiten. Gegen eine derartige Regelung bestünden keine grundlegenden Bedenken.

Die einschränkungslose Ausweitung des Beobachtungsauftrags auf Einzelpersonen erzeugt im Übrigen auch systematische Unstimmigkeiten. In der Folge können isoliert handelnde Einzelpersonen leichter zum Beobachtungsobjekt werden als Personen, die für einen Personenzusammenschluss handeln. Denn Personen handeln gemäß § 4 Abs. 1 Satz 2 BVerfSchG nur dann für einen Personenzusammenschluss, wenn sie ihn in seinen Bestrebungen nachdrücklich unterstützen. Dies setzt eine Unterstützung von bedeutendem Gewicht voraus.[3] Hingegen sollen fortan Einzelpersonen ohne Bezug zu einem Personenzusammenschluss auch dann dem Beobachtungsauftrag des Verfassungsschutzes unterfallen, wenn von ihnen bislang lediglich Handlungen ohne besonderes Bedrohungspotenzial für die Schutzgüter des Verfassungsschutzes ausgegangen sind. Maßgeblich ist nach § 4 Abs. 1 Satz 4 BVerfSchG-E lediglich die Zielrichtung dieser Handlungen. Nach allgemein anerkannter Wertung, die auch die Gesetzesbegründung nicht grundsätzlich in Frage stellt,[4] sind jedoch Personenzusammenschlüsse gefährlicher als Einzelpersonen, da sie typischerweise über weitergehende Handlungsmöglichkeiten verfügen und eine Gruppendynamik aufbauen können.[5] Es ist darum wenig folgerichtig, den Beobachtungsauftrag gegenüber Einzelpersonen weiter zu fassen als gegenüber Personen, die einen solchen Zusammenschluss unterstützen.

Die Erweiterung des Beobachtungsauftrags birgt als Folgeproblem erhebliche (zusätzliche) verfassungsrechtliche Bedenken gegen einige Eingriffsermächtigungen des Verfassungsschutzrechts. Diese Ermächtigungen erlauben den Einsatz nachrichtendienstlicher Mittel, wenn Tatsachen die Annahme rechtfertigen, dass dadurch Erkenntnisse über verfassungsfeindliche Bestrebungen erlangt werden können.[6] Eingriffsermächtigungen des Nachrichtendienstrechts müssen jedoch aus verfassungsrechtlichen Gründen zumindest daran anknüpfen, dass der Eingriff „zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten ist“.[7] Solange der Bestrebungsbegriff an gewaltgerichtete bzw. besonders schadensgeneigte Verhaltensweisen von Einzelpersonen (Aktionen) oder an Personenzusammenschlüsse (Gruppierungen) anknüpft, mögen die genannten Eingriffsermächtigungen diesem Erfordernis noch genügen.[8] Wird der Bestrebungsbegriff aber für Einzelpersonen

[3] Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 4 BVerfSchG Rn. 35.
[4] Vgl. BT-Drs. 19/24785, S. 17.
[5] Vgl. Warg, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, V § 1 Rn. 28; Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 4 BVerfSchG Rn. 38.
[6] § 9 Abs. 1 Satz 1 Nr. 1, § 9a Abs. 1 Satz 1, § 9b Abs. 1 Satz 1 BVerfSchG; vgl. ferner zur Weiterverarbeitung erhobener Daten § 10 Abs. 1 Nr. 1 und 2 BVerfSchG.
[7] BVerfGE 130, 151 (206); BVerfG, Beschluss vom 27. Mai 2020 - 1 BvR 1873/13 -,Rn. 151.
[8] Vgl. aber generell zur Reformbedürftigkeit der Eingriffstatbestände des Nachrichtendienstrechts Bäcker, in: Dietrich u.a., Nachrichtendienste im demokratischen Rechtsstaat, 2018, S. 137 (144 ff.).

6 derart ausgedehnt, dass er im Wesentlichen von deren subjektiven Zielsetzungen ausgeht, sind die verfassungsrechtlichen Grenzen überschritten.[9]

Die ausufernde Erweiterung des Beobachtungsauftrags lässt sich nicht – wie es die Gesetzesbegründung anscheinend annimmt – dadurch kompensieren, dass den Verfassungsschutzbehörden für die Beobachtung von Einzelpersonen anders als für die Beobachtung von Personenzusammenschlüssen ein Entschließungsermessen eingeräumt wird. Insbesondere soweit der Bestrebungsbegriff in gesetzlichen Eingriffsermächtigungen in Bezug genommen wird, ist es Sache des Gesetzgebers, durch eine hinreichend restriktive Normfassung zu gewährleisten, dass der Verhältnismäßigkeitsgrundsatz gewahrt bleibt. Dies darf nicht dem behördlichen Ermessen überlassen werden. Im Übrigen ist der geplanten Regelung nicht zu entnehmen, dass ein Entschließungsermessen bestehen soll. Dass die Verfassungsschutzbehörden grundsätzlich über kein solches Ermessen verfügen, wird gemeinhin nicht aus § 4 BVerfSchG, sondern primär aus § 3 Abs. 1 BVerfSchG abgeleitet.[10] Die vorgesehene Formulierung in § 4 Abs. 1 Satz 3 BVerfSchG-E „Bestrebungen… können auch von Einzelpersonen ausgehen…“ gibt für ein behördliches Ermessen nichts her. Das Verb „können“ bezieht sich nicht auf die Beobachtungstätigkeit der Verfassungsschutzbehörden, sondern auf den Gegenstand der Beobachtung. Wenn ein Entschließungsermessen bestehen soll, müsste § 3 Abs. 1 BVerfSchG ergänzt werden.

II. Informationssystem der Verfassungsschutzbehörden

Gegen die durch § 6 Abs. 2 Satz 2 BVerfSchG-E eröffnete Möglichkeit, den MAD in das nachrichtendienstliche Informationssystem einzubinden, und gegen die in § 6 Abs. 2 Satz 4 BVerfSchG-E vorgesehene technische Verkoppelung des Informationssystems mit gemeinsamen Dateien bestehen für sich genommen keine Bedenken.

Die geplanten Regelungen vertiefen jedoch die erheblichen rechtsstaatlichen Mängel des geltenden Rechts. Das nachrichtendienstliche Informationswesen ist insgesamt unzureichend geregelt und bedarf einer grundlegenden Überarbeitung. Mit Blick auf das nachrichtendienstliche Informationssystem habe ich dies bereits in meiner Stellungnahme zu dem Entwurf eines Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes näher ausgeführt.[11] Die wesentlichen Kritikpunkte, an denen die vorgesehenen Regelungen nichts ändern, seien hier lediglich noch einmal kurz zusammengefasst:

– Die gesetzlichen Bevorratungsregelungen ermöglichen es den Verfassungsschutzbehörden, einander personenbezogene Daten jeglicher Art und Herkunft zur Verfügung zu stellen.

---

[9] Vgl. zum Polizeirecht BVerfGE 141, 220 (273); zur Übertragbarkeit des verfassungsrechtlichen Maßstabs für präventivpolizeiliche Eingriffsermächtigungen auf das Nachrichtendienstrecht BVerfG, Beschluss vom 27. Mai 2020 - 1 BvR 1873/13 -,Rn. 151.

[10] Warg, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, 2017, V § 1 Rn.40; Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 4 BVerfSchG Rn. 131.

[11] BT-Ausschussdrs. 18(4)328 A; vgl. daneben Bergemann, NVwZ 2015, S. 1705 f.

7 – Die tatbestandlichen Voraussetzungen einer Datenspeicherung im nachrichtendienstlichen Informationssystem sind sehr niedrig angesetzt. Das Gesetz sieht weder einen besonderen Speicherungsanlass vor noch beschränkt es die Speicherung auf bestimmte Personenkreise.

– Die am Informationssystem teilnehmenden Behörden können die gespeicherten Daten umfassend abrufen, mit beliebigen Analysemethoden auswerten und weiterverarbeiten. Voraussetzung ist lediglich, dass dies zur Aufgabenerfüllung erforderlich ist. Damit ist ein besonderer Weiterverarbeitungsanlass nicht benannt. Das Gesetz ermöglicht auch etwa Datenabrufe und Datenanalysen aufgrund strategischer Erkenntnisinteressen oder zur Abrundung eigener Datenbestände.[12]

– Der durch das Informationssystem geschaffene umfassende Datenverbund der Verfassungsschutzbehörden greift damit intensiv in die Grundrechte der betroffenen Personen ein. Die äußerst weit gefassten Ermächtigungen zur Speicherung und Weiterverarbeitung personenbezogener Daten im Informationssystem verfehlen die grundrechtlichen Anforderungen weit.

III. Quellen-Telekommunikationsüberwachung

Die vorgesehene Ermächtigung der Nachrichtendienste zu Quellen-Telekommunikationsüberwachungen in § 11 Abs. 1a G 10-E i.V.m. § 3 G 10 weist mehrere verfassungsrechtliche Defizite auf: Sie enthält keine hinreichenden Vorkehrungen zum Schutz der IT-Sicherheit in der Bundesrepublik (unten 1), ermöglicht eine Datenerhebung auch außerhalb laufender Kommunikationsvorgänge (unten 2) und teilt im Übrigen die Mängel des bereits geltenden Rechts (unten 3).

1. Ausnutzung von IT-Sicherheitslücken

In tatsächlicher Hinsicht besteht ein Hauptproblem von Überwachungsmaßnahmen, die auf der Infiltration eines informationstechnischen Systems beruhen, in der Installation der Überwachungssoftware. Hierfür sind verschiedene Wege denkbar. Einer von ihnen besteht darin, Sicherheitslücken der Hardware oder der Software des Zielsystems auszunutzen. Dass dieser Infiltrationsweg tatsächlich ins Auge genommen wird, zeigt die vorgesehene Pflicht der Anbieter von Telekommunikationsdiensten in § 2 Abs. 1a Satz 1 Nr. 4 G 10-E, bei der Umleitung von Telekommunikation zu Infiltrationszwecken mitzuwirken. Eine Infiltration mithilfe eines technisch manipulierten Datenstroms muss zwar nicht zwangsläufig auf der Ausnutzung von Sicherheitslücken des Zielsystems oder seines informationstechnischen Umfelds (etwa eines Routers) beruhen. Dies dürfte aber das bedeutsamste Szenario sein.

Die Ausnutzung von IT-Sicherheitslücken zur Vorbereitung einer Quellen-Telekommunikationsüberwachung lässt sich jedoch nicht in jedem Fall verfassungsrechtlich legitimieren. Ihr steht partiell das von dem Bundesverfassungsgericht entwickelte Grundrecht auf Gewährleistung der

[12] Vgl. BVerfG, Beschluss vom 27. Mai 2020 - 1 BvR 1873/13 -,Rn. 218.

8 Vertraulichkeit und Integrität informationstechnischer Systeme[13] entgegen. Dieses Grundrecht vermittelt nicht nur ein subjektives Abwehrrecht gegen staatliche Eingriffe. Es begründet – wie schon der Begriff der Gewährleistung zeigt – auch eine staatliche Pflicht dazu beizutragen, dass die Sicherheit der informationstechnischen Infrastruktur der Bundesrepublik ein hohes Niveau erreicht. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme trägt so einerseits der hohen Bedeutung der Informationstechnik für die Funktionsfähigkeit von Staat und Gesellschaft, andererseits der erheblichen Verwundbarkeit dieser Technologie Rechnung.[14]

Die objektiv-rechtliche Dimension des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist praktisch hoch bedeutsam, weil solche Systeme strukturell bedingt stets eine Vielzahl von Sicherheitslücken aufweisen, die eigenständig zu Fehlfunktionen führen oder durch Dritte missbräuchlich ausgenutzt werden können. Die Sicherheit informationstechnischer Systeme ist daher als dauerhafte öffentliche Aufgabe anzusehen. Diese Aufgabe kann der Staat allerdings weitgehend nicht eigenhändig erfüllen, da es ihm hierfür sowohl an Ressourcen als auch an Expertise fehlt. In erster Linie obliegt es vielmehr den Herstellern und Betreibern von informationstechnischen Systemen und der darauf laufenden Software, vermeidbare Sicherheitslücken nicht entstehen zu lassen und später erkannte Sicherheitslücken zeitnah zu schließen. Die staatliche Gewalt kann hierbei lediglich eine unterstützende Rolle einnehmen. Welche Beiträge sie dazu übernimmt, hängt von Gestaltungsentscheidungen ab, für die das Grundgesetz beträchtliche Spielräume lässt. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist in seiner objektiv-rechtlichen Dimension erst verletzt, wenn die staatlichen Anstrengungen offenkundig unzureichend sind.[15]

Der grundrechtliche Mindeststandard wird allerdings zumindest dann unterschritten, wenn eine staatliche Stelle ohne zureichenden Grund eine Gefährdungslage für die Vertraulichkeit und Integrität der informationstechnischen Infrastruktur in der Bundesrepublik bewusst aufrechterhält oder sogar selbst schafft. Eine solche Situation kann im Zusammenhang mit Quellen-Telekommunikationsüberwachungen abhängig von dem genutzten Infiltrationsweg auftreten. Insbesondere ist dies der Fall, wenn für die Infiltration des Zielsystems eine noch unbekannte Sicherheitslücke von Hardware oder Software ausgenutzt wird (sogenannter Zero-Day).

Da ein Zero-Day dem Hersteller und den Nutzer*innen des betroffenen informationstechnischen Systems noch unbekannt ist, gibt es gegen ihn aus Sicht dieser Personen keine wirksamen Gegenmaßnahmen. Soweit die Sicherheitslücke sich prinzipiell durch eine Anpassung des Sys-

---

[13] BVerfGE 120, 274 (302 ff.).

[14] Vgl. etwa Sachs/Krings, JuS 2008, 481 (486); Kutscha, NJW 2008, 1042 (1044); Roßnagel/Schnabel, NJW 2008, 3534 (3535); Heckmann, in: FS Käfer, 2009, S. 129 (133 ff.); Hoffmann-Riem, JZ 2009, S. 165 ff.; ders., AöR 134 (2009), S. 513 ff.; ders., JZ 2014, S. 53 ff.; Becker, NVwZ 2015, 1335 (1339 f.).

[15] Vgl. zu aus unterschiedlichen Grundrechten hergeleiteten staatlichen Schutzpflichten etwa BVerfGE 49, 89 (142); 77, 17 (214 f.); 88, 203 (251 ff.); 92, 26 (46); 106, 28 (37); 125, 39 (78 f.); 143, 313 (337 f.); BVerfG, Beschluss vom 24. März 2021 - 1 BvR 2656/18 u.a. -, Rn. 143 ff.

9 tems (etwa ein Software-Update) schließen ließe, steht der dafür erforderliche technische Baustein noch nicht zur Verfügung. Für die ansonsten notfalls gebotene vollständige oder partielle Außerbetriebnahme des Systems besteht aus Sicht der betroffenen Personen kein Anlass, solange die Sicherheitslücke nicht bekannt ist.

Sicherheitsbehörden können Zero-Days ausnutzen, um informationstechnische Systeme zu infiltrieren und so eine Quellen-Telekommunikationsüberwachung zu ermöglichen. Dieser Infiltrationsweg erzeugt jedoch einen Zielkonflikt zwischen den Sicherheitsbelangen, denen die Maßnahme dient, und dem durch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität gewährleisteten Anliegen, dass der Staat zur Sicherheit der informationstechnischen Infrastruktur in der Bundesrepublik beiträgt.[16]

Im Sinne der Effektivität der Überwachungsmaßnahme muss die Sicherheitslücke möglichst lange geheim gehalten werden. Wird die Sicherheitslücke bekannt, besteht die Gefahr, dass sie geschlossen wird und darum die Infiltration von vornherein misslingt oder die Maßnahme vorzeitig abgebrochen werden muss. Selbst nach Beendigung der einzelnen Überwachungsmaßnahme besteht ein Anreiz, den Zero-Day weiterhin geheim zu halten, um ihn für weitere Quellen-Telekommunikationsüberwachungen nutzen zu können.

Die Ausnutzung von Zero-Days durch staatliche Stellen kann zugleich in mehrfacher Hinsicht die ohnehin gegebene Bedrohungslage für die informationstechnische Infrastruktur in der Bundesrepublik aufrechterhalten oder sogar noch verschärfen.

Wird eine Sicherheitslücke aus den eben genannten Gründen geheim gehalten, so trägt die handelnde Behörde durch ihr Unterlassen dazu bei, dass diese Sicherheitslücke nicht geschlossen wird. Da sich aus technischer Sicht die Infiltration informationstechnischer Systeme durch staatliche Stellen und durch Kriminelle nicht unterscheiden, perpetuiert dieses Unterlassen das Risiko krimineller Übergriffe auf die informationstechnische Infrastruktur.

Einen darüber hinausgehenden Beitrag zur Schwächung der Informationssicherheit in der Bundesrepublik leistet der Staat dann, wenn eine Behörde Informationen über eine Sicherheitslücke nicht selbst generiert, sondern von Dritten bezieht. Dies ist kein unrealistisches Szenario. So hat der Präsident der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) noch im Jahr 2018 eingeräumt, seine Stelle verfüge nicht über die technische Expertise, um Sicherheitslücken im benötigten Umfang selbst aufzudecken.[17] Werden Zero-Days auf dem Markt eingekauft, so stützt die beschaffende staatliche Stelle diesen Markt aktiv. Schon wegen der strengen strafrechtlichen Regulierung des Umgangs mit Informationen und Software, die zum Ausspähen oder Abfangen von Daten bestimmt sind (vgl. § 202c StGB), ist anzunehmen, dass die Akteure

---

[16] Vgl. BVerfGE 120, 274 (326), wo jedoch dieser Zielkonflikt nicht näher analysiert und darum aus ihm keine weiteren Folgerungen gezogen werden. Dies war in dem damaligen Verfahren auch nicht angezeigt, da die seinerzeit angegriffene Eingriffsermächtigung bereits die subjektiv-rechtlichen Anforderungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (weit) verfehlte.

[17] Vgl. https://www.heise.de/newsticker/meldung/Schlagabtausch-zu-ZITiS-IT-Sicherheitsluecken-schliessen-oder-ausnutzen-3976587.html.

10 auf diesem Markt regelmäßig zumindest in einem rechtlichen Graubereich agieren. Die staatliche Teilnahme an diesem Markt birgt darum das erhebliche Risiko, Straftaten zu begünstigen. Sie setzt zudem einen Anreiz für IT-Sicherheitsexpert*innen, ihr Wissen um Sicherheitslücken zu monetarisieren statt damit zur Stärkung der Informationssicherheit beizutragen. So kann die staatliche Marktteilnahme zur Stabilisierung auch des illegalen Marktes und zur Vermehrung der angebotenen Sicherheitslücken beitragen, die von Dritten aufgekauft und ausgenutzt werden können.

Eine staatliche Stelle, die über einen geheim gehaltenen Bestand von Informationen über Zero-Days verfügt, ist schließlich selbst ein lohnendes Angriffsziel für Kriminelle, die sich diese Informationen beschaffen und für eigene Zwecke nutzen wollen. Hierbei handelt es sich nicht um ein weitgehend hypothetisches Szenario, das als Restrisiko der staatlichen Aufklärung außer Acht bleiben könnte. Solche Angriffe liegen vielmehr ausgesprochen nahe und sind schon vorgekommen. So hat im Mai 2017 das Schadprogramm „WannaCry“ weltweit erhebliche Schäden verursacht. In Deutschland war davon etwa die Deutsche Bahn betroffen. Besonders schwer traf es das Gesundheitssystem in Großbritannien. Zahlreiche Rechner des National Health Service waren befallen. Die Daten von Krebs- und Herzpatient*innen standen nicht mehr zur Verfügung. Viele Kranke mussten in andere Kliniken umgeleitet werden. Dieses Schadprogramm nutzte eine Sicherheitslücke in Windows-Betriebssystemen aus, welche die kriminellen Angreifer nach verbreiteter Einschätzung bei der US-amerikanischen National Security Agency (NSA) ausgespäht hatten, die ihrerseits diese Sicherheitslücke für eigene Zwecke eingesetzt und geheim gehalten hatte.[18] Chinesische Spione sollen die Sicherheitslücke bereits im Jahr 2016 von der NSA erlangt und für eigene Angriffe genutzt haben.[19] Es liegt fern, dass deutsche Sicherheitsbehörden die bei ihnen vorhandenen Informationen über Sicherheitslücken bedeutend besser schützen können als die NSA. Vielmehr ist anzunehmen, dass sich ein Verlust nie ausschließen lässt. Mit vergleichbaren Vorfällen infolge einer Sammlung von Sicherheitslücken bei deutschen Behörden ist daher zu rechnen.

Werden die Risiken und die möglichen Erträge der staatlichen Infiltration informationstechnischer Systeme mithilfe von Zero-Days einander gegenübergestellt, so ergibt sich, dass dieser Infiltrationsweg ausgeschlossen werden muss.

Die durch die Nutzung und Geheimhaltung von Zero-Days eröffneten oder zumindest erhöhten Risiken wiegen äußerst schwer.

Zum einen kann der kriminelle Missbrauch der geheim gehaltenen Sicherheitslücken hochrangige Rechtsgüter empfindlich bedrohen. Nahezu alle lebenswichtigen Leistungen werden heute mit informationstechnischer Unterstützung erbracht. Ebenso verfügen so gut wie alle staatlichen und gesellschaftlichen Einrichtungen, deren Ausfall oder Funktionsstörung schwere Schäden verursachen kann, über informationstechnische Komponenten. Werden solche informations-

[18] Vgl. https://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung.
[19] Vgl. https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html.

11 technischen Komponenten gestört, so kann dies zu Leistungsausfällen oder Schadensereignissen führen, die schlimmstenfalls den Verlust von Menschenleben zur Folge haben können. Beispielsweise hat das Schadprogramm „WannaCry“, wie oben erwähnt, informationstechnische Systeme in britischen Krankenhäusern infiltriert. In der Folge mussten unter anderem geplante Operationen verschoben werden. Die Infiltration von Rechnern der Deutschen Bahn führte unter anderem zum Ausfall einer regionalen Leitstelle. Ein weiterer Angriff, der auf von der NSA erbeuteter Technologie basierte, hatte zur Folge, dass bei dem Arzneimittelunternehmen Merck ein kritischer Minderbestand eines Impfstoffs eintrat. Im September 2020 verstarb eine Patientin eines Wuppertaler Krankenhauses nach erfolgloser Behandlung. Sie hätte eigentlich in der Uniklinik Düsseldorf sein sollen, wo ihre Behandlung bereits eine Stunde früher als in Wuppertal hätte stattfinden können. Die Uniklinik war jedoch zu diesem Zeitpunkt aufgrund eines Ausfalls ihrer IT-Systeme von der Notfallversorgung abgemeldet. Hacker hatten eine Sicherheitslücke in der IT des Klinikums ausgenutzt, um 30 Server zu verschlüsseln und ein Lösegeld für deren Freigabe zu erpressen.[20]

Zum anderen erstreckt sich die Bedrohung durch den Missbrauch von Zero-Days auf praktisch die gesamte Bevölkerung, also ganz überwiegend auf Menschen, die für sicherheitsbehördliche Überwachungsmaßnahmen keinen Anlass geben. Es fehlt mithin vollständig an einer Zurechnungsbeziehung zwischen diesen Menschen und den Belangen, die der Geheimhaltung von Sicherheitslücken zugrunde liegen. Angesichts dessen und wegen der drohenden schweren Schäden ist die Grenze der Aufopferungspflicht der Betroffenen für das Gemeinwohl weit überschritten.

Hingegen wiegt der Effektivitätsverlust, der durch ein Verbot der Ausnutzung von Zero-Days für die Aufgabenerfüllung der Sicherheitsbehörden droht, weniger schwer. Dies gilt besonders für die Nachrichtendienste, die Überwachungsmaßnahmen anders als die Polizei nicht unmittelbar zur Abwehr konkreter Gefahren oder zur Verhütung von Straftaten einsetzen. Zwar hat der Beobachtungsauftrag des Verfassungsschutzes hohes Gewicht. Jedoch kann er zumeist auch auf weniger riskanten Wegen erreicht werden. So ist es aus objektiv-rechtlicher Sicht beispielsweise unbedenklich, wenn zur Infiltration des Zielsystems einer Quellen-Telekommunikationsüberwachung eine psychische Einflussnahme auf die Nutzer des Zielsystems *(Social Engineering)*, eine physische Zugriffsmöglichkeit auf das Zielsystem oder eine bereits bekannte, auf diesem System jedoch noch nicht geschlossene Sicherheitslücke ausgenutzt werden. Soweit im Einzelfall eine Infiltration auf diesen Wegen nicht möglich sein sollte, ist der damit verbundene Ausfall dieser Überwachungsmaßnahme hinzunehmen und auf andere, gegebenenfalls aufwändigere Maßnahmen auszuweichen.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verpflichtet die staatliche Gewalt mithin dazu, auf die Nutzung und Geheimhaltung von Zero-Days zum Zweck der Infiltration informationstechnischer Systeme zu verzichten. Es ist Sache des Gesetzgebers, diese Pflicht durch ein ausdrückliches gesetzliches Verbot umzusetzen.

---

[20] Vgl. https://heise.de/-4904134.

12 Nur durch ein ausdrückliches Verbot erhalten die Sicherheitsbehörden eine eindeutige Vorgabe, die das objektiv-grundrechtlich nicht hinzunehmende Risiko für die Sicherheit der informationstechnischen Infrastruktur der Bundesrepublik sicher ausschließt. Dass es einer solchen Vorgabe bedarf, illustriert beispielhaft die Antwort der Bundesregierung auf eine parlamentarische Kleine Anfrage, in der die Bundesregierung im Jahr 2018 mit Blick auf das Bundeskriminalamt eine Nutzung von Zero-Days zumindest nicht ausgeschlossen hat:

> „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."[21]

Selbst wenn entgegen der oben begründeten Auffassung eine staatliche Infiltration informationstechnischer Systeme mithilfe von noch unbekannten Sicherheitslücken verfassungsrechtlich überhaupt rechtfertigungsfähig wäre, müsste die gesetzliche Grundlage der Infiltration zumindest Vorgaben für ein behördliches Schwachstellen-Management enthalten. Nur aufgrund prozeduraler Sicherungen und materieller Kriterien für ein solches Schwachstellen-Management kann das enorme Risiko für die informationstechnische Infrastruktur der Bundesrepublik hinnehmbar sein. In diesem Rahmen wäre ein Bündel von maßstabsbildenden Faktoren zu beachten, etwa

- die Verbreitung der Sicherheitslücke:
  - in quantitativer Hinsicht: Zahl der betroffenen Nutzer*innen,
  - in qualitativer Hinsicht: Art der betroffenen Nutzer*innen,
- das Gewicht der Sicherheitslücke:
  - zur Ausnutzung erforderlicher Aufwand,
  - aus der Ausnutzung resultierender Schaden,
- die Wahrscheinlichkeit, dass Betroffene die Ausnutzung der Lücke bemerken und im Einzelfall Gegenmaßnahmen einleiten,
- die Wahrscheinlichkeit einer technischen Lösung für die Lücke,

---

[21] Antwort der Bundesregierung auf Fragen 26 bis 31 einer Kleinen Anfrage, BT-Drs. 18/13413. Die Antwort auf diese Fragen ist eingestuft, aber online zugänglich unter https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/#Antwort-Drucksache-18-13566-NfD.

13 – die Wahrscheinlichkeit einer Verbreitung der technischen Lösung,

– Möglichkeiten zur Linderung der Folgen bei einer (zeitweisen) Geheimhaltung der Lücke,

– die Wahrscheinlichkeit, dass Dritte die Lücke finden.[22]

Da es an derartigen Schutzregelungen in der vorgesehenen Ermächtigung zu Quellen-Telekommunikationsüberwachungen vollständig fehlt, steht sie insgesamt mit dem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme nicht in Einklang.

2. Zugriff auf gespeicherte Kommunikationsinhalte

Nicht mehr als Quellen-Telekommunikationsüberwachung darstellbar ist die in § 11 Abs. 1a Satz 2, Satz 3 Nr. 1 lit. b G 10-E vorgesehene Überwachung gespeicherter Kommunikationsinhalte.

Die eigenständige Regulierung der Quellen-Telekommunikationsüberwachung erklärt sich daraus, dass nach dem Bundesverfassungsgericht die Infiltration eines informationstechnischen Systems, mit deren Hilfe ausschließlich laufende Telekommunikation überwacht werden soll, materiell lediglich am Fernmeldegeheimnis des Art. 10 GG zu messen ist. Eine Ermächtigung zu Quellen-Telekommunikationsüberwachungen muss daher nicht den strengeren Anforderungen genügen, die sich für Online-Durchsuchungen aus dem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ergeben. Die Beschränkung des Überwachungszugriffs auf laufende Telekommunikation muss rechtlich und tatsächlich gewährleistet sein.[23]

Demgegenüber beschränkt sich die geplante Ermächtigung gerade nicht auf laufende Kommunikation. Die Nachrichtendienste sollen vielmehr auch lokal gespeicherte Kommunikationsinhalte auslesen dürfen, wenn diese ab dem Zeitpunkt der Anordnung der Maßnahme Gegenstand eines Kommunikationsvorgangs waren. Solche ehemaligen Kommunikationsinhalte unterfallen jedoch gerade nicht dem Fernmeldegeheimnis.[24] Sollen sie mit Hilfe einer Infiltration des informationstechnischen Systems erhoben werden, auf dem sie gespeichert sind, so handelt es sich verfassungsrechtlich um eine Online-Durchsuchung und nicht um eine Quellen-Telekommunikationsüberwachung. Dieses Ergebnis, das aus einer Zuordnung der Schutzbereiche von Art. 10 GG und Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG auf der Grundlage der Rechtsprechung des Bundesverfassungsgerichts folgt, überzeugt auch bei wertender Betrachtung. Soll die Überwachung auf ehemalige Kommunikationsinhalte erstreckt werden, so reicht es nicht aus, die Kommunikationssoftware lediglich so zu manipulieren, dass bei einem Kommunikationsvorgang die über-

---

[22] Vgl. Herpig, Schwachstellen-Management für mehr Sicherheit, 2018, abrufbar unter https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf.
[23] BVerfGE 120, 274 (308 f.).
[24] Vgl. BVerfGE 115, 166 (183 ff.); 120, 274 (307 f.); 124, 43 (54).

14 mittelten Inhalte zeitgleich an die Überwachungsbehörde ausgeleitet werden. Stattdessen müssen die auf dem Zielsystem gespeicherten Kommunikationsinhalte ausgelesen werden, um festzustellen, welche von ihnen im Zeitraum nach der Anordnung übermittelt und gespeichert wurden. Eine solche Auswertung der lokal gespeicherten Daten ist ein typisches Erkennungsmerkmal einer Online-Durchsuchung.

Die Ausweitung der Quellen-Telekommunikationsüberwachung zu einer „kleinen Online-Durchsuchung“ hat zur Folge, dass die vorgesehene Ermächtigung die verfassungsrechtlichen Anforderungen verfehlt. Unabhängig davon, dass der in Bezug genommene § 3 G 10 schon als Ermächtigung zu Telekommunikationsüberwachungen unzureichend ist (siehe sogleich unter 3), genügt diese Regelung den Anforderungen an Online-Durchsuchungen noch weniger. So ermöglicht § 3 Abs. 2 Satz 2 G 10 eine gezielte Überwachung sogenannter Nebenbetroffener.[25] Online-Durchsuchungen dürfen sich hingegen nur gegen die verdächtige Person richten.[26]

3. Allgemeine Defizite des Artikel 10-Gesetzes

Abgesehen von den originären Defiziten der vorgesehenen Ermächtigung zu Quellen-Telekommunikationsüberwachungen führt diese Ermächtigung die zahlreichen verfassungsrechtlichen Mängel fort, die schon das geltende Recht auszeichnen. Diese seien im Folgenden lediglich knapp und ohne Anspruch auf Vollständigkeit skizziert:

- Es ist fragwürdig, ob das G 10 mit der Kompetenzordnung in Einklang steht, soweit dieses Gesetz auch Telekommunikationsüberwachungen durch Landesverfassungsschutzbehörden regelt. Richtigerweise lässt sich dieser Regelungsumfang mit dem auf die Regelung der Zusammenarbeit von Bund und Ländern beschränkten Kompetenztitel des Art. 73 Abs. 1 Nr. 10 lit. b und c GG nicht vereinbaren.[27]
- Die in § 3 Abs. 1 G 10 geregelten Eingriffsvoraussetzungen sind in weitem Umfang zu weit und zu unbestimmt formuliert. Das Gesetz ermöglicht eine Telekommunikationsüberwachung teilweise bereits dann, wenn lediglich die Planung von vergleichsweise geringfügigen Straftaten im Raum steht. Zu nennen sind etwa das Verbreiten von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 3 G 10), die Zuwiderhandlung gegen ein Vereinsverbot (§ 20 Abs. 1 Nr. 1 bis 4 VereinsG, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 3 G 10) und die Zugehörigkeit zu einer geheim gehaltenen Vereinigung von Ausländern (§ 95 Abs. 1 Nr. 8 AufenthG, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 7 G 10). Darüber hinaus führt der Überwachungsansatz bereits im Planungsstadium im Zusammenwirken mit Straftatbeständen wie der Vorbereitung einer schweren staatsgefährden-

---

[25] Vgl. zum Begriff Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 3 G 10 Rn. 33.
[26] Vgl. BVerfGE 141, 220 (273 f.).
[27] Bäcker, DÖV 2011, S. 840 (844); ders., GSZ 2018, 213 (215 f.); Bergemann, NVwZ 2015, S. 1705 (1706); Pieroth, in: Jarass/Pieroth, GG, Art. 87 Rn. 5; a.A. Risse/Kathmann DÖV 2012, 555 ff.; Gärditz AöR 144 (2019), 81 (91 ff.); Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, Rn. 20 vor § 1 G 10.

15 den Gewalttat (§ 89a StGB, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 2 G 10) oder der Beteiligung an einer terroristischen Vereinigung (§ 129a StGB, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 6 lit. a G 10) zu einer weitreichenden Entgrenzung des tatsächlichen Überwachungsanlasses.

– Gleichfalls zu weit geraten sind die in § 4 Abs. 4 Satz 1 G 10 enthaltenen Ermächtigungen zur Übermittlung von Daten, die durch eine Überwachungsmaßnahme gewonnen wurden.

– Die Zurückstellung der grundrechtlich gebotenen Mitteilung an die betroffene Person wird in § 12 Abs. 1 Satz 2 G 10 deutlich zu pauschal und in zu weitem Umfang ermöglicht.