Anja Heinrich, Stefan Hügel

Staatstrojaner – Förderung oder Gefährdung der inneren Sicherheit?

Aktuell werden die Polizeiaufgabengesetze mehrerer Bundesländer novelliert – zuletzt unter anderem in Bayern, Nordrhein-Westfalen und Hessen. Gleichzeitig hat die Große *Koalition in ihrem Koalitionsvertrag angekündigt, ein* Musterpolizeigesetz *vorzulegen, an dem sich die Polizeigesetzgebung in den Ländern orientieren soll.*

Niedersachsen gehört zu den Ländern, die darauf nicht warten wollen. Die Fraktionen der Regierungskoalition in Hannover brachten einen Gesetzentwurf in den Landtag ein. Dieser Beitrag befasst sich mit der im Gesetzentwurf vorgesehenen Einführung von Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und Online-Durchsuchung. Er basiert in großen Teilen auf der schriftlichen Stellungnahme der Humanistischen Union[1] für die im August 2018 stattgefundene öffentliche Sachverständigenanhörung und verortet den niedersächsischen Gesetzentwurf in der gesamtdeutschen Entwicklung.

Entwicklung der Quellen-TKÜ und Online-Durchsuchung in Deutschland

Durch den zunehmenden Einfluss informationstechnischer Systeme auf den Alltag der Menschen bestehen auch Begehrlichkeiten der Sicherheitsbehörden, auf diese Systeme zuzugreifen, entweder um an die darauf gespeicherten Daten zu gelangen (Online-Durchsuchung) oder die darüber laufende verschlüsselte Kommunikation (z. B. Skype oder Messenger-Dienste) zu überwachen (Quellen-TKÜ). Lange war jedoch umstritten, ob die neu entwickelten Instrumente der Quellen-TKÜ und der Online-Durchsuchung auf bereits bestehende Ermächtigungsgrundlagen gestützt werden können, insbesondere auf die Standardbefugnisnormen zur Telekommuniktionsüberwachung. Ungeachtet dessen wendeten Polizei- und Verfassungsschutzbehörden die grundrechtsintensiven Maßnahmen sowohl zwecks Strafverfolgung als auch zur Gefahrenabwehr ohne spezielle Gesetzesgrundlage an. Im Januar 2007 entschied der 3. Strafsenat des Bundesgerichtshofs (BGH), dass die repressive Online-Durchsuchung weder auf die strafprozessuale Regelung zur Wohnraumdurchsuchung (§ 102 StGB) noch auf diejenige zur Telekommunikationsüberwachung (§ 100a StPO) gestützt werden kann, sondern eine spezielle Ermächtigungsgrundlage erforderlich ist. Zu diesem Zeitpunkt hatte der Gesetzgeber in Nordrhein-Westfalen für den Landesverfassungsschutz bereits eine Befugnisnorm für die Anwendung der Online-Durchsuchung geschaffen. Im Februar 2008 wurde diese seit 2006 bestehende Regelung vom Bundesverfassungsgericht in seinem berühmten, das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme begründenden Urteil, für nichtig erklärt.[2]

Die Entwicklung, die Geheimdienste und Polizeibehörden zu diesen Maßnahmen zu ermächtigen, setzte sich jedoch fort. Noch im selben Jahr der Entscheidung traten in Bayern Regelungen in Kraft, die der Landespolizei und dem Landesamt für Verfassungsschutz die Online-Durchsuchung erlauben. Seit Januar 2009 war das Bundeskriminalamt zwecks Terrorismusbekämpfung in der Lage, Online-Durchsuchung und Quellen-TKÜ durchzuführen. Es folgte Rheinland-Pfalz, das seine Polizei seit Februar 2011 zur Anwendung beider Instrumente ermächtigt und Sachsen-Anhalt, welches 2013 eine Regelung zur Online-Durchsuchung in sein Polizeigesetz einfügte. Letztere wurde ein Jahr später vom Landesverfassungsgericht für nichtig erklärt.[3] Die erfolgte Novellierung des BKA-Gesetzes führte im April 2016 zu einem zweiten wegweisenden Urteil des Bundesverfassungsgerichts (sog. BKAG-Urteil), in dem das Gericht wesentliche Grundsätze für heimliche Überwachungsmaßnahmen aufstellte, darüber hinaus auch die im damaligen BKA-Gesetz enthaltenen Regelungen zur Quellen-TKÜ und Online-Durchsuchung für unvereinbar mit der Verfassung erklärte und bestimmte, dass die beiden Befugnisnormen nur mit Einschränkungen bis zum 30.6.2018 fortgelten.[4] Der Bundesgesetzgeber kam seinem Auftrag zur Neuregelung mit dem im Mai 2018 in Kraft getretenen Gesetz zur Umstrukturierung des Bundeskriminalamtes nach. Das Gesetz folgte den bereits im August 2017 in Kraft getretenen, strafprozessualen Ermächtigungsgrundlagen, die zum Zwecke der Strafverfolgung nun auch die Ermittlungsbehörden zur Quellen-TKÜ und Online-Durchsuchung ermächtigen. Gegen die Regelungen wurden bereits mehrere Verfassungsbeschwerden eingelegt.[5]

Derzeit geht der Trend dahin, insbesondere den Werkzeugkasten der Polizeibehörden der Bundesländer mit den Instrumenten der Quellen-TKÜ und der Online-Durchsuchung auszustatten. Das Bundesinnenministerium hat einen Mustergesetzentwurf angekündigt, der das Vorbild für runderneuerte Landespolizeigesetze liefern und auch Standardbefugnisnormen für die Quellen-TKÜ und Online-Durchsuchung enthalten soll. In vielen Bundesländern hat jedoch der Gesetzgebungsprozess bereits eingesetzt. Baden-Württemberg hat die Quellen-TKÜ schon im Jahr 2017 eingeführt und Bayern und Hessen haben ihre Polizeigesetze in diesem Jahr gründlich überarbeitet. In beiden Bundesländern sind nun Quellen-TKÜ und Online-Durchsuchung möglich; zumindest gegen das bayerische Gesetz wurden ebenfalls bereits mehrere Verfassungsbeschwerden eingelegt. Auch in Bremen wollte die rot-grüne Koalition das Polizeigesetz noch in diesem Jahr überarbeiten, inklusive der Einführung der Quellen-TKÜ. Massiver Protest in der Bevölkerung hat jedoch dazu geführt, dass der grüne Koalitionspartner den bereits vorgelegten Gesetzentwurf nicht mittragen will und das Gesetzesvorhaben vorerst auf Eis gelegt wurde. Neben dem niedersächsischen Landtag befasst sich derzeit auch der Landtag in Nordrhein-Westfalen mit der Novellierung des Polizeigesetzes, inklusive der Einführung von Quellen-TKÜ und Online-Durchsuchung. Der derzeit im Sächsischen Landtag befindliche Gesetzentwurf zur Novellierung des Polizeigesetzes sieht zwar in vielen Teilen erhebliche Erweiterungen der polizeilichen Befugnisse vor, wie die Vorverlagerung der Standardbefugnisse ins Gefahrenvorfeld und die Einführung neuer Befugnisse wie sog. elektronische Fußfessel, auf die Quellen-TKÜ und Online-Durchsuchung soll jedoch auf Grund des Widerstands der SPD vorerst verzichtet werden.

Online-Durchsuchung und Quellen-TKÜ gefährden die Grundrechte

Vor dem Hintergrund, dass der Bundesgesetzgeber die Quellen-TKÜ als Instrument zur Abwehr terroristischer Gefahren gerade erst in das BKA-Gesetz eingefügt hat, stellt sich die Frage der tatsächlichen Notwendigkeit zusätzlicher Regelungen für die Landespolizeibehörden. In vielen Bundesländern hat nicht nur die Skepsis gegen die Einführung neuer grundrechtsintensiver Maßnahmen, sondern gerade auch die in Frage stehende tatsächliche Notwendigkeit solcher Regelungen zu erheblichem Widerstand und massiver Kritik geführt. Die Niedersächsische Landesdatenschutzbeauftragte, Barbara Thiel, hat zu dem niedersächsischen Gesetzentwurf in der öffentlichen Anhörung ebenfalls sehr kritisch Stellung bezogen. Ein Statement auf ihrer Homepage fasst ihre Kritik zusammen:

> *„Unter dem Deckmantel, den internationalen Terrorismus zu bekämpfen, beschneiden die vorgeschlagenen Regelungen die Freiheitsrechte der Bürgerinnen und Bürger bis zur Unkenntlichkeit. Aus dem Gesetzentwurf wird nicht ansatzweise erkennbar, warum derartige Verschärfungen erforderlich sind. Keine der einzelnen neuen Überwachungsmaßnahmen wird ausführlich begründet. Das betrifft insbesondere die Maßnahmen der elektronischen Fußfessel, Quellen-Telekommunikationsüberwachung (TKÜ) und Online-Durchsuchung. Ich habe vielmehr den Eindruck, dass alle verfassungsrechtlichen Möglichkeiten zur Stärkung der inneren Sicherheit auf Biegen und Brechen ausgeschöpft werden sollen, ohne dabei die Freiheitsrechte angemessen zu berücksichtigen."*[6]

Zu der berechtigten Kritik an der äußerst fraglichen Notwendigkeit stetiger grundrechtsintensiver Befugniserweiterungen kommt hinzu, dass es gegen die Einführung der Quellen-TKÜ und der Online-Durchsuchung aufgrund vieler technischer und rechtlicher Unwägsamkeiten insgesamt erhebliche Bedenken gibt.

Grenzen rechtlicher Regelbarkeit

Fehlende Eingrenzbarkeit der Quellen-TKÜ

Bedenken begründet besondere die Tatsache, dass die Regelungen zur Quellen-TKÜ formal zwar lediglich zur Überwachung der laufenden Kommunikation ermächtigen, jedoch erhebliche Zweifel an der Eingrenzbarkeit der Maßnahme bestehen.

Die technischen Schritte zur Aufbringung von Software für die Quellen-TKÜ sind mit denjenigen für die Online-Durchsuchung weitgehend identisch.[7] Für die für derartige Eingriffe verwendete *Remote Forensic Software*[8] hat sich in der politischen Debatte mittlerweile die Bezeichnung *Staatstrojaner*[9] eingebürgert. Inwieweit die Staatstrojaner derart programmiert werden können und in der Praxis dann auch derart programmiert werden, dass sie bei einer Maßnahme zur Telekommunikationsüberwachung keine weiteren Daten aus dem informationstechnischen System erfassen, ist zweifelhaft. Am 8. Oktober 2011 veröffentlichte der Chaos Computer Club (CCC) eine Analyse[10] eines Programms zur Quellen-TKÜ und deckte dabei auf, dass das untersuchte Programm über weit mehr Fähigkeiten verfügt als die Überwachung der Telekommunikation. Dazu gehörte das Erstellen von Bildschirmfotos, das Nachladen von beliebigen Programmen aus dem Internet sowie der Mitschnitt von Tastaturanschlägen. Zudem konnten auch einfache Daten wie Bilder auf den Computer aufgespielt werden.

Eingrenzbarkeitsprobleme entstehen zudem dadurch, dass technisch nicht zuverlässig zwischen Kommunikations- und anderen Prozessen auf dem Rechnersystem unterschieden werden kann. Denn bei der Quellen-TKÜ werden zur Überwachung der verschlüsselten Kommunikation die Daten (z. B. eine E-Mail) vor der Verschlüsselung und damit in einem Zeitpunkt abgefangen, zu dem weder der Trojaner erkennen kann noch der Verfasser vielleicht selbst weiß, ob die Daten später tatsächlich versendet werden. So werden bei der Überwachung des E-Mail-Verkehrs insbesondere auch alle Entwürfe unabhängig von ihrer späteren Versendung erfasst.[11]

Erfassung kernbereichsrelevanter Daten bei der Online-Durchsuchung unvermeidbar

Das Bundesverfassungsgericht hat festgestellt, dass die Online-Durchsuchung anders als andere Überwachungsmaßnahmen keine Überwachung eines zeitlich gegliederten Geschehens an verschiedenen Orten darstellt, sondern dass der Zugriff stets auf ein gesamtes System erfolgt und dass damit in Bezug auf den Zugriff weitgehend nur die Alternativen von ganz oder gar nicht bestehen. Damit existiert faktisch keine Möglichkeit, Betroffene vor dem Zugriff auf kernbereichsrelevante – also höchstpersönliche, der Menschenwürde zuzuordnende – Informationen zu schützen. Als Konsequenz ist das Bundesverfassungsgericht in Bezug auf die Online-Durchsuchung von seinem vormals entwickelten 2-stufigen Schutzkonzept[12] abgewichen. Nach dem 2-stufigen Schutzkonzept hat der Schutz des Kernbereichs privater Lebensgestaltung bei heimlichen Überwachungsmaßnahmen sowohl bei der Datenerhebung (1. Stufe) als auch bei der Datenverarbeitung (2. Stufe) zu erfolgen. So ist der Gesetzgeber auf der 1. Stufe der Datenerhebung gehalten, Schutzmaß-

Nein zum Polizeigesetz: 7. Juli 2018 Großdemo Düsseldorf Landesverband NRW von Bündnis 90/Die Grünen, CC BY-SA 2.0

nahmen vorzusehen, die verhindern, dass kernbereichsrelevante Daten überhaupt erst erhoben werden. Auf der 2. Stufe hat er zu regeln, dass höchstpersönliche Daten, die trotz dieser Schutzvorkehrung gleichwohl versehentlich erhoben worden sind, unverzüglich zu löschen sind. In Bezug auf die Online-Durchsuchung hat das Bundesverfassungsgericht jedoch zuletzt festgestellt, dass Schutzmaßnahmen vor Kernbereichsverletzungen nicht primär auf die Verhinderung der Erfassung und des Festhaltens höchstpersönlicher Daten zielen, sondern auf die Verhinderung des Auslesens dieser Informationen und hat damit den notwendigen Kernbereichsschutz auf der Erhebungsebene weitgehend zurückgefahren.[13] Die Anpassung der bundesverfassungsgerichtlichen Rechtsprechung an die Besonderheiten der Online-Durchsuchung hat die mit ihr verbundenen Zugriffe auf höchstpersönliche Informationen zwar rechtlich legitimiert, hat jedoch gleichzeitig die massiven Bedenken ihrer Kritiker bestätigt. Denn Fakt bleibt: Ein Zugriff auf höchst persönliche Informationen, wie Tagebuchaufzeichnungen, ist bei der Online-Durchsuchung kaum verhinderbar und Schutzmaßnahmen, die erst auf der Stufe der Datenverarbeitung und -verwendung greifen, können die bei der Datenerhebung eingetretenen Kernbereichsverletzungen lediglich noch kompensieren. Ein effektiver Schutz der Intimsphäre von Betroffenen muss daher nun zwar nicht mehr rechtlich, aber faktisch weiterhin bei der Datenerhebung ansetzen. D. h. bereits die Erhebung höchstpersönlicher Informationen ist zu unterlassen.[14]

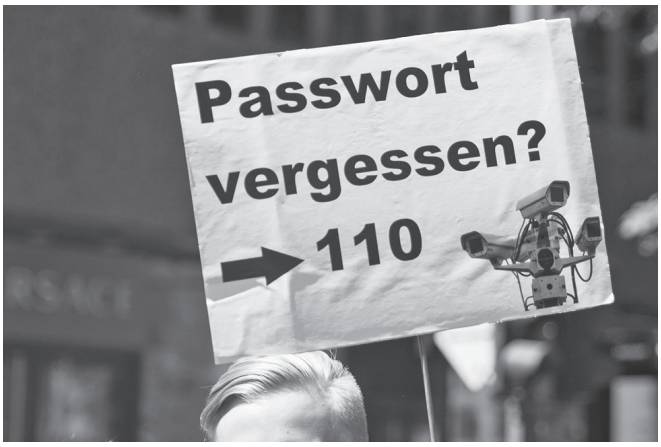
Rechtliche Grauzonen des Staatstrojaners

Es stellt sich zudem die Frage des Einsatzes – wie kann die Überwachungssoftware in rechtmäßiger Art und Weise auf die entsprechenden Rechnersysteme aufgespielt und aktiviert werden? Offensichtlich ist die Maßnahme nur sinnvoll, wenn der Zielperson die Tatsache ihrer Überwachung nicht bekannt ist, da sie sonst ihr Verhalten anpassen würde. Grundsätzlich sind drei Wege der Infiltration denkbar:

- Installieren der Software im Rahmen kurzzeitiger Verfügung über den zu überwachenden Rechner, in einem unbeobachteten Moment während einer Sicherheitskontrolle am Flughafen,
- Eindringen in die Wohnung der Zielperson, um an den Rechner zu gelangen – dies ist aber rechtlich kaum möglich, ohne dass die Zielperson Kenntnis davon erlangt,
- Nutzen von Trojanersoftware – dies ist in der Praxis unserer Einschätzung nach der häufigste Weg und wird im Folgenden den schwerpunktmäßig behandelt.

Keine Rechtsgrundlagen für den physischen Zugriff auf das informationstechnische System

Die *Remote Forensic Software* kann durch unmittelbaren physischen Zugriff auf dem informationstechnischen System installiert werden. „Nur auf diese Weise kann – was gelegentlich übersehen wird – ausgeschlossen werden, dass beispielsweise Rechner von unbeteiligten Dritten ebenfalls in den Fokus der Ermittler geraten".[15] Häufig wird ein solcher Zugriff am Aufbewahrungsort des informationstechnischen Systems erfolgen müssen. Bei Rechnern ist dies i. d. R. die Wohnung. Der damit unmittelbar verbundene Eingriff in die Unverletzlichkeit der Wohnung, Art. 13 Abs. 1 GG, kann jedoch schon deshalb nicht rechtmäßig erfolgen, weil es hierfür schlicht an entsprechenden Gesetzesgrundlagen fehlt. Entsprechendes gilt für die Mitnahme des informationstechnischen Systems unter einem Vorwand und das dabei erfolgende Aufspielen der Software.



Nein zum Polizeigesetz: 7. Juli 2018 Großdemo Düsseldorf Landesverband NRW von Bündnis 90/Die Grünen, CC BY-SA 2.0

Erfolgt der Zugriff und das Aufspielen der Software auf das System dagegen extern über eine Online-Verbindung, setzt dies voraus, dass es im Zielsystem eine Schwachstelle gibt, die für die Maßnahme genutzt werden kann. Solche Schwachstellen werden durch *Exploits*[16] ausgenutzt. Damit sind Strafverfolgungsbehörden nicht anders als das kriminelle Millieu darauf angewiesen, Schwachstellen bzw. die auf ihnen fußenden Exploits für die Quellen-TKÜ bzw. Online-Durchsuchung zu nutzen. In diesem Sinn sind Staatstrojaner nichts anderes als ein Schadcode, der auf dem zu infiltrierenden System installiert wird. Um die Wahrscheinlichkeit für den Erfolg der Maßnahme zu erhöhen, werden insbesondere Zero-Day-Exploits benötigt. Die Schwachstellen können durch entsprechende Analysen selbst *entdeckt* oder auf dem Schwarzmarkt *erworben* werden. Aufgrund des Aufwands für die Entdeckung von Schwachstellen und Entwicklung von Exploits wird es in der Praxis häufig zum Kauf kommen. Eine weitere Möglichkeit ist das bewusste Schaffen von Schwachstellen durch staatliche Stellen, beispielsweise durch die Standardisierung schwacher Sicherheitsstandards.

Alle Methoden führen dazu, dass bewusst und vorsätzlich Schwachstellen geschaffen oder aufrecht erhalten werden, die auch durch Dritte – beispielsweise in krimineller oder terroristischer Absicht – ausgenutzt werden können. Neben dem unmittelbaren Risiko der Nutzung untergräbt dies langfristig die Vertrauenswürdigkeit und damit die Funktionsfähigkeit der technischen Infrastruktur. Eine sichere Infrastruktur ist nicht zuletzt für Wirtschaftsunternehmen von hoher Bedeutung, um ihre geschäftlichen Transaktionen sicher abzuwickeln und Akzeptanz für die Digitalisierung der Wirtschaft zu schaffen. Das damit verbundene Ziel, keine Angriffsflächen für die Verursachung von Datenpannen oder Wirtschaftsspionage zu bieten, wird durch Staatstrojaner konterkariert.

Die Folge ist, dass durch das Offenhalten von Schwachstellen potenziell Terroristen ein Werkzeug in die Hand gegeben wird, durch das sie weiteren, erheblichen Schaden verursachen können, der möglicherweise den durch einen Ermittlungserfolg verhinderten Schaden bei Weitem übersteigt.[17] Ein Beispiel für eine Schadsoftware, die solchen Schaden verursachen kann, ist der *Ransomware-Trojaner WannaCry*[18], der 2017 unter anderem Systeme des britischen National Health Service und der Deutschen Bahn befallen und für erhebliche Beeinträchtigungen gesorgt hat. Der zugrundeliegende Exploit stammte aus dem Fundus der US-amerikanischen National Security Agency. Das Beispiel zeigt, dass die Kompromittierung von IT-Systemen nicht auf bestimmte Nutzungsweisen eingeschränkt werden kann.[19] Durch den Ankauf von Schwachstellen und Exploits sorgen staatliche Stellen zudem dafür, dass ein lukrativer Schwarzmarkt etabliert und gefördert wird, da sie für die notwendige Nachfrage sorgen bzw. sie fördern. Dies trägt zusätzlich dazu bei, die öffentliche Infrastruktur nachhaltig zu gefährden.[20] Der Staat begibt sich damit insgesamt in einen erheblichen Zielkonflikt: Durch die Nutzung von Software zum Eingriff in informationstechnische Systeme zur Verhinderung von Straftaten fördert er die Möglichkeit von Straftaten gleichzeitig in erheblichem Maß.[21]

Zu den technischen Rahmenbedingungen nimmt eine aktuelle Studie der *Stiftung Neue Verantwortung* Stellung.[22] Der Autor der Studie entwirft einen Prozess für das Schwachstellen-Management, nach dem beim Umgang mit Schwachstellen vorgegangen und entschieden werden soll. Der Vorschlag enthält vier Elemente:

- Institutioneller Aufbau und Workflow,
- Beurteilung der Schwachstellen,
- Management der Schwachstellen,
- Schutz- und Kontrollmaßnahmen.

Der Prozess soll durch ein Sekretariat gesteuert werden, das auch die Entscheidung zwischen Zurückhalten oder Offenlegung einer Schwachstelle koordiniert. Der Vorschlag sieht auch mehr Transparenz, unter anderem durch parlamentarische Kontrolle, vor.

Ob dies tatsächlich die Sicherheitsprobleme zu lösen imstande ist, erscheint zweifelhaft. Probleme wie die Schaffung eines Schwarzmarkts für Schwachstellen und Exploits werden durch den Vorschlag nicht adressiert. Die Prämisse, dass in einem rechtlichen Graubereich wie dem Handel mit Schwachstellen nach festgelegten Prozeduren und vertraglichen Vereinbarungen vorgegangen wird, wirkt naiv. Es ist wohl auch kaum vorstellbar, dass eine nachrichtendienstliche Behörde Schwachstellen – wie in der Studie unterstellt – auf dem Schwarzmarkt ankauft, nur um sie danach auf Empfehlung eines unabhängigen Gremiums sogleich offenzulegen. Zurückgehaltene Schwachstellen stellen stets eine Gefahr für die öffentliche Sicherheit dar – neben dem Risiko, dass die Information darüber durch die nutzende Behörde selbst an die Öffentlichkeit gerät, kann sie auch durch andere Akteure gefunden und anschließend genutzt werden. Eine parlamentarische Kontrolle ist zwar wünschenswert aber nicht besonders erfolgversprechend, nachdem die Kontrolle der Nachrichtendienste in der heutigen Form wohl als gescheitert zu betrachten ist[23].

Manipulation, Dokumentation, Missbrauch

Die Rechtmäßigkeit der verwendeten Software lässt sich nicht sicherstellen

Der Gesetzentwurf fordert für eine Maßnahme der Online-Durchsuchung sowie der Quellen-TKÜ eine richterliche Anordnung bzw. bei Gefahr im Verzug die Anordnung eines dazu befugten Polizeibeamten. Dafür ist es u. a. erforderlich, dass die Rechtmäßigkeit der für die Maßnahme verwendeten Software geprüft wird.

Diese Prüfung der Rechtmäßigkeit kann nur in Kenntnis der Funktionsweise der Software und damit des Quelltexts durch sachkundige Experten erfolgen. Um die Rechtmäßigkeit sicherzustellen, ist beispielsweise eine Zertifizierung durch eine unabhängige Zertifizierungsstelle erforderlich. Diese müsste für jedes Release erneuert werden, da jede Änderung prinzipiell der Software neue rechtswidrige Funktionalität hinzufügen kann.

Durchsuchungsergebnisse können manipuliert werden

Die Kompromittierung eines IT-Systems ermöglicht weitergehende Manipulation bis hin zur Ablage kompromittierender Dateien auf dem System der Zielperson. Ebenso wie die Ermittlungspersonen sind die zu überwachenden Zielpersonen technisch prinzipiell in der Lage, die Ermittlungsergebnisse in ihrem Sinne zu manipulieren.[24] Damit haben die erhobenen Daten keine forensische Beweiskraft.

Die Eingriffe in die informationstechnischen Systeme müssten rechtssicher dokumentiert werden

Wegen der mit dem Einsatz von Staatstrojanern verbundenen, äußerst weitgehenden Eingriffsmöglichkeiten müssten zur Gewährleistung von Transparenz und Kontrolle Eingriffe in informationstechnische Systeme stets dokumentiert werden. Die Möglichkeit zur rechtssicheren Dokumentation auf einem fremden System ist jedoch in der Regel sehr eingeschränkt, denn dieses System kann manipuliert werden, weil es in den meisten Fällen nicht vollständig durch die Ermittlungsbeamten kontrolliert wird.

Auch die kryptographische Absicherung solcher Protokolle kann die Authentizität nicht gewährleisten. Auf die dafür benötigten Schlüssel kann auch das infiltrierte System zugreifen.

Regelungen zur Quellen-TKÜ und Online-Durchsuchung in Niedersachsen und Kritikpunkte an der dortigen Ausgestaltung der Maßnahmen

Niedersachsen ist auf dem Weg, die Quellen-TKÜ und die Online-Durchsuchung als Standardbefugnis für die Polizei zur Gefahrenabwehr einzuführen. Die allgemeinen Kritikpunkte, die es an der Einführung solcher Instrumente gibt, muss daher auch Niedersachsen gegen sich gelten lassen. Außerdem ist die spezielle gesetzliche Ausgestaltung der Regelungen mangelhaft, die die niedersächsische Polizei zur Quellen-TKÜ und Online-

Durchsuchung ermächtigen sollen. Das erhöht die Eingriffsintensität der Maßnahmen zusätzlich und wirft Bedenken bezüglich ihrer Verfassungsmäßigkeit auf.

Sowohl die Quellen-TKÜ als auch die Online-Durchsuchung reichen tief in das Privatleben der betroffenen Personen hinein und stellen einen schwerwiegenden Eingriff in das verfassungsrechtlich geschützte Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) dar. Die Anforderungen an die gesetzliche Ausgestaltung sind entsprechend hoch. Welche konkreten verfassungsrechtlichen Anforderungen an heimliche Überwachungsmaßnahmen wie die Quellen-TKÜ und die Onlinedurchsuchung zu stellen sind, hat das Bundesverfassungsgericht in seinem BKAG-Urteil aufgezeigt. Danach müssen die Maßnahmen auf den Schutz oder die Bewehrung hinreichend gewichtiger Rechtsgüter begrenzt sein, eine Gefährdung dieser Rechtsgüter muss hinreichend konkret absehbar sein, und sie dürfen sich nur unter eingeschränkten Bedingungen auf nichtverantwortliche Dritte aus dem Umfeld der Zielperson erstrecken. Erforderlich sind zudem besondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung sowie der Schutz von Berufsgeheimnisträgern. Solche Regelungen unterliegen Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle und müssen mit Löschpflichten bezüglich der erhobenen Daten flankiert sein.

Eingriffsschwellen und Eingriffsbefugnisse

Eingriffsschwelle zu weit und zu unbestimmt

Für heimliche Überwachungsmaßnahmen hat das Bundesverfassungsgericht in seinem BKA-Urteil Minimalanforderungen an die Eingriffsschwelle festgelegt. Für solche Maßnahmen, wie die Quellen-TKÜ und die Online-Durchsuchung, muss zwar keine konkrete Gefahr i. S. d. Polizeirechts vorliegen, wenn sie dem Schutz überragend wichtiger Rechtsgüter dienen. Es sind aber mindestens „tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr" nötig. Damit verzichtet das Bundesverfassungsgericht für den Schutz überragend wichtiger Rechtsgüter auf das Vorliegen einer hinreichenden Wahrscheinlichkeit des Schadenseintritts, fordert aber gleichwohl eine gewisse Konkretisierung ein. Zwei Konkretisierungen sind möglich: Entweder (1) muss es die geforderten tatsächlichen Anhaltspunkte geben, die auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen schließen lassen, sowie darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest soviel bekannt ist, dass die Überwachungsmaßnahmen gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden können. Oder (2) das individuelle Verhalten einer Person begründet die konkrete Wahrscheinlichkeit, dass sie in überschaubarer Zukunft terroristische Straftaten begehen wird.

Die im niedersächsischen Gesetzentwurf geregelten Voraussetzungen für die Quellen-TKÜ und die Online-Durchsuchung entsprechen in ihrem Wortlaut zwar in weiten Teilen den Ausführungen des Bundesverfassungsgerichts, in Bezug auf die Online-Durchsuchung gab es jedoch eine wesentliche Änderung. Sie steht im neuen § 33d im Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung. Online-Durchsuchungen sollen u. a. dann zulässig sein, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums Leib, Leben oder Freiheit einer Person schädigen wird. Außerdem sollen Online-Durchsuchungen dann zulässig sein, wenn das so beschriebene Verhalten Rechtsgüter schädigen wird, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschheit berührt. Damit weicht der Gesetzentwurf vom Erfordernis der terroristischen Straftat ab. Denn die mögliche Gefährdung der im Gesetzentwurf aufgezählten gewichtigen Rechtsgüter stellt nicht automatisch auch eine mögliche Gefahr einer terroristischen Straftat dar. Für eine terroristische Straftat wird man zusätzlich zumindest auch immer eine politische, staatsfeindliche und umstürzlerische Absicht des Täters verlangen müssen. Die bloße Verletzung der im Gesetzentwurf genannten Rechtsgüter erfüllt diese Voraussetzung nicht.

Darüber hinaus stellt sich die Frage, ob die im Gesetzentwurf für die Quellen-TKÜ und Online-Durchsuchung definierten Eingriffsvoraussetzungen dem Bestimmtheitsgebot genügen. Fraglich ist insbesondere, ob BürgerInnen vorhersehen und Rechtsanwender und Gerichte feststellen können, wann die (Geschehens-)Weise einer Straftat zumindest „ihrer Art nach konkretisiert" ist. Indem der niedersächsische Gesetzentwurf in weiten Teilen Begrifflichkeiten aus dem BKA-Urteil des Bundesverfassungsgerichts quasi im Wege des Copy-and-Paste wiederverwendet, genügt er nicht automatisch dem verfassungsrechtlichen Bestimmtheitsgebot. Denn während es lediglich Aufgabe des Bundesverfassungsgerichts ist, dem Gesetzgeber allgemeingültige Grenzen der Einschränkbarkeit eines Grundrechts aufzuzeigen, ist es Aufgabe des Gesetzgebers, die Eingriffsvoraussetzungen für die Anwendung im Einzelfalls hinreichend bestimmt auszugestalten. Der Gesetzgeber muss die Eingriffsvoraussetzungen so klar definieren, dass die Bürger Eingriffe in ihre Grundrechte vorhersehen können, die Rechtsanwender (Polizis-

Anja Heinrich und Stefan Hügel

Anja Heinrich ist Rechtsanwältin in Berlin und Mitglied im Bundesvorstand der *Humanistischen Union*. Seit einigen Jahren befasst sie sich insbesondere auch mit präventiv-polizeilichen Befugnissen und deren Rechtmäßigkeit.

Stefan Hügel, Diplom-Informatiker, ist Vorsitzender des FIfF und Mitglied des Bundesvorstands der Humanistischen Union. Beruflich arbeitet er als Berater für IT-Prozesse. Er lebt in Frankfurt am Main.

ten und andere) die Maßnahmen anwenden und die Gerichte diese Maßnahmen überprüfen können. In Bezug auf den Gesetzentwurf stellt sich daher die Frage, ob der Gesetzgeber, der den Begriff der terroristischen Straftat in § 2 seines Gesetzentwurfs definiert hat, vor dem Hintergrund des Bestimmtheitsgebotes nicht auch definieren muss, wann die (Geschehens-) Weise eine derartigen terroristischen Straftat im Einzelfall „ihrer Art nach konkretisiert ist".

Fehlender Richtervorbehalt bei der Quellen-TKÜ

Bei der Quellen-TKÜ hat es die Regierungsfraktion zudem versäumt, die Maßnahme unter den Vorbehalt einer richterlichen Anordnung zu stellen. Das Urteil des Bundesverfassungsgerichts zum BKA-Gesetz verlangt eine richterliche Anordnung oder eine anderweitige unabhängige vorherige Kontrolle für eingriffsintensive heimliche Überwachungsmaßnahmen, bei denen damit zu rechnen ist, dass auch höchst private Informationen erfasst werden. Der Gesetzgeber hat hierbei zu normieren, dass es vor der Datenerhebung einer gerichtlichen Anordnung mit strengen Anforderungen an Inhalt und Begründung sowie eines hinreichend substantiierten sowie hinreichend begründeten Antrags auf eine solche Anordnung bedarf. Der Gesetzentwurf regelt den Richtervorbehalt für die TKÜ in § 32 Abs. 6 und 7 NPOG-E. Kein Richtervorbehalt ist für die Quellen-TKÜ vorgesehen. Ein Verweis in § 32 Abs. 6 auf § 33a Abs. 2 NPOG-E fehlt.

Fehlende Eingrenzung der zulässigen Maßnahmen

Wer die Rechtsfolgen betrachtet, wünscht sich bei so schwerwiegenden Eingriffen mindestens, dass die neuen Befugnisse die Polizei nicht nur pauschal ermächtigen. Sie darf in „von der betroffenen Person genutzte informationstechnische Systeme"[25] zwecks Überwachung der Telekommunikation (Quellen-TKÜ) oder der Erhebung von Daten (Online-Durchsuchung) eingreifen. Der Gesetzgeber hätte die informationstechnischen Systeme, bei denen ein Eingriff zulässig sein soll, benennen oder zumindest in anderen näheren Bestimmungen eingrenzen müssen. Denn in seiner jetzigen Form erfassen die Befugnisnormen Eingriffe in alle denkbaren informationstechnischen Systeme, d. h. vom PC übers Handy bis hin zum IT-gesteuerten Herzschrittmacher. Durch aktuelle informationstechnische Konzepte wie *Cloud Computing*, *Internet of Things*, *Smart City* oder *Industrie 4.0* ist der Kreis informationstechnischer Systeme, auf die durch die neuen Befugnisnormen zugegriffen werden kann, enorm weit.

Bedauernswert ist zudem, dass der Gesetzentwurf weder für die TKÜ noch für die Quellen-TKÜ eine zeitliche Höchstgrenze vorsieht. Die Maßnahme kann immer wieder um jeweils drei Monate verlängert werden. Damit wird dem Grunde nach eine unbegrenzte, also jahre- oder gar jahrzehntelange Überwachung von Telefonaten, E-Mails, SMS, Messengerdienstnachrichten und allen anderen informationstechnischen Systemen ermöglicht.

Schutz des Kernbereichs privater Lebensgestaltung

Überwachungsmaßnahmen sind stets verfassungswidrig, wenn sie den Kernbereich privater Lebensgestaltung nicht hinreichend beachten und damit in die Menschenwürde der Betroffenen eingreifen. Können Überwachungsmaßnahmen typischerweise zur Erhebung kernbereichsrelevanter Daten führen, ist der Gesetzgeber verpflichtet, die Befugnisnormen mit Regelungen zu flankieren, die einen wirksamen Schutz gewährleisten.[26] Zu den kernbereichsnahen Überwachungsmaßnahmen gehören auch die Quellen-TKÜ und die Online-Durchsuchung.

Kernbereichsschützende Regelungen finden sich für alle kernbereichsnahen Überwachungsnormen zentral in § 31b des Gesetzentwurfs. In Bezug auf die Quellen-TKÜ und die Online-Durchsuchung weist § 31b jedoch erhebliche Defizite auf und wird den Anforderungen, die an einen verfassungsmäßig ausgestalteten Kernbereichsschutz zu stellen sind, nicht vollends gerecht.

Keine technischen Sicherungen für die Online-Durchsuchung vorgesehen

Nach dem Bundesverfassungsgericht hat der Gesetzgeber auf der Ebene der Datenerhebung Vorkehrungen zu treffen, die eine unbeabsichtigte Miterfassung von zum Kernbereich gehörenden Informationen nach Möglichkeit ausschließen.[27] Insbesondere muss der Gesetzgeber durch eine vorgelagerte Prüfung sicherstellen, dass die Erfassung von kernbereichsrelevanten Situationen und Gesprächen jedenfalls insoweit ausgeschlossen ist, als sich diese mit praktisch zu bewältigendem Aufwand im Vorfeld vermeiden lässt.[28] Bei der Online-Durchsuchung, bei der eine Nichterhebung von kernbereichsrelevanten Daten praktisch nicht ausschließbar ist, ist gesetzlich zu regeln, dass die Erhebung höchstpersönlicher Daten jedenfalls dann zu unterbleiben hat, wenn dies durch informationstechnische und ermittlungstechnische Mittel verhindert werden kann. Verfügbare informationstechnische Sicherungen, mit deren Hilfe höchstvertrauliche Informationen aufgespürt und isoliert werden können, sind dabei zu verwenden.[29] Ein solcher Einsatz von technischen Sicherungen zur Vermeidung der Erhebung kernbereichsrelevanter Daten ist in § 31b Abs. 1, der den Kernbereichsschutz für die Ebene der Datenerhebung im Wesentlichen regelt, nicht vorgesehen.

Mangelhafte Regelung zum Abbruch der Datenerhebung und zur Protokollierung bei Datenlöschung

Ein verfassungsmäßiger Kernbereichsschutz auf der Ebene der Datenerhebung setzt zusätzlich für alle Arten von Maßnahmen voraus, dass das Gesetz den Abbruch der Datenerhebung vorsieht, wenn erkennbar ist, dass die Überwachung den Kernbereich berührt.[30] Im niedersächsischen Gesetzentwurf ist mit § 31b Abs. 2 zwar eine solche Unterbrechung der Datenerhebung vorgesehen, die Regelung verengt die Pflicht zum Abbruch jedoch in nicht verfassungskonformer Weise, weil sie Ausnahmen vorsieht. Die Ausnahmen von der Pflicht zur Unterbrechung der Datenerhebung sollen gelten, wenn diese informationstechnisch nicht möglich ist oder durch die Unterbrechung dem/der Betroffenen die Datenerhebung bekannt wird. Diese Ausnahmen genügen nicht den Vorgaben des Bundesverfassungsgerichts, das beim erkennbaren Eindringen in den Kernbereich „in jedem Fall"[31] den Abbruch der Maßnahme vorsieht.

Für die Fälle, dass kernbereichsrelevante Daten trotz aller Vorkehrungen erhoben worden sind, hat das ermächtigende Gesetz sofortige Löschung der Daten vorzusehen. Zudem hat das Gesetz zu regeln, dass die Löschung in einer Art und Weise proto-

kolliert wird, die eine spätere Kontrolle ermöglicht.[32] Der niedersächsische Gesetzentwurf sieht in § 32 b Abs. 2 S. 3 NPOG-E für solche Fälle vor, dass „die Tatsache, dass Daten aus dem Kernbereich privater Lebensgestaltung erhoben wurden, und die Löschung dieser Daten […] zu dokumentieren" sind. Diese Regelung dürfte jedoch unzureichend sein, denn allein die Dokumentation der Tatsache der Datenerhebung und der Löschung ermöglichen im Nachhinein keine Kontrolle. Für eine spätere Kontrolle dürfte vielmehr erforderlich sein, dass zumindest auch der Zeitpunkt der Löschung und die Person, die die Löschung vorgenommen hat, protokolliert werden.

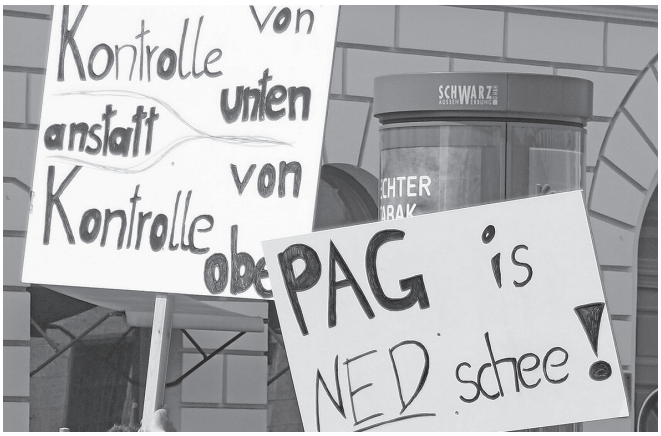
Unzureichende Sichtung

Auf der Ebene der Auswertung und Verwertung der erhobenen Daten fordert das Bundesverfassungsgericht für den Fall, dass die Erfassung von kernbereichsrelevanten Daten nicht vermieden werden konnte, in der Regel die Sichtung der erfassten Daten durch eine unabhängige Stelle im Gesetz vorzusehen.[33] Da bei der Online-Durchsuchung immer auch kernbereichsrelevante Daten miterfasst werden, sieht es eine solche Sichtung hier als zwingend an.[34] Das Ziel dieser vorgeschalteten Sichtung ist sowohl das Herausfiltern von Daten als auch die Gewährleistung einer unabhängigen Kontrolle der dem Kernbereichsschutz dienenden Anforderungen insgesamt (Rechtmäßigkeitskontrolle).[35] Diesem Maßstab wird der Gesetzentwurf nicht in vollem Umfang gerecht, weil er in § 32b Abs. 4 lediglich regelt, dass eine gerichtliche Entscheidung darüber zu ergehen hat, „ob Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erhoben wurden". Zum einen lässt diese Regelung vermissen, dass das Gericht auch eine Gesamtschau bezüglich der Rechtmäßigkeit vorzunehmen hat. Zum anderen sollte die Regelung zwecks Normenklarheit ausdrücklich anordnen, dass gegebenenfalls gefundene höchstpersönliche Daten herauszufiltern sind, bevor die Aufzeichnungen an die Polizeibehörden übermittelt werden. Eine verfassungsrechtliche Ausgestaltung der Datenerhebung erfordert, dass die Sicherheitsbehörden zeitweise von einem Zugriff auf die Daten abgeschnitten werden. In dieser Zeit erfolgt eine externe Prüfung der Rechtmäßigkeit der Datenerhebung, und sofern diese bejaht wird, folgt eine Entscheidung darüber, welche Daten die Sicherheitsbehörden auswerten dürfen.[36]

Ausblick

In den Bundesländern, welche die Maßnahmen bereits eingeführt haben, wurden zum Teil Verfassungsbeschwerden eingelegt oder angekündigt.

Die durch die Bevölkerung derzeit geäußerte und auf zahlreichen Demonstrationen zur Schau gestellte massive Kritik an der Einführung neuer grundrechtsintensiver Polizeibefugnisse wie Quellen-TKÜ und Online-Durchsuchung hat bisher dazu geführt, dass vorerst zumindest in Bremen und Sachsen auf diese Befugnisse verzichtet wird. Andere Bundesländer wie Niedersachsen halten weiterhin auch trotz Kritik von Fachleuten und aus der Bevölkerung an ihren Vorhaben fest. So hat der niedersächsische Ministerpräsident Weil noch vor Beendigung der Sachverständigenanhörung im Landtag erklärt, dass er eine Nachbesserung nicht für notwendig erachtet.[37] Welche Bundesländer dem Trend zur Einführung der neuen Befugnisse folgen



Ned schee, Protest in München gegen das PAG
Foto: Günther Gerstenberg, CC BY

und welche die Kritik daran berücksichtigen werden, bleibt abzuwarten. Es kann jedenfalls erwartet werden, dass auch allen künftigen Gesetzesvorhaben mit massiver Kritik und zahlreichen Protesten begegnet werden wird. Im Übrigen bleiben die Entscheidungen des Bundesverfassungsgerichts zu den Regelungen in der Strafprozessordnung und dem bayerischen Polizeiaufgabengesetz abzuwarten. Diese Gerichtsentscheidungen werden die Einführung von Quellen-TKÜ und Online-Durchsuchung zwar nicht verhindern können, jedoch dem Gesetzgeber zumindest erneut die rechtlichen Grenzen aufzeigen.

Anmerkungen

1 *Heinrich A, Hügel S, Wiese K (2018) Stellungnahme zum Entwurf eines Reformgesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze – Gesetzentwurf der Fraktionen der SPD und der CDU (LT-Drs. 18/850). Humanistische Union, http://www.humanistische-union.de/nc/aktuelles/aktuelles_detail/back/aktuelles/article/niedersachsen-erweiterung-polizeilicher-befugnisse/*

2 *BVerfG, U. v. 07.02.2008, BVerfGE 120, 274.*

3 *LVerfG Sachsen-Anhalt, U. v. 11.11.2014, LVG 9/13.*

4 *BVerfG, U. v. 20.04.2016, BVerfGE 141, 220 (sog. BKAG-Urteil).*

5 *Verfassungsbeschwerden wurden eingelegt von Tele Trust, von Digitalcourage und gemeinsam von der Gesellschaft für Freiheitsrechte, dem Deutschen Anwaltsverein und der Humanistischen Union. https://freiheitsrechte.org/home/wp-content/uploads/2018/08/GFF_Verfassungsbeschwerde_Staatstrojaner_anonym.pdf*

6 *https://www.lfd.niedersachsen.de/startseite/allgemein/presseinformationen/stellungnahme_polizeigesetz/entwurf-zum-neuen-polizeigesetz-2018-167435.html*

7 *Auf die Ununterscheidbarkeit zwischen Quellen-TKÜ und Online-Durchsuchung hinsichtlich des Ausnutzens von Sicherheitslücken weist Fredrik Roggan hin: Roggan F (2017) Die strafprozessuale Quellen-TKÜ und Online- Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit. StV – Strafverteidiger, 12/2017, S. 821-829*

8 *Der Begriff „Remote Forensic Software" (RFS) ist aber irreführend. Er suggeriert, dass die damit gewonnenen Erkenntnisse den Beweiswert einer forensischen Analyse besitzen, was nicht der Fall ist. Dazu Fox D (2007) Stellungnahme zur „Online-Durchsuchung". Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07, Karlsruhe: Secorvo Security Consulting GmbH, https://secorvo.de/publikationen/*

stellungnahme-secorvo-bverfg-online-durchsuchung.pdf. Man könnte von „Durchsuchungssoftware" sprechen; bei Software für die Quellen-TKÜ von „Remote Communication Interception Software" (RCIS). De Facto ist es aber nichts anderes als Schadsoftware, die das Rechnersystem infiltriert und seine Funktion manipuliert.

9 *Der Begriff „Trojaner" entspricht dem „Trojanischen Pferd" aus der griechischen Mythologie. Die Schad- bzw. Überwachungssoftware ist technisch „eingepackt", um sie auf den Zielrechner zu bringen.*

10 *https://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf*

11 *Dazu Roggan F (2017), a. a. O., S. 824*

12 *BVerfG, U. v. 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07 – Rn. (280-283).*

13 *BKAG-Urteil, a.a.O Rn. 218 f.*

14 *So auch Maximilian Warntjen (2008): Der Kernbereichsschutz nach dem Online-Durchsuchungsurteil. in: Fredrik Roggan (Hg.) (2008): Online-Durchsuchung. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008. Berlin: Berliner Wissenschafts-Verlag.*

15 *Roggan F (2008) Präventive Online-Durchsuchungen. Überlegungen zu den Möglichkeiten einer Legalisierung im Polizei- und Geheimdienstrecht, in: Roggan F (Hg.) (2008) Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008. Berlin: Beliner Wissenschafts-Verlag, S. 100*

16 *Ein Exploit ist ein Stück Software, das eine Sicherheitslücke für einen Angriff ausnutzt. Von besonderem Interesse für Angreifer sind die sog. Zero-Day-Exploits, für die zum Zeitpunkt des Einsatzes noch keine Gegenmaßnahme entwickelt wurde.*

17 *Frank Kuhn kommt in einer Untersuchung zu diesem Ergebnis: Kuhn F (2018) Gefährdet der staatliche Einsatz von Spionagesoftware die Innere Sicherheit? Bachelor-Arbeit, Goethe-Universität Frankfurt am Main, https://cdn.netzpolitik.org/wp-upload/2018/09/2018-07-02_Frank-Kuhn_Bachelor_Gefaehrdet-Spionagesoftware-die-Innere-Sicherheit.pdf*

18 *Briegleb V, heise.de (2017) WannaCry: Was wir bisher über die Ransomware-Attacke wissen. https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html, 13. Mai 2017 und Stefan Hügel (2018): Öffentliche Sicherheit durch unsichere IT? Bundeswehr und Bundesnachrichtendienst gefährden die Sicherheit der öffentlichen Infrastruktur, in: Till Müller-Heidelberg, Marei Pelzer, Martin Heimig, Cara Röhner, Rolf Gössner, Matthias Fahrner, Helmut Pollähne, Maria Seitz: Grundrechte-Report 2018. Zur Lage der Bürger- und Menschenrechte in Deutschland. Frankfurt am Main: Fischer-Taschenbuchverlag*

19 *Das Beispiel zeigt auch, dass die Wirkung der Schadsoftware nicht an Landesgrenzen Halt macht. Damit stellt sich die Frage nach Cyberangriffen auf souveräne Staaten. Wird dadurch physischer Schaden verursacht, verletzten solche Angriffe nach Ansicht internationaler Experten die Souveränität. Vgl. dazu Schmitt MN (Hg.) (2013) Tallinn Manual on the International Law applicable to Cyber Warfare, Cambridge, UK u. a.: Cambridge University Press, Section 1, A 6.*

20 *Rehak R (2018) Stellungnahme des FIfF zur Anhörung des Hessischen Landtags am 8. Februar 2018 zum Gesetzentwurf für die Neuausrichtung des Verfassungsschutzes in Hessen: Hessischer Landtag, Ausschussvorlagen – Teil 3, S. 389-409, https://hessischer-landtag.de/sites/default/files/scald/files/INA-AV-19-63-T3-NEU.pdf*

21 *Fredrik Roggan weist darauf hin, dass der Staat „ein Interesse an der Lückenhaftigkeit des Schutzes von potentiell zu infiltrierenden Kommunikationsgeräten haben" muss, und: „Deutsche Strafverfolgungsbehörden müssen … ein Interesse an unsicherer IT-Infrastruktur haben. … Das freilich kollidiert – andererseits – mit dem staatlichen Auftrag das Schutzes derselben: Namentlich das Bundesamt für die Sicherheit in der Informationstechnologie hat die Sicherheit in der Informationstechnik zu fördern (§ 3 Abs. 1 S. 1 BSIG)". Roggan F (2017), a. a. O., S. 828-829*

22 *Herpig S (2018) Schwachstellenmanagement für mehr Sicherheit. Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte. Berlin: Stiftung Neue Verantwortung, https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf*

23 *Zu einer ernüchternden Einschätzung der parlamentarischen Kontrolle der Geheimdienste kommt Daniel Leisegang: Er stellt fest, „… dass die politische und juristische Aufarbeitung des [NSA-] Abhörskandals hierzulande keine nennenswerten Konsequenzen zeitigte. Im Gegenteil hat die Macht des BND in den vergangenen Jahren erheblich zugenommen. […] Dafür verantwortlich ist vor allem das dramatische Versagen der parlamentarischen Kontrolle." Leisegang D (2018) Fünf Jahre NSA-Affäre: Die neue Macht des BND. Blätter für deutsche und internationale Politik 6'18, S. 21–24*

24 *Fox D (2007), a. a. O.*

25 *§ 33a Abs. 2 und § 33d Abs. 1 S. 1 des niedersächsischen Gesetzentwurfs.*

26 *BVerfG, U. v. 20. April 2016 – 1 BvR 966/09 – Rn. (124).*

27 *BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (126).*

28 *BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (128).*

29 *BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (219).*

30 *BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (128).*

31 *BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (128).*

32 *BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (129).*

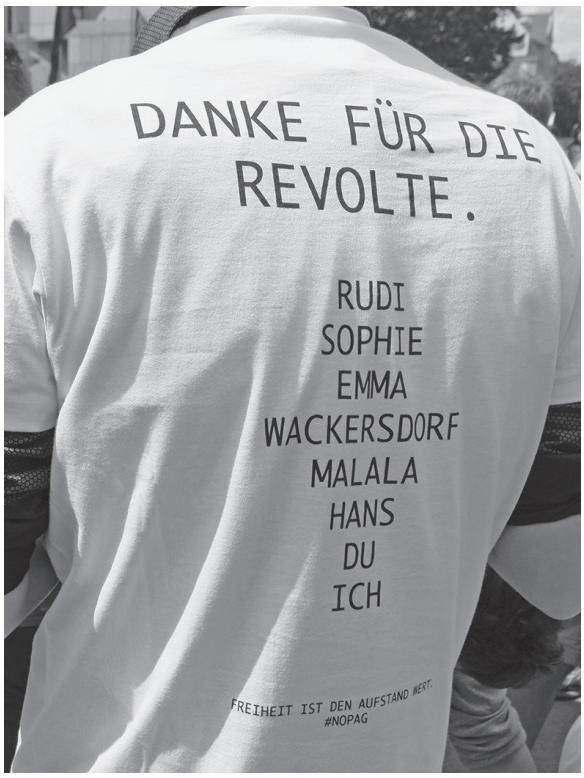
33 *BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (129).*

34 *BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (200 und 218).*

35 *BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (200 und 204).*

36 *Entsprechend zum BKA: Roggan F (2016) Enzyklopädie des Polizeirechts. Das Urteil des Verfassungsgerichts zum BKA-Gesetz. Bürgerrechte & Polizei / CILIP 111 (Dezember 2016).*

37 *https://www.ndr.de/nachrichten/niedersachsen/Ministerpraesident-Niedersachsens-im-Sommerinterview,sommerinterview266.html*



Freiheit ist den Aufstand wert, #NOPAG München
Foto: Günther Gerstenberg, CC BY