HUMANISTISCHE UNION e.V. - Haus der Demokratie und Menschenrechte
Greifswalder Straße 4, 10405 Berlin

Tel.: 030 / 20 45 02 –56
Fax: 030 / 20 45 02 –57
info@humanistische-union.de
www.humanistische-union.de

Humanistische Union

Berlin, 08.08.2018

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)

Autor*innen:

Anja Heinrich, Stefan Hügel, Dr. Kirsten Wiese

Sehr geehrte Frau Präsidentin,
sehr geehrte Damen und Herren Abgeordnete,

wir danken Ihnen für die Möglichkeit zur Stellungnahme zum oben genannten Antrag. Allerdings möchten wir nicht verschweigen, dass wir die Stellungnahmefrist insbesondere angesichts der zeitgleich stattfindenden Schulsommerferien für zu kurz halten.

INHALT

A. VORBEMERKUNG 4

B. ZUSAMMENFASSUNG DER STELLUNGNAHME 5

C. ZU EINZELNEN REGELUNGEN UND ASPEKTEN DES KOALITIONSENTWURFS 6

1. Neue Begrifflichkeiten 6
2. Gefährderansprache, Gefährderanschreiben 9
3. Freiheitsbeschränkende und -entziehende Maßnahmen 10
4. Besondere Datenerhebungsbefugnisse 13
5. Kernbereich privater Lebensgestaltung (§ 31 b NPOG-E) 14
6. Body-Cams (§ 32 Abs. 4 S. 2 NPOG-E) 16
7. TKÜ und Quellen-TKÜ (§ 33 a NPOG-E) 18
8. Online-Durchsuchung (§ 33 d NPOG-E) 19
9. Einsatz von Tasern (§ 69 Abs. 4 NPOG-E) 23
10. Versammlungsgesetz: Vermummungsverbot (§ 20 Abs. 2 Nr. 5 VersG-E) 24

A. VORBEMERKUNG

Die Humanistische Union e.V., vereinigt mit der Gustav Heinemann-Initiative, ist eine bundesweit tätige Bürgerrechtsorganisation, die 1961 in München gegründet wurde. Wir engagieren uns für das Recht auf freie Entfaltung der Persönlichkeit und wenden uns gegen jede unverhältnismäßige Einschränkung dieses Rechts durch Staat, Wirtschaft oder Religions- und Weltanschauungsgemeinschaften. Laut unserer Satzung unterstützen wir Bestrebungen, die „es jeder Bürgerin und jedem Bürger gestatten, von den im Grundgesetz garantierten Rechten der individuellen Lebensgestaltung, der Glaubens-, Gewissens- und Bekenntnis-, der Meinungs-, Informations- und Koalitionsfreiheit ohne Furcht vor Nachteilen Gebrauch zu machen". Hinsichtlich der notwendigen Gefahrenabwehr im Inland treten wir deshalb für die Wahrung der Rechtsstaatlichkeit auch in Krisenzeiten ein. Eine offene Gesellschaft, in der der Staat die Freiheits- und Gleichheitsrechte wahrt und durch soziale Leistungen allen ein menschenwürdiges Leben ermöglicht, halten wir weiterhin für ein probates Mittel, um Menschen gar nicht erst dazu zu verleiten, die Rechte und Freiheiten anderer zu bedrohen. Wir wollen diese Rechte und Freiheiten nicht für zum Teil nur trügerische Sicherheit opfern und halten wider den Trend zum Präventionsstaat am Rechtsstaat fest. Zwar gehen auch wir davon aus, dass der Staat die Bürger und Bürgerinnen vor Straftaten schützen soll. Allerdings sind polizeiliche grundrechtsbeschränkende Befugnisse nicht das einzige mögliche Mittel der Gefahrenabwehr. Gefahren können zum Beispiel auch im Vorfeld verhindert werden durch Sozialarbeiter*innen, die mit Menschen arbeiten, von denen möglicherweise Gefahren ausgehen, oder Städteplanung, die verhindert, dass dunkle Orte entstehen, an denen sich Menschen bedroht fühlen. Ebenso können die Polizeibehörden selbst durch Informations- und Aufklärungskampagnen und zum Teil auch durch mehr körperliche Präsenz Gefahren abwehren, ohne dadurch die Grundrechte der Bürger*innen zu beschränken. In diesem Sinne nimmt die Humanistische Union e.V. seit Jahren zu Entwürfen von Sicherheitsgesetzen in Bund und Ländern Stellung, zuletzt zu Beginn dieses Jahres zum Entwurf eines Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen vom 14.11.2017.[1]

Aus Kapazitätsgründen können wir keine Stellungnahme zum Entschließungsantrag der Fraktion Bündnis 90/Die Grünen "Für ein Niedersächsisches Gefahrenabwehrgesetz ohne Symbolpolitik und Generalverdacht" (LT-Drs. 18/828) abgeben, von denen wir jedoch zahlreiche Aspekte begrüßen. Genannt seien an dieser Stelle insbesondere

- eine Kennzeichnungspflicht der Polizei insbesondere in geschlossenen Einsätzen,[2]
- eine Erweiterung der unabhängigen Beschwerdestelle und die Einführung eines Polizeibeauftragten, [3]
- eine gesetzliche Definition des „terroristischen Gefährders"[4] und
- eine gesetzliche Regelung der Gefährderansprache.[5]

---

1 (Autor: Till Müller-Heidelberg). Abrufbar unter http://www.humanistische-union.de/nc/themen/rechtspolitik/gutachten/details/back/rechtspolitische-stellungnahmen/article/hessen-gesetzentwurf-ueber-die-neuausrichtung-des-landesverfassungsschutzes/

2 Die Humanistische Union fordert seit langem eine solche Kennzeichnungspflicht und hat dies in zahlreichen Stellungnahmen zu entsprechenden Gesetzesinitiativen geäußert, wie z.B. am 28.10.2013 zur hessischen LT-Drs. 18/7522 „Polizeiliche Kennzeichnungspflicht" (Autorin: Anja Heinrich), abrufbar unter http://www.humanistische-union.de/fileadmin/hu_upload/doku/2013/HU2013-10-28_AH_HSOG.pdf

3 S. auch unsere Stellungnahme vom 24.02.2016 zur schleswig-holsteinischen LT-Drs. 18/3655 „Einführung eines Landes-Polizeibeauftragten" (Autorin: Anja Heinrich), abrufbar unter http://www.humanistische-union.de/nc/themen/innere_sicherheit/polizei/polizei_detail/back/polizei/article/schleswig-holstein-einfuehrung-eines-landes-polizeibeauftragten/

4 S. Punkt C.1.1.2. dieser Stellungnahme

5 S. Punkt C.1.2 dieser Stellungnahme

B. ZUSAMMENFASSUNG DER STELLUNGNAHME

Die niedersächsische Regierungskoalition will mit dem Entwurf insbesondere durch Änderungen des Gesetzes über die öffentliche Sicherung und Ordnung (Polizeigesetz) den Polizeibehörden mehr präventive grundrechtsrelevante Befugnisse einräumen. Darüber hinaus sollen andere im Zusammenhang mit dem Polizei- und Ordnungsgesetz stehende Gesetze geändert werden. Hervorzuheben ist die im Niedersächsischen Versammlungsgesetz angestrebte Pönalisierung des Vermummungsverbotes.

Folgende Aspekte des Gesetzentwurfs sehen wir besonders kritisch:

- Die Einführung neuer Gefahrenbegriffe in das niedersächsische Polizeigesetz: Erstens wird nicht deutlich, warum der Landesgesetzgeber überhaupt zusätzlich zur konkreten Gefahr und den Gefahrenvariationen der gegenwärtigen und erheblichen Gefahr sowie der Gefahr für Leib und Leben neue Gefahrenbegriffe einführt (siehe § 2 Nds. SOG). Zweitens geht damit einher, dass die Polizeibehörden noch stärker als gegenwärtig zeitlich und mit Blick auf die Kausalkette vor dem Eintritt des möglichen oder tatsächlichen Schadens für ein Rechtsgut – mit anderen Worten: im Gefahrenvorfeld[6] – tätig werden dürfen. Drittens sind die neuen Gefahrenbegriffe keiner hinreichend klaren Auslegung zugänglich und genügen damit nicht dem verfassungsrechtlich verankerten Bestimmtheitsgebot.
- Die elektronische Fußfessel greift unverhältnismäßig insbesondere in das Recht auf informationelle Selbstbestimmung ein und ist zudem wenig geeignet zur Gefahrenabwehr.
- Die zeitliche und tatbestandliche Ausdehnung des Präventivgewahrsams: Freiheit ist ein hohes Gut, das nur unter den strengen Voraussetzungen des Grundgesetzes und der Europäischen Menschenrechtskonvention entzogen werden darf. Die neuen Regelungen zum Präventivgewahrsam genügen diesen Anforderungen nicht.
- Effektiver Kernbereichsschutz kann nur bei der Datenerhebung ansetzen. Die vorliegende Regelung zum Kernbereich enthält im Übrigen zahlreiche Unzulänglichkeiten, die den bundesverfassungsgerichtlichen Vorgaben in Bezug auf den notwendigen Abbruch von Datenerhebungen, die Protokollierungspflichten bei Datenlöschungen, die Verwendung von informationstechnischen Sicherungen bei der Online-Durchsuchung sowie die notwendige richterliche Sichtung erhobener Daten nicht genügen.
- Es ist technisch nicht möglich, die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) auf laufende Telekommunikationsvorgänge in einem Rechnersystem einzugrenzen. Damit müssen für die Quellen-TKÜ und die Online-Durchsuchung die gleichen Rahmenbedingungen und Bestimmungen gelten.
- Für den heimlichen Zugriff mit Remote Forensic Software müssen Sicherheitslücken auf dem Zielsystem ausgenutzt werden, die zu diesem Zweck geschaffen oder auf einem Schwarzmarkt gekauft und geheimgehalten werden müssen. Da die Sicherheitslücken auch durch Andere genutzt werden können, führt die Geheimhaltung potenziell zu einer - auch grenzüberschreitenden - Gefährdung der öffentlichen IT-Infrastruktur. Zusätzlich wird ein Markt für Schadsoftware gefördert, durch den die Gefährdung weiter verstärkt wird.
- Durchsuchungsergebnisse können durch die Zielpersonen und die Ermittlungspersonen manipuliert werden; eine rechtssichere Dokumentation kann auf einem fremden System nicht gewährleistet werden. Damit haben sie keine forensische Beweiskraft. Die rechtskonforme Funktion der verwendeten Software muss sichergestellt werden; dies ist bei kommerzieller, proprietärer Software oft nicht möglich.

---

[6] Siehe die Gesetzesbegründung, Nds. Landtag, Drucksache 18/850, unter anderem S. 45, 55, 59.

- Taser sollten allenfalls als mildere Alternative zum Schusswaffengebrauch dienen. Alle Anwendungsvoraussetzungen und –grenzen sind durch den parlamentarischen Gesetzgeber zu regeln.
- Die anonyme Teilnahme an Versammlungen ist als Gestaltungsfreiheit von der Versammlungsfreiheit geschützt. Es gibt berechtigte Interessen, die eine anonyme Teilnahme an Versammlungen begründen. Eine Pönalisierung von Verstößen steht flexiblem und situationsgerechtem Handeln der Polizeibehörden vor Ort entgegen.

C. Zu einzelnen Regelungen und Aspekten des Koalitionsentwurfs

Aus Kapazitätsgründen können wir im Folgenden nur zu einzelnen Regelungen und Aspekten Stellung beziehen.

1. Neue Begrifflichkeiten

1.1. Gefahrenbegriffe

Etabliert hat sich in den Landespolizeigesetzen und in der Rechtsprechung der Begriff der „konkreten Gefahr". Die „konkrete Gefahr" ist „eine Sachlage, bei der im einzelnen Fall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für die öffentliche Sicherheit oder Ordnung eintreten wird" (§ 2 Nr. 1 a Nds. SOG). Das BVerfG hatte ausgesprochen, dass dieser Begriff – auch in der Generalklausel – zwar vom Wortlaut her nicht sonderlich bestimmt ist, aber von der Rechtsprechung in rechtsstaatlich ausreichender Weise über Jahrzehnte konkretisiert sei.[7]

Die Definition der „konkreten Gefahr" gibt den Polizeibehörden bereits sehr weitreichende Eingriffsbefugnisse, da die gängige Definition der Schutzgüter für die Gefahrenabwehr an die Unversehrtheit der Rechtsordnung anknüpft. Damit sind jegliche Gesetzesverstöße erfasst: Straftaten, die „Funktionsfähigkeit staatlicher Einrichtungen" und die Rechtsgüter der einzelnen Menschen. Auch ein Gefahrenverdacht eröffnet bereits beschränkte polizeiliche Handlungsmöglichkeiten; das heißt, dass die Polizei in bestimmten Situationen auch dann handeln darf, wenn sie noch nicht davon überzeugt ist, dass tatsächlich ein Schaden für ein Rechtsgut eintreten wird.

Schon jetzt dürfen die niedersächsischen Polizeibehörden darüber hinaus in bestimmten Situationen anlasslos handeln. So dürfen sie Identitätskontrollen und Personendurchsuchungen an „kriminalitätsbelasteten" Orten, gefährdeten Objekten und Kontrollstellen durchführen (§§ 13, 14, 22 Nds. SOG).

Durch den Entwurf sollen zwei neue Gefahrenbegriffe in das Gesetz eingeführt werden.

Der Begriff der „dringenden Gefahr" wird definiert als „eine im Hinblick auf das Ausmaß des zu erwartenden Schadens und die Wahrscheinlichkeit des Schadenseintritts erhöhte Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt" (§ 2 lit. a) Nr. 4 NPOG-E).

Der Begriff der „dringenden Gefahr" steht in Art. 13 Abs. 4 und 7 GG, und dem folgend machen einige Landespolizeigesetze die „dringende Gefahr" zur Voraussetzung für eine der Tatbestandsalternativen der Wohnungsdurchsuchung (z.B. § 21 Abs. 3 Bremisches Polizeigesetz). Im Niedersächsischen Polizeigesetz ist die „dringende Gefahr" dagegen bislang nicht enthalten. Art. 13 Abs. 4 GG nennt

7 BVerfG, Beschluss vom 23. 5. 1980 - 2 BvR 854/79; Waechter, NVwZ 2018, 458

„insbesondere eine gemeine Gefahr oder eine Lebensgefahr" als Beispiele für die dringende Gefahr. Aus Art. 13 Abs. 7 GG wird gefolgert, dass eine Gefahr jedenfalls nur dann dringend ist, wenn ein Schaden für ein hochrangiges Rechtsgut droht. Art. 13 Abs. 7 GG nennt die Behebung der Raumnot, die Bekämpfung von Seuchengefahr und den Schutz gefährdeter Jugendlicher als solche hochrangigen Rechtsgüter. Für die Dringlichkeit sind zudem das Ausmaß als auch die Wahrscheinlichkeit des zu erwartenden Schadens zu berücksichtigen, ohne dass eine besondere zeitliche Nähe erforderlich ist.[8] Im Urteil zum BKA-Gesetz führte das BVerfG aus, dass an das Vorliegen einer dringenden Gefahr strengere Anforderungen als an eine konkrete Gefahr zu richten seien.[9]

Im Gesetzentwurf soll eine dringende Gefahr unter anderem dann vorliegen, wenn ein Schadenseintritt für „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt" droht, sofern das Ausmaß des zu erwartenden Schadens und die Schadenswahrscheinlichkeit erhöht sind. Was solche „Sachen von bedeutendem Wert" sind, bleibt aber unklar, so dass zumindest dieser Begriffsbestandteil zu unbestimmt ist.[10]

Zudem werden in §§ 12a, 16a, 17 b, 33a, 33d, 34, 35a NPOG-E neue Tatbestandsvoraussetzungen für polizeiliches Handeln eingeführt, die letztlich einen weiteren neuen Gefahrenbegriff begründen, der jedoch nicht ausdrücklich in § 2 NPOG-E definiert wird. Danach sollen die Polizeibehörden bestimmte Maßnahmen ergreifen dürfen, wenn „1. bestimmte Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat begehen wird, oder 2. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird". Hier werden Begrifflichkeiten aufgegriffen, die das BVerfG im Urteil zum BKA-Gesetz 2016 erstmalig verwendet hat.[11] Im reformierten Bayerischen Polizeiaufgabengesetz werden diese neuen Tatbestandsvoraussetzungen als „drohende Gefahr" bezeichnet (Art. 11 Abs. 3 BayPAG).

Obwohl das BVerfG selbst diese Begrifflichkeiten eingeführt hat, ist fraglich, ob sie mit dem verfassungsrechtlichen Bestimmtheitsgebot in Einklang stehen. Nach dem aus dem Rechtsstaatsprinzip abgeleiteten allgemeinen Bestimmtheitsgebot muss sichergestellt bleiben, dass das Handeln der Verwaltung messbar und in gewissem Ausmaß für die Bürger*innen voraussehbar und berechenbar ist, und dass eine Gerichtskontrolle ermöglicht wird.[12] In Bezug auf die erweiterten Datenerhebungsbefugnisse des BKA hat das BVerfG im BKA-Gesetz-Urteil festgestellt: „Die diesbezüglichen Anforderungen sind normenklar zu regeln".[13] Das Mindestmaß an Tatbestandsanforderungen für die BKA-Befugnisse – bzw. das Übermaßverbot für die damit verbundenen Grundrechtseingriffe - legte das BVerfG mit den neuen von der niedersächsischen Regierungskoalition nun aufgegriffenen Begrifflichkeiten fest: Für Maßnahmen zur Straftatenverhütung sei erforderlich, „dass insoweit ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist". In Bezug auf terroristische Straftaten könne der Gesetzgeber stattdessen aber auch darauf abstellen, „ob das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft terroristische Straftaten

8 BeckOK Grundgesetz/Kluckert/Fink GG Art. 13 Rn. 24-30, beck-online

9 BVerfGE 141, 220 Rn. 184, NJW 2016, 1781 ff

10 Ebenso Weichert, Stellungnahme zum Entwurf eines Reformgesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze… vom 13.7.2018.

11 BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 – Rn. 112.

12 BeckOK Grundgesetz/Huster/Rux GG Art. 20 Rn. 182-183, beck-online

13 BVerfG, U. v. 20. April 2016 - 1 BvR 966/09 - Rn. (164.).

begeht".[14] Weder legt das BVerfG hier aber klare Tatbestandsvoraussetzungen fest, noch kann dieses Mindestmaß an Tatbestandsvoraussetzungen ohne weiteres für andere Maßnahmen als Datenerhebungsbefugnis übernommen werden.

Ob die im niedersächsischen Gesetzentwurf verwendeten Begrifflichkeiten Inhalt, Zweck und Ausmaß des zulässigen Handelns derart begrenzen, dass für die Bürger*innen vorhersehbar ist, wann die Polizeibehörden im Gefahrenvorfeld Maßnahmen durchführen können, ist vielmehr zweifelhaft.

Zwar werden die neuen Tatbestandsvoraussetzungen beschränkt auf die Erwartung, dass eine „terroristische Straftat" begangen wird. Eine solche soll nach der neu einzuführenden Definition in § 2 NPOG-E Straftaten wie Mord und Totschlag, schwere Körperverletzung und erpresserischen Menschenraub umfassen, sofern diese Straftat (entsprechend § 129a StGB) dazu bestimmt ist, „die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates, eines Landes oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und durch die Art der Begehung oder ihre Auswirkungen einen Staat, ein Land oder eine internationale Organisation erheblich schädigen kann". Schon diese Definition selbst ist aber sehr auslegungsbedürftig. Zudem können nach dem NPOG-E 28 Straftaten in terroristischer Weise begangen werden. Freiheitsfoo weist in ihrer Stellungnahme zu dem hier zu diskutierenden Gesetzentwurf darauf hin, dass aktuell ein Dutzend migrantische linke Aktivist*innen in Stuttgart und München unter dem Vorwurf des Terrorismus inhaftiert seien – „ihre Straftat: Spendensammeln für oppositionelle Organisationen in der Türkei. Verurteilt wegen Terrorismus - in Deutschland".[15]

Wir regen an, jedenfalls auf die aus dem Bundesverfassungsgerichtsurteil zum BKA-Gesetz übernommenen Begrifflichkeiten („drohende Gefahr") zu verzichten, und „dringende Gefahr" und „terroristische Straftat" enger zu fassen.

1.2. Terroristische*r Gefährder*in

Laut Gesetzesbegründung dient ein gewichtiger Teil der gesetzlichen Änderungen der Bekämpfung des islamistischen Terrorismus.[16] Insbesondere „die sogenannten Gefährderinnen und Gefährder" sollen effektiver überwacht werden. Insbesondere soll durch die angestrebten Änderungen die präventive Bekämpfung und Abwehr des islamistisch motivierten Terrorismus verbessert werden.

Angesichts des islamistisch motivierten Anschlags auf den Breitscheidtplatz in Berlin 2016 und der zahlreichen weiteren islamistisch motivierten grausamen Anschläge weltweit ist es gut, dass die Regierungskoalition die Bevölkerung vor solchen Gefahren noch besser schützen möchte. Allerdings konnten deutsche Sicherheitsbehörden bereits ohne die jetzt angestrebten Änderungen in den Landespolizeigesetzen mehrere mutmaßliche Anschläge verhindern, unter anderem solche der Sauerlandgruppe.

Der Begriff „terroristischer Gefährder" ist zwar jenseits der Gefährderansprache in § 12 a NPOG-E kein geschriebenes Tatbestandsmerkmal im Gesetzentwurf. Allerdings ist er (wohl tatsächlich männliche Gefährder) die Person, die den Schutzzweck einiger der neuen – wie elektronische Aufenthaltsüberwachung und Meldeauflage - bzw. neu-erweiterten Normen bestimmt,[17] und insoweit ist der „terroristische Gefährder" ein relevanter Gesetzesbegriff.

---

14 BVerfG, U. v. 20. April 2016 - 1 BvR 966/09 - Rn. (164.).

15 https://wiki.freiheitsfoo.de/uploads/Main/20180728stellungahme-freiheitsfoo-NPOG-anon.pdf, S. 7.

16 Nds. Landtag, Drs. 18/850, S. 34.

17 Siehe zum Bespiel die Begründung zur elektronischen Aufenthaltsüberwachung, Nds Landtag, Drucksache 18/850, S. 45

Dieser Begriff ist ähnlich wie die neuen Gefahrenbegriffe – und im Zusammenhang mit diesen – problematisch und unbestimmt[18].

Der Gefährderbegriff ist derzeit nicht legal definiert. Eher handelt es sich um einen „Arbeitsbegriff" der Sicherheitsbehörden, der insbesondere bei der Bekämpfung des Terrorismus Anwendung findet. Die Arbeitsgemeinschaft der Leiter der Landeskriminalämter und des Bundeskriminalamtes hat im Jahr 2004 eine Definition beschlossen, die von der Bundesregierung und verschiedenen Sicherheitsbehörden der Länder verwendet wird. Seitdem wird folgende Definition verwendet: „Ein Gefährder ist eine Person, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie politisch motivierte Straftaten von erheblicher Bedeutung, insbesondere solche im Sinne des § 100a der Strafprozessordnung (StPO), begehen wird".[19] An die Einstufung einer Person als „Gefährder" sind nicht nur gegen diese gerichtete Eingriffsbefugnisse geknüpft, sondern Datensätze zu Gefährdern werden an Europol und ausländische Polizeien übermittelt. [20]

Zugleich wird der Begriff Gefährder aber im NPOG-E im Zusammenhang mit der Gefährderansprache und dem Gefährderanschreiben auch für Personen verwendet, denen kein Terrorismus unterstellt wird. Nach § 12a NPOG-E soll sich die Polizei schriftlich oder mündlich an eine Person wenden können, die eine Gefahr verursacht oder bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie „innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat begehen wird". In diesem Zusammenhang ist „Gefährder" also eher zu verstehen als Verursacher einer Gefahr, ohne dass es zwingend auf das Begehen einer Straftat oder gar einer terroristischen Straftat ankäme. Schon bislang werden in Niedersachsen und anderen Bundesländern Gefährderansprachen z.B. an gewaltbereite Fußballfans oder Demonstrant*innen vor entsprechenden Ereignissen gerichtet.

Der weite Begriff des/der Gefährder*in im Zusammenhang mit der angestrebten Verlagerung von Eingriffsbefugnissen ins Vorfeld der vermuteten Schadensverwirklichung (siehe oben) birgt das Risiko, dass immer mehr Menschen in den Fokus der Sicherheitsbehörden geraten, immer mehr Verhaltensweisen unter Sicherheitsaspekten problematisiert werden, immer mehr Daten von den Polizeibehörden gesammelt werden und diese auch immer mehr Maßnahmen tatsächlich gegen Menschen richten.[21]

Wir regen an, die Begriffe „Gefährder" und „terroristischer Gefährder" in § 2 NPOG-E eng und klar zu definieren.[22]

2. Gefährderansprache, Gefährderanschreiben

In § 12a NPOG-E sollen erstmalig Gefährderansprache und Gefährderanschreiben normiert werden. Grundsätzlich begrüßen wir, dass diese Maßnahmen ausdrücklich geregelt werden sollen.[23] Bereits jetzt werden in Niedersachsen ebenso wie in anderen Bundesländern Gefährderansprachen

18 Siehe die Antwort der Bundesregierung auf die Kleine Anfragen der Fraktion Die Linke zur Problematik des Gefährderbegriffes vom 3.3.2017 und 2.5.2017, Drs. 18/11369 und 18/12196.

19 Wissenschaftlicher Dienst des Bundestages, Sachstand „Legaldefinition des GEfährders", 27.2.2017, https://www.bundestag.de/blob/503066/8755d9ab3e2051bfa76cc514be96041f/wd-3-046-17-pdf-data.pdf

20 Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion Die Linke zur Problematik des Gefährderbegriffes 2.5.2017, Drs. 18/12196.

21 Kritisch dazu unter anderem Singelnstein, "Innere Unsicherheit", Süddeutsche Zeitung vom 14./15.4.2018.

22 Siehe auch Antrag der Fraktion Bündnis 90/Die Grünen – LT-Drs. 18/828, Forderung Nr. 6 „Einführung einer Legaldefinition „Terroristische Straftat", damit der Begriff des „terroristischen Gefährders" unter ausschließlicher Berücksichtigung der „besonders schwerwiegenden Straf-taten" und der „Straftaten von erheblicher Bedeutung" bestimmt wird,"

23 Ebenso Antrag der Fraktion Bündnis 90/Die Grünen – LT-Drs. 18/828, Forderung Nr. 9.

insbesondere gegenüber gewaltbereiten Fußballfans und Demonstrant*innen, aber auch anderen Personen, die eine Gefahr verursachen könnten - z.B. Störer*innen eines polizeilichen Einsatzes -, praktiziert. Die Polizei signalisiert diesen Personen „Wir kennen dich, wir haben dich im Auge", zeigt ihr die polizeilichen und möglichen strafrechtlichen Folgen ihres Tuns auf, und versucht sie so von der tatsächlichen Verursachung des Schadenseintritts abzuhalten.

Bislang wurde dieses polizeiliche Vorgehen auf die Generalklausel gestützt, wobei umstritten war, ob es mit Grundrechtseingriffen verbunden ist und demnach überhaupt einer gesetzlichen Regelung bedurfte.

Durch eine Gefährderansprache oder ein Gefährderanschreiben wird jedenfalls in das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützte Allgemeine Persönlichkeitsrecht eingegriffen. Durch das Allgemeine Persönlichkeitsrecht werden die persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen geschützt. Es sichert einen autonomen Bereich privater Lebensgestaltung und garantiert die Freiheit innerhalb der persönlichen Lebenssphäre (zum Kernbereich der persönlichen Sphäre siehe weiter unten).[24]

In diesen Schutzbereich wird bereits dadurch eingriffen, dass die Lebensgestaltung des/der Betroffenen dadurch beeinflusst werden kann, dass er/sie weiß, dass er/sie im polizeilichen Fokus steht, und sein/ihr Leben möglicherweise danach ausrichtet. Jedenfalls wird in das Allgemeine Persönlichkeitsrecht eingegriffen, wenn andere Menschen – Freund*innen, Arbeitgeber*in, zufällig Anwesende – die Gefährderansprache miterleben.[25]

Wir halten deshalb eine gesetzliche Regelung der Gefährderansprache und des Gefährderanschreibens für erforderlich. Zugleich gehen wir davon aus, dass diese Maßnahmen taugliche Mittel der Gefahrenprävention sind, die weniger als andere polizeiliche Maßnahmen in Grundrechte eingreifen.

Wir regen aber an, die Tatbestandsvoraussetzungen enger zu fassen und auf das Verursachen einer Gefahr zu beschränken (siehe oben die Ausführungen zu den Gefahrenbegriffen). Zudem sollte in § 12a NPOG-E klargestellt werden, dass unter Verhältnismäßigkeitsgesichtspunkten die Polizeibehörden sich ausdrücklich bemühen müssen, die Ansprache von erwachsenen Personen ohne Anwesenheit anderer Personen durchzuführen.

3. Freiheitsbeschränkende und -entziehende Maßnahmen

Durch Meldeauflage (§ 16a NPOG-E), Aufenthaltsvorgabe und Kontaktverbot (§ 17b NPOG-E), Elektronische Aufenthaltsüberwachung (§ 17c NPOG-E) und die Erstreckung des Präventivgewahrsams auf diese Maßnahmen und die gleichzeitige Erhöhung der Höchstdauer des Präventivgewahrsams (§§ 18 I Nr. 3, 21 NPOG-E) werden neue bzw. verschärfende insbesondere die Freiheit der Person beschränkende bzw. entziehende Maßnahmen eingeführt.

Die durch Art. 2 Abs. 2 S. 2, Art. 104 GG geschützte Freiheit der Person nimmt – so das Bundesverfassungsgericht – „als Grundlage […] der Entfaltungsmöglichkeiten des Bürgers einen hohen Rang unter den Grundrechten ein. Das kommt darin zum Ausdruck, dass Art. 2 Abs. 2 Satz 2 GG sie als unverletzlich bezeichnet".[26] Eingriffe in die Freiheit der Person, die der Gefahrenabwehr dienen, sind deshalb nur zulässig, „wenn der Schutz hochwertiger Rechtsgüter sie unter strikter

24 Siehe statt vieler Fisahn/Kutscha, Verfassungsrecht konkret – Die Grundrechte, 3. Auflage, 2018.

25 Siehe Stellungnahme von freiheitsfoo zu den hier besprochenen Anträgen, S. 22, https://wiki.freiheitsfoo.de/uploads/Main/20180728stellungahme-freiheitsfoo-NPOG-anon.pdf

26 BVerfG, Urteil vom 4.11.2011 - Az. 2 BvR 2365/09 (nachträgliche Sicherungsverwahrung).

Beachtung des Verhältnismäßigkeitsgrundsatzes erfordert. Dem Freiheitsanspruch des Betroffenen ist das Sicherungsbedürfnis der Allgemeinheit entgegenzuhalten".[27]

Vor diesem Hintergrund beurteilen wir die angestrebten Änderungen kritisch:

3.1. Meldeauflage, § 16a NPOG-E

In § 16a NPOG-E ist vorgesehen, dass die Polizeibehörden eine Person verpflichten können, sich auf einer bestimmten Polizeidienststelle vorzustellen, wenn "Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat begehen wird".

Es muss sich nicht um eine terroristische Straftat handeln, vielmehr reicht jede Straftat aus. Nimmt die Polizei an, dass eine Person eine terroristische Straftat begehen wird, sind die Tatbestandsanforderungen niedriger. Es reicht aus, wenn "das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird".

Bei Verstoß gegen die Meldeauflage, die wegen der Gefahr einer terroristischen Straftat angeordnet wurde (§ 16a Abs. 2 NPOG-E), soll Gewahrsam angeordnet werden können (§ 18 Abs. 1 Nr. 3 lit a) NPOG-E).

Durch Meldeauflagen wird die Freiheit der Person beschränkt, weil die körperliche Bewegungsfreiheit an den Tagen, an denen sich die betroffene Person auf einer bestimmten Polizeidienststelle vorzustellen hat, insofern gelenkt wird, als sie sich nur in einem bestimmten Umkreis von der Polizeidienststelle aufhalten kann.

Meldeauflagen werden bereits gegenwärtig in Niedersachsen und anderen Bundesländern praktiziert insbesondere gegenüber Fußballfans, von denen die Polizeibehörden Gewaltausübung beim Auswärtsspiel erwarten, und im Vorfeld großer Demonstrationen gegenüber potenziellen Versammlungsteilnehmenden, von denen die Polizeibehörden Gewaltausübung erwartet.

Bislang sind Meldeauflagen nicht gesetzlich geregelt, vielmehr werden sie auf die polizeiliche Generalklausel gestützt (§ 11 Nds. SOG).

Eine ausdrückliche gesetzliche Regelung ist aber wegen des freiheitsbeschränkenden Charakters der Meldeauflage mit Blick auf das Wesentlichkeitsprinzip erforderlich. Soweit potenzielle Versammlungsteilnehmende von der Anreise abgehalten werden sollen, ist zudem auch die Versammlungsfreiheit, Art. 8 GG, betroffen.

In der angestrebten Regelung der Meldeauflage sind aber die Tatbestandsvoraussetzungen zu weit. Eine Meldeauflage sollte nur zulässig sein, wenn die konkrete Gefahr besteht, dass die betroffene Persone eine Straftat von erheblicher Bedeutung (§ 2 Nr. 14 NPOG-E), eine terroristische Straftat (§ 2 Nr. 14 NPOG-E) oder eine schwere organisierte Gewalttat (§ 2 Nr. 16 NPOG-E) begehen wird.[28]

Zudem sollte entsprechend dem Bestimmtheitsgebot und dem Verhältnismäßigkeitsgrundsatz normiert werden, in welchen Abständen und ggf. auch zu welchen Tageszeiten sich die betroffene Person bei der Polizeidienststelle melden soll. Die inklusive der Verlängerung mögliche Höchstdauer von einem Jahr ist unter Verhältnismäßigkeitsgesichtspunkten zu lang.[29]

---

27 BVerfG, Beschluss vom 18.4.2016 – Az. 2 BvR 1833/12, 2 BvR1945/12 (Ingewahrsamnahmen von „Schotterern")

28 Ähnlich Antrag der Fraktion Bündnis 90/Die Grünen – LT-Drs. 18/828, Forderung Nr. 10.

29 So auch Weichert, Stellungnahme zu den hier besprochenen Anträgen, vom 13.7.2018, S. 3.

Wir begrüßen demnach die gesetzliche Regelung der Meldeauflage, regen jedoch Änderungen der angestrebten Regelung an. Der Verstoß gegen die Meldeauflage sollte nur mit einem Bußgeld geahndet werden können, jedoch kein Anlass für eine Ingewahrsamnahme sein.

3.2. Aufenthaltsverbot, Aufenthaltsvorgabe und Kontaktverbot zur Verhütung einer terroristischen Straftat (§ 17b NPOG-E)

Die Polizeibehörden sollen zur Verhütung von terroristischen Straftaten eine Person daran hindern dürfen, einen bestimmten örtlichen Bereich aufzusuchen dürfen (Aufenthaltsverbot), oder sie dazu verpflichten dürfen, sich für eine bestimmte Zeit nicht von ihrem Wohn- oder Aufenthaltsort zu entfernen (Aufenthaltsvorgabe) und / oder Kontakt mit bestimmten Personen oder Personen einer bestimmten Gruppe aufzunehmen (Kontaktverbot).

Das Aufenthaltsverbot betrifft die Freizügigkeit der Person, Art. 11 GG, die Aufenhaltsvorgabe dagegen die Freiheit der Person, das Kontaktverbot betrifft jedenfalls das Allgemeine Persönlichkeitsrecht und – sofern sich die Personen, die nicht kontaktiert werden dürfen, regelmäßig an einem bestimmten Ort aufhalten, der dadurch nicht aufgesucht werden darf (z.B. eine Moschee) – auch die Freiheit der Person.

Aufenthaltsverbote sind schon länger bundesweit praktizierte Maßnahmen. Aufenthaltsvorgaben und Kontaktverbote sind neue Maßnahmen. Grundsätzlich erscheinen uns diese Maßnahmen zulässig, insbesondere weil sie im Vergleich zum Präventivgewahrsam mildere Mittel sind.

Erneut sind allerdings die Tatbestandsvoraussetzungen zu weit gefasst. Die Maßnahmen sollten nur zulässig sein, wenn eine konkrete Gefahr und zumindest – entsprechend der bisherigen Regelung des allgemeinen Aufenthaltsverbotes in § 17 IV Nds. SOG – ein Gefahrenverdacht vorliegt.

Zudem muss die Regelung mit Blick auf den Verhältnismäßigkeitsgrundsatz Ausnahmeregelungen vergleichbar dem Aufenthaltsverbot enthalten.

Zuletzt sollte jedenfalls in Bezug auf diese neue Regelung eine Evaluationspflicht ins Gesetz geschrieben werden.

Zusammenfassend halten wir die Regelung von Aufenthaltsvorgabe und Kontaktverbot grundsätzlich für zulässig, die Tatbestandsvoraussetzungen müssen aber enger gefasst werden, es fehlt eine Ausnahmeregelung, und die Effektivität dieser Maßnahmen sollte in zwei Jahren evaluiert werden.

3.3. Elektronische Aufenthaltsüberwachung (§ 17c NPOG-E)

Die in § 17 c geregelte elektronische Aufenthaltsüberwachung (elektronische Fußfessel) stellt durch die damit vorgesehene Erhebung, Speicherung und Nutzung der Aufenthaltstaten des Betroffenen einen dreifachen Eingriff in das Recht auf Informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1) dar. Zudem handelt es sich unserer Ansicht nach auch um eine freiheitsbeschränkende Maßnahme, Art. 2 Abs. 2 S. 2 GG, da durch die Fußfessel erreicht werden soll, dass die Person sich an bestimmten Orten nicht aufhält. Sofern die Person sich in Wohnungen aufhält, ist zudem Art. 13 GG der Wohnungsinhaber*innen betroffen.

Fußfesseln können mangels hinreichender Verdeckungsmöglichkeit stigmatisierend wirken. Äußerst fraglich ist zudem ihre Geeignetheit zur Gefahrenabwehr, da Straftaten auch mit einer elektronischen Fußfessel begangen werden können.

Mit Meldeauflage, Aufenthaltsverbot, Aufenthaltsanordnung und Kontaktverbot stehen zudem mildere Maßnahmen zur Verfügung.

Wir lehnen die Regelung einer elektronischen Fußfessel demnach als verfassungswidrig und ungeeignet ab. Sollte es bei der Regelung bleiben, müssen jedenfalls die Tatbestandsvoraussetzungen enger gefasst werden.

3.4. Präventivgewahrsam (§§ 18 – 21 Nds. SOG/NPOG-E)

Der Präventivgewahrsam soll insoweit ausgeweitet werden, als die Höchstdauer von gegenwärtig zehn Tagen auf 30 Tage Erstanordnung und auf 2 ½ Monate maximale Anordnungszeit ausgeweitet wird.

Eine solche zeitliche Ausweitung des Präventivgewahrsams ist mit Blick auf den hohen Wert der Freiheit der Person unverhältnismäßig. Zehn Tage Präventivgewahrsam wirken unserer Ansicht nach bereits abschreckend genug.

Zudem soll die präventive Ingewahrsamnahme zulässig sein zur Durchsetzung einer Meldeauflage und bei Verstoß gegen die Verpflichtung aus § 17 c NPOG-E, eine elektronische Fußfessel „ständig in betriebsbereitem Zustand am Körper bei sich zu führen, dessen Anlegung zu dulden und dessen Funktionsfähigkeit nicht zu beeinträchtigen".

Damit wird die Ingewahrsamnahme bereits zulässig sein, ohne dass eine konkrete Gefahr vorliegt, vielmehr reichen Tatsachen aus, die das Begehen einer terroristischen Straftat vermuten lassen (siehe oben).

Das verstößt nicht nur gegen Art. 2 II Satz 2 GG sondern auch gegen Art. 5 EMRK. Zur Präventivhaft hat der Europäische Menschenrechtsgerichtshof entschieden, dass diese zur Verhinderung einer Straftat nur zulässig sei, „wenn Ort und Zeitpunkt der bevorstehenden Begehung der Straftat sowie ihr potenzielles Opfer / ihre potenziellen Opfer hinreichend konkretisiert wurden".[30]

Wir lehnen die zeitliche und tatbestandliche Ausweitung des Präventivgewahrsams ab. Sollte der Gesetzgeber aber an der Regelung festhalten, sollte er zugleich auch eine Ordnung für den Präventivgewahrsam schaffen, die berücksichtigt, dass dort Menschen zukünftig nicht mehr nur maximal 10 Tage, sondern 74 Tage lang versorgt werden müssen. Zum Beispiel sollten für die in Gewahrsam Genommenen Sozialarbeiter*innen zur Verfügung stehen.

4. Besondere Datenerhebungsbefugnisse

Das Bundesverfassungsgericht hat mit den Urteilen zum BKA-Gesetz 2016 [31] und zur Online-Durchsuchung 2008 die Grundrechtsgrenzen für Datenerhebungsbefugnisse aufgezeigt.[32] In dem Urteil zur Online-Durchsuchung hat das Bundesverfassungsgericht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geprägt (Art. 2 I i. V. m. Art. 1 GG). Urteile des Bundesverfassungsgerichts zeigen dem Gesetzgeber die äußersten Grenzen gerade noch zulässiger Grundrechtseingriffe auf. Sie machen deutlich, welches Mindestmaß an Grundrechten der deutsche Staat den von ihm betroffenen Menschen zu gewährleisten hat. Sie binden den Gesetzgeber jedoch nicht an dieses Mindestmaß. Der Gesetzgeber sollte vielmehr Grundrechtseingriffe auf ein für die effektive Sicherheitsgewährleistung notwendiges Maß beschränken. Der Gesetzentwurf der Regierungskoalition schöpft aber die Grenzen des gerade noch Zulässigen vielfach aus und überschreitet es in Teilen sogar.

---

30 EGMR, Urteil vom 7.3.2013 - 15598/08 (Präventivhaft eines deutschen Hooligans vor und während des Spiels SV Werder Bremen gegen Eintracht Frankfurt 2004)

31 BVerfG, U. v. 20. April 2016 - 1 BvR 966/09

32 BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 - Rn. (1-333), http://www.bverfg.de/e/rs20080227_1bvr037007.html

5. Kernbereich privater Lebensgestaltung (§ 31 b NPOG-E)

Überwachungsmaßnahmen sind stets verfassungswidrig, wenn sie den Kernbereich privater Lebensgestaltung nicht hinreichend beachten und damit in die Menschenwürde des 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.[33] Zu den kernbereichsnahen Überwachungsmaßnahmen gehören die Wohnraumüberwachung, die Online-Durchsuchung sowie die Telekommunikationsüberwachung (TKÜ). Für diese und andere Überwachungsbefugnisse sieht der NPOG-E in § 31 b als zentrale Norm Regelungen vor, die den Schutz des Kernbereichs privater Lebensgestaltung gewährleisten sollen. Diese zentrale Regelung wird jedoch den Anforderungen, die an einen verfassungsmäßig ausgestalteten Kernbereichsschutz zu stellen sind, teilweise nicht gerecht.

Zunächst ist festzuhalten, dass die Anforderungen, die an kernbereichsschützende Regelungen zu stellen sind, zwar stets dem vom Bundesverfassungsgericht entwickelten zweistufigen Schutzkonzept entsprechen müssen, je nach Art der Datenerhebung aber im Einzelnen differieren.[34] Soll dem Kernbereichsschutz für unterschiedliche Befugnisnormen durch eine gemeinsame zentrale Regelung Rechnung getragen werden, ergibt sich daraus zwangsweise, dass die Anforderungen stets der Überwachungsbefugnis mit dem strengsten Maßstab zu entsprechen haben.

5.1. Wirksamer Kernbereichsschutz muss bei der Datenerhebung ansetzen

Das vom Bundesverfassungsgericht zum Schutz des Kernbereichs privater Lebensgestaltung entwickelte Konzept sieht vor, dass der Gesetzgeber Vorkehrungen vorzusehen hat, die den Schutz dieses Kernbereichs gewährleisten. Solche Schutzvorkehrungen müssen sowohl bei der Datenerhebung (1. Stufe) als auch bei der Datenverwendung und -verarbeitung (2. Stufe) vorhanden sein. Das Bundesverfassungsgericht hat dem Gesetzgeber für seine Verpflichtung zum Schutz des Kernbereichs einen relativ großen Spielraum überlassen und sogar festgestellt, dass nicht jede tatsächliche Erfassung von höchstpersönlichen Informationen stets einen Verfassungsverstoß begründet und den Schwerpunkt des Kernbereichsschutzes bei der Online-Durchsuchung auf der 2. Stufe des Schutzkonzeptes als ausreichend erachtet.[35] Die Humanistische Union weist jedoch darauf hin, dass Schutzmaßnahmen, die erst auf der Stufe der Datenverarbeitung und -verwendung greifen, bereits bei der Datenerhebung eingetretene Kernbereichsverletzungen lediglich noch kompensieren können. Damit wird deutlich, dass ein wirksamer Kernbereichsschutz letztendlich bei der Datenerhebung ansetzen muss, d.h. dass bereits die Erhebung höchstpersönlicher Informationen, wie tagebuchähnliche Aufzeichnungen und Kommunikation mit Vertrauenspersonen, zu unterlassen sind.[36] Soweit dies z.B bei der Online-Durchsuchung nach Art der Maßnahme nicht möglich ist, ist die Einführung entsprechender Befugnisnormen aus Sicht der Humanistischen Union grundsätzlich zu überdenken.

---

33 BVerfG, U. v. 20. April 2016 - 1 BvR 966/09 - Rn. (124).

34 BVerfG, U. v. 20. April 2016, a.a.O. - Rn. (126 f.).

35 BVerfG, U. v. 20. April 2016, a.a.O. - Rn. (124 und 218)

36 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

5.2. Mangelhafter Kernbereichsschutz für die Online-Durchsuchung

Nach dem Bundesverfassungsgericht hat der Gesetzgeber auf der Ebene der Datenerhebung Vorkehrungen zu treffen, die eine unbeabsichtigte Miterfassung von Kernbereichsinformationen nach Möglichkeit ausschließen.[37] 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.[38] Bei der Online-Durchsuchung, bei der eine Nichterhebung von kernbereichsrelevanten Daten praktisch nicht ausschließbar ist, ist gesetzlich vorzusehen, 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.[39] Ein solcher Einsatz von technischen Sicherungen zur Vermeidung der Erhebung kernbereichsrelevanter Daten ist in § 31 b Abs. 1, der den Kernbereichsschutz für die Ebene der Datenerhebung im Wesentlichen regelt, nicht vorgesehen.

5.3. Mangelhafte Regelung zum Abbruch der Datenerhebung

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.[40] Im vorliegenden Gesetzentwurf ist mit § 31 b Abs. 2 zwar eine solche Unterbrechung der Datenerhebung vorgesehen, die Regelung verengt die Pflicht zum Abbruch jedoch in nicht verfassungskonformer Weise, indem sie Ausnahmen für solche Fälle vorsieht, in denen eine Unterbrechung 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"[41] den Abbruch der Maßnahme vorsieht.

5.4. Umfangreichere Protokollierung bei Datenlöschung erforderlich

Sind kernbereichsrelevante Daten trotz aller Vorkehrungen gleichwohl erhoben worden, ist für diese Fälle im Gesetz eine sofortige Löschung vorzusehen. Zudem hat das Gesetz zu regeln, dass die Löschung in einer Art und Weise protokolliert wird, die eine spätere Kontrolle ermöglicht.[42] § 32 b Abs. 2 S. 3 NPOG-E sieht vor, dass für solche Fälle die Tatsache der Erhebung und der Löschung dokumentiert wird. Die Dokumentation dieser Daten ist jedoch für eine spätere Kontrolle unzureichend. Für eine spätere Kontrolle dürfte erforderlich sein, dass zumindest auch der Zeitpunkt der Löschung und die Person, die die Löschung vorgenommen hat, protokolliert werden.

5.5. 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

37 BVerfG, U. v. 20. April 2016- 1 BvR 966/09 - Rn. (126).

38 BVerfG, U. v. 20. April 2016, a.a.O. - Rn. (128).

39 BVerfG, U. v. 20. April 2016, a.a.O. - Rn. (219).

40 BVerfG, U. v. 20. April 2016, a.a.O. - Rn. (128).

41 BVerfG, U. v. 20. April 2016, a.a.O. - Rn. (128).

42 BVerfG, U. v. 20. April 2016, a.a.O. - Rn. (129).

Stelle im Gesetz vorzusehen.[43] Als zwingend sieht es eine solche Sichtung für die Wohnraumüberwachung und Online-Durchsuchung an.[44] 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).[45] Diesem Maßstab wird der Gesetzentwurf, der in § 32b Abs. 4 regelt, dass eine gerichtliche Entscheidung darüber zu ergehen hat, „ob Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erhoben wurden", nicht in vollem Umfang gerecht. Zum einem lässt die Norm 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.[46]

6. Body-Cams (§ 32 Abs. 4 S. 2 NPOG-E)

Die Humanistische Union sieht die Einführung von Body-Cams kritisch, da mit dem Einsatz der Kameras ein Grundrechtseingriff verbunden ist und sowohl die Geeignetheit des Einsatzes von Body-Cams als auch die Erforderlichkeit äußerst fraglich sind.

Für den Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtags hat die Humanistische Union im Jahr 2016 eine umfassende und quellenbasierte Stellungnahme zur Einführung von Body-Cams[47] erarbeitet, auf deren Lektüre an dieser Stelle verwiesen wird. Vorliegend sollen nur folgende Punkte hervorgehoben werden:

6.1. Geeignetheit der Maßnahme ungeklärt und zweifelhaft

Bezüglich der Geeignetheit weisen wir zunächst darauf hin, dass Body-Cams in der Fachliteratur mit Blick auf zwei mögliche Ziele diskutiert werden: 1. Verhinderung und Nachweisbarkeit rechtswidrig ausgeübter Polizeigewalt, 2. Verhinderung und Nachweisbarkeit von Straftaten von Bürger*innen gegenüber Polizist*innen. Der vorliegende Gesetzentwurf verfolgt nur letzteren Zweck.

a) Nutzen zur Verhinderung rechtswidriger Polizeigewalt

Die Humanistische Union bedauert zunächst, dass sich die niedersächsische Regierungskoalition im Zuge der beabsichtigten Einführung von Body-Cams nicht mit den in der Bundesrepublik bestehenden Defiziten bei der Aufklärung und Ahndung rechtswidriger Polzeigewalt[48] befasst hat.

---

43 BVerfG, U. v. 20. April 2016, a.a.O. - Rn. (129).

44 BVerfG, U. v. 20. April 2016, a.a.O. - Rn. (200 und 218).

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

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

47 Stellungnahme der Humanistischen Union zur Anhörung des Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtages zum Antrag der Fraktion der CDU „Body-Cams unverzüglich einsetzen" (Drs. 18/3849) und dem Änderungsantrag der Fraktion der PIRATEN „Überwachungskameras verhindern keine Gewalt gegen Polizeibeamte" (Drs. 18/3886) [Drs. 18/ 6091] (Autorin: Anja Heinrich) – abrufbar unter: http://www.landtag.ltsh.de/infothek/wahl18/umdrucke/6000/umdruck-18-6091.pdf.

48 Vgl. Singelnstein, Institutionalisierte Handlungsnormen bei den Staatsanwaltschaften im Umgang mit Ermittlungsverfahren wegen Körperverletzung im Amt, in: Monatsschrift für Kriminologie und Strafrechtsreform 1/2003; Luczak, Gewalttätige Polizei – Eine Fortsetzungsgeschichte, in: Müller-Heidelberg u.a. (Hrsg.), Grundrechte-

Die Frage nach der Wirksamkeit der Body-Cams hinsichtlich der Aufklärung und Ahndung rechtswidriger Polizeigewalt kann nicht eindeutig beantwortet werden. Fest steht jedoch, dass es bei der Eignung maßgeblich auf die Ausgestaltung der zugrundliegenden Regelungen und insbesondere darauf ankommt, ob die Polizeibeamt*innen selbst darüber entscheiden, wann aufgezeichnet wird und ob sie nach der Maßnahme „Herr über die Bilder sind", sprich über die Notwendigkeit der weiteren Speicherung und den Umfang der zu speichernden Bild-Sequenzen selbst entscheiden, oder ob die Daten ohne Zugriffsmöglichkeit der Polizeibeamt*innen zentral gespeichert werden.

Die vorliegende Regelung ist derart ausgestaltet, dass ein signifikanter Nutzen zur Verhinderung und Aufklärung rechtswidrig ausgeübter Polizeigewalt nicht zu erwarten ist.

b) Wirksamkeit zur Bekämpfung von Straftaten gegenüber Polizist*innen

Die Wirksamkeit von Body-Cams zur Bekämpfung von Straftaten gegenüber Polizeivollzugsbeamt*innen ist bisher ungeklärt.

Insbesondere ist ein Nachweis für die Wirksamkeit nicht etwa durch das in der politischen Debatte häufig genannte und auch in der Begründung des vorliegenden Gesetzentwurfs erwähnte hessische Modellprojekt „Einsatz mobiler Videoüberwachung"[49] erfolgt. Denn diesem Modellprojekt, das von Befürwortern der Body-Cams vielfach als erfolgreich verkauft wird, fehlt es an wissenschaftlichen Standards (insbesondere einer repräsentativen Fallzahl), die zuverlässige Rückschlüsse auf die Wirksamkeit zulassen. Zudem belegen die Zahlen des hessischen Modellprojekts keinen signifikanten Rückgang von Widerstandshandlungen. So kam es in den 2 Testgebieten des Modellprojekts in einem Gebiet zur Reduzierung von Widerstandshandlungen, in dem anderen zu einem leichten Anstieg.[50]

Auch allgemeine Überlegungen zur möglichen Wirkungsweise von Body-Cams – insbesondere für die Verhinderungen von Straftaten gegenüber Polizist*innen - lassen an der Wirksamkeit zweifeln, da sich ein von den Kameras ausgehender Abschreckungseffekt nicht überzeugend begründen lässt. Die den Body-Cams zugeschriebene Abschreckungswirkung wird in der Regel mit der den Bürger*innen vor Augen geführten Schaffung von Beweismitteln für ein mögliches Strafverfahren begründet. Eine durch die Body-Cams gesteigerte Abschreckungswirkung kann sich im Umkehr-Schluss damit jedoch nur ergeben, wenn ohne den Einsatz von Body-Cams entsprechende Beweisdefizite bestünden. Dies ist jedoch nicht der Fall. Vielmehr liegt die Aufklärungsquote bei nahezu 100 %.[51]

6.2. Erforderlichkeit der Maßnahme nicht belegt

Die verfassungsrechtliche Erforderlichkeit dürfte aufgrund der bundesverfassungsgerichtlich weit verstandenen Einschätzungsprärogative des Gesetzgebers zwar gegeben sein. Die politische und tatsächliche Notwendigkeit der Maßnahme ist jedoch in keinster Weise dargelegt. Soweit der Gesetzentwurf pauschal auf eine steigende Zahl von Straftaten gegenüber Polizeibeamt*innen verweist, fehlt es gänzlich an entsprechenden Belegen.

Report 2015, S. 33 ff.; Amnesty International, „Nichts zu verbergen" –Transparenz schützt Menschenrechte: Mehr Verantwortung bei der Polizei, Bericht 2010.

49 Hessisches Polizeipräsidium, Abschlussbericht über die Erfahrungen des Einsatzes der mobilen Videoüberwachung gemäß § 14 Abs. 6 HSOG i.R.d. Maßnahmen „Alt-Sachsenhausen" sowie im Bereich des 1. Polizeireviers des Polizeipräsidiums Frankfurt am Main 2014.

50 Stellungnahme der HU zu Body-Cams (Schleswig-Holstein), a.a.O. (S. 5 f.).

51 Stellungnahme der HU zu Body-Cams (Schleswig-Holstein), a.a.O. (S. 6 f.).

7. TKÜ und Quellen-TKÜ (§ 33 a NPOG-E)

7.1. Regelungsflut

Vor dem Hintergrund, dass der Bundesgesetzgeber die präventive TKÜ sowie die Quellen-TKÜ im Gefahrenvorfeld zur Terrorabwehr ins Bundeskriminalamtsgesetz eingefügt hat, stellt sich die Frage nach der tatsächlichen Notwendigkeit zusätzlicher derart eingriffsintensiver Regelungen auf Landesebene.

7.2. Eingriffsschwelle

Für die mit einem Eingriff in das Telekommunikationsgeheimnis (Art. 10 GG) verbundene TKÜ nach § 30a Abs. 1 soll die Eingriffsschwelle erheblich abgesenkt werden. Während das bisherige Gesetz eine Telekommunikationsüberwachung nur unter der Voraussetzung einer gegenwärtigen Gefahr für bestimmte Rechtsgüter zulässt, soll die grundrechtsintensive Telekommunikationsüberwachung künftig bereits im Gefahrenvorfeld zulässig sein.

Die in § 33a Abs. 2 geregelte Quellen-TKÜ greift durch den mit ihr verbundenen Eingriff in informationstechnische Systeme nicht nur in das Telekommunikationsgeheimnis (Art. 10 GG), sondern durch die Beeinträchtigung der Integrität dieser Systeme auch in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. i. V. m. 1 Abs. 1 GG) ein. Ein solcher Eingriff ist damit gleichwohl schwieriger zu rechtfertigen, denn ein solcher Eingriff stellt stets einen Grundrechtseingriff von großer Intensität dar, denn im Gegensatz zu beispielsweise einem klassischen Telefon oder einer Schreibmaschine, die für einen eng umrissenen Zweck konzipiert und eingesetzt wird, ist ein Computer – PC, Table-Computer oder Smartphone – eine universell einsetzbare Maschine, deren Einsatzzweck nicht von vorneherein bestimmt werden kann. Damit entstehen bei der Quellen-TKÜ Gefahren für das Persönlichkeitsrecht des Menschen, die denjenigen der Online-Durchsuchung in vielfacher Weise entsprechen: Zwischen Quellen-TKÜ und Online-Durchsuchung kann technisch nicht unterschieden werden; die technischen Schritte zur Aufbringung von Software für die Quellen-TKÜ oder die Online-Durchsuchung sind weitgehend identisch.[52] Für die für derartige Eingriffe verwendete Software hat sich mittlerweile die Bezeichnung „Staatstrojaner" eingebürgert. Bezüglich der mit der Verwendung von Staatstrojanern verbundenen Gefahren, insbesondere in Bezug auf die Kompromittierung der öffentlichen Infrastruktur, wird auf die Ausführungen zur Online-Durchsuchung verwiesen.

§ 33 a Abs. 1 und 2 NPOG-E sehen mittels TKÜ und Quellen-TKÜ sowohl die Überwachung als auch die Aufzeichnung des Telekommunikationsverkehrs vor. Aufgrund der unterschiedlichen Eingriffsintensität sollte die Norm jedoch konkret regeln, unter welchen besonderen Voraussetzungen die eingriffsintensivere Aufzeichnung zulässig sein soll.

7.3. Die Quellen-TKÜ kann technisch nicht auf laufende Kommunikationsvorgänge eingegrenzt werden

Es bestehen erhebliche Zweifel an der Eingrenzbarkeit der Quellen-TKÜ auf laufende Kommunikation, wie in § 33a Abs. 2 Satz 1 NPOG-E gefordert. Es kann technisch nicht zuverlässig zwischen Kommunikations- und anderen Prozessen auf dem Rechnersystem unterschieden werden. Beispielsweise müsste eine E-Mail bei der Überwachung vor ihrer Verschlüsselung und Versendung

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

auf dem Zielsystem abgegriffen werden. Zu diesem Zeitpunkt kann nicht sicher entschieden werden, ob die E-Mail überhaupt versendet oder lediglich im Entwurfsordner abgelegt werden soll.[53]

7.4. Richtervorbehalt

Es fehlt für die TKÜ und Quellen-TKÜ an einem hinreichenden Richtervorbehalt.

Nach dem Bundesverfassungsgerichtsurteil zum BKA-Gesetz bedürfen eingriffsintensive heimliche Überwachungsmaßnahmen, bei denen damit zu rechnen ist, dass auch höchstprivate Informationen erfasst werden, eines Richtervorbehalts oder einer anderweitigen unabhängigen vorherigen Kontrolle. Wobei der Gesetzgeber zu normieren hat, 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.

7.5. Dauer der Maßnahme

Die Humanistische Union bedauert zudem, dass für die TKÜ und die Quellen-TKÜ keine zeitliche Höchstgrenze vorgesehen ist. Gem. § 33 a Abs. 5 S. 3 NPOG-E kann die Maßnahme oft um jeweils 3 Monate verlängert werden. Damit ermöglicht die Norm eine unbegrenzte, also jahre- oder gar jahrzehntelange, Überwachung von Telefonaten, E-Mails, SMS und Messengerdienstnachrichten.

8. Online-Durchsuchung (§ 33 d NPOG-E)

Die im Gesetzentwurf vorgesehene neue Regelung zur Online-Durchsuchung ist aus Sicht der Humanistischen Union verfassungswidrig, denn die in § 33 d NPOG-E geregelten Eingriffsvoraussetzungen werden den Anforderungen der im Bundesverfassungsgerichtsurteil zum BKA-Gesetz aufgestellten Maßstäbe nicht gerecht.

Die Online-Durchsuchung stellt einen äußerst schwerwiegenden Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG) dar. Entsprechend hohe Anforderungen bestehen an ihre Rechtfertigung.

8.1. Eingriffsschwelle

Soweit die Regelung in § 33 d Abs. 1 S. 2 Nr. 2 NPOG-E die Online-Durchsuchung im Gefahrenvorfeld zulässt, ist sie unverhältnismäßig, denn sie erfüllt die Voraussetzungen, die an eine Online-Durchsuchung im Gefahrenvorfeld bestehen, nicht.

Das Bundesverfassungsgericht hat im Urteil zum BKA-Gesetz klargestellt, dass heimliche Überwachungsmaßnahmen zulässig sind, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie Straftaten in überschaubarer Zukunft begehen wird, sofern es sich bei diesen Straftaten um terroristische Straftaten handelt.

§ 33 d Abs. 1 S. 2 Nr. 2 NPOG-E setzt für die Online-Durchsuchung im Gefahrenvorfeld zwar ein individuelles Verhalten voraus, das eine entsprechende konkrete Wahrscheinlichkeit begründet, nicht jedoch, dass sich die Wahrscheinlichkeit auf eine terroristische Straftat bezieht. Ausreichen soll vielmehr jede Schädigung von Leib, Leben oder Freiheit einer Person oder solcher Güter der Allgemeinheit, deren Bedrohung die Grundlage oder den Bestand des Bundes oder eines Landes oder

53 Dazu Fredrik Roggan (2017), a.a.O., S. 824

die Grundlagen der Existenz der Menschen berührt. Ein Bezug zu einer terroristischen Straftat wird nicht vorausgesetzt.

8.2. Eingrenzung der zulässigen Maßnahmen

Die in § 33 d NPOG-E geregelte Online-Durchsuchung ermöglicht Eingriffe in alle denkbaren informationstechnischen Systeme, also 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" muss dieser Kreis sehr weit gefasst werden; die Intensität von möglichen Eingriffen ist entsprechend hoch anzusetzen. Vor diesem Hintergrund empfiehlt sich, die polizeilich überwachbaren Systeme in § 33 d NPOG-E einzugrenzen.[54]

8.3. Der physische Zugriff auf ein informationstechnisches System erfordert einen Eingriff in die Unverletzlichkeit der Wohnung

Die Software[55] zur Durchführung der Online-Durchsuchung kann bei unmittelbarem Zugriff durch Aufspielen installiert werden. „Eine Methode zur Manipulation eines informationstechnischen Systems besteht im unmittelbaren, physischen Zugriff. Nur auf diese Weise kann – was gelegentlich übersehen wird – ausgeschlossen werden, dass beispielsweise Rechner von unbeteiligten Dritten ebenfalls in den Fokus der Ermittler geraten".[56] Dies ist mit einem Eingriff in die Unverletzlichkeit der Wohnung, Art. 13 Abs. 1 GG, verbunden.[57]

8.4. Externer Zugriff auf das informationstechnische System bedingt als Konsequenz die Kompromittierung der öffentlichen Infrastruktur

Neben dem physischen Zugriff auf das zu überwachende System kommt zur Infiltrierung vor allem der externe Zugriff über eine Online-Verbindung und das Aufspielen einer entsprechenden Software in Betracht. Dieser verdeckte Eingriff in das informationstechnische System setzt voraus, dass es im Zielsystem ein „Einfallstor" gibt, das für die Maßnahme genutzt werden kann. Solche Einfallstore sind Sicherheitslücken im zu überwachenden System, die durch sog. „Exploits"[58] ausgenutzt werden.

Ebenso wie Straftäter sind also Strafverfolgungsbehörden darauf angewiesen, Sicherheitslücken bzw. die auf ihnen fußenden Exploits für die Quellen-TKÜ bzw. Online-Durchsuchung zu nutzen. In diesem Sinn sind Staatstrojaner nichts anderes als Schadcode, der auf dem zu infizierenden System installiert wird. Um die Wahrscheinlichkeit für den Erfolg der Maßnahme zu erhöhen, werden insbesondere

---

54 Es sei aber darauf hingewiesen, dass Schadsoftware nicht zwischen verschiedenen Anwendungen unterscheidet und alle Systeme schädigen kann, solange sie auf der gleichen technischen Plattform basieren.

55 Solche Software wird als „Remote Forensic Software" (RFS) bezeichnet. Dieser Begriff ist irreführend: Er kann suggerieren, dass die damit gewonnenen Erkenntnisse den Beweiswert einer forensischen Analyse besitzen, was nicht der Fall ist. Dazu Dirk Fox (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.

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

57 ebd.

58 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.

Zero-Day-Exploits benötigt. Die Sicherheitslücken können durch entsprechende Analysen selbst „entdeckt" oder auf dem Schwarzmarkt erworben werden. Aufgrund des Aufwands für die Entdeckung von Schwachstellen wird es in der Praxis häufig zum Kauf solcher Sicherheitslücken und Exploits auf dem Schwarzmarkt kommen. Eine dritte Möglichkeit ist die bewusste Schaffung von Sicherheitslücken durch staatliche Stellen, beispielsweise durch die Standardisierung schwacher Sicherheitsstandards.

Die Folge ist in allen Fällen die gleiche: Es werden bewusst und vorsätzlich Sicherheitslücken geschaffen oder aufrechterhalten, die auch durch Dritte – beispielsweise in krimineller oder terroristischer Absicht – ausgenutzt werden können. Neben dem unmittelbaren Risiko der Nutzung solcher Sicherheitslücken untergräbt dies langfristig die Vertrauenswürdigkeit und damit die Funktionsfähigkeit der technischen Infrastruktur. Eine sichere Infrastruktur ist 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 Sicherheitslücken potenziell Terroristen ein Werkzeug in die Hand gegeben wird, durch das sie weiteren, erheblichen Schaden verursachen können, der prinzipiell unbegrenzt ist und möglicherweise den durch einen Ermittlungserfolg verhinderten Schaden bei Weitem übersteigt. Unter diesem Gesichtspunkt ist es besonders zu bedauern, dass der Gesetzentwurf keinerlei Vorgaben zur Einschätzung möglicher Folgeschäden oder zur Reduzierung des entstehenden Risikos enthält.

Ein Beispiel für eine Schadsoftware, die solchen Schaden verursachen kann, ist der Ransomware-Trojaner WannaCry[59], 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.[60]

Durch den Ankauf von Sicherheitslücken und Exploits sorgen staatliche Stellen 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.[61]

---

59 Volker Brigleb, 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

60 Das Beispiel zeigt auch, dass die Wirkung der Schadsoftware nicht an Landesgrenzen Halt macht. Damit stellt sich die Frage nach Cyberangriffen auf souveräne Staaten durch den Einsatz dieser Software. Wird dadurch physischer Schaden verursacht, verletzten solche Angriffe nach Ansicht internationaler Experten die Souveränität; ob das auch gilt, wenn kein physischer Schaden verursacht wird, darüber besteht jedoch keine Einigkeit. Vgl. dazu Michael N. Schmitt (Hg.) (2013): Tallinn Manual on the International Law applicable to Cyber Warfare, Cambridge, UK u. a.: Cambridge University Press, Section 1, A 6.

61 Rainer Rehak (2018): Stellungnahme des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) zur öffentlichen mündlichen Anhörung des Hessischen Landtags am 8. Februar 2018 zum Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur 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

Der Staat begibt sich also in einen erheblichen Zielkonflikt: Durch die Nutzung von Software zum Eingriff in informationstechnische Systeme zur Verhinderung von Straftaten fördert er sie gleichzeitig in erheblichem Maß.[62]

8.5. Die Rechtmäßigkeit der verwendeten Software kann nicht sichergestellt werden

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.[63]

Diese Prüfung der Rechtmäßigkeit kann nur in Kenntnis der Funktionsweise der Software und damit des Quelltexts durch sachkundige Experten erfolgen. In der Vergangenheit wurde in der Praxis neben Eigenentwicklungen auch kommerzielle, proprietäre Software für die Maßnahmen vorgesehen.[64] Eine Prüfung der Rechtmäßigkeit kann so nicht ohne Weiteres geleistet werden; der Gesetzentwurf enthält auch keinerlei Vorgaben für das Vorgehen in einem solchen Fall.

Der Gesetzentwurf schreibt nicht fest, dass ausschließlich staatlicherseits erstellte Software für die Überwachung eingesetzt werden darf. Damit kann auch Software externer Anbieter verwendet werden. Eine „Whitelist" von Softwareprodukten, die in diesen Fällen zulässig sind, ist jedoch offenbar nicht vorgesehen. Auch von einer Zertifizierung der Software durch eine unabhängige Zertifizierungsstelle ist nicht die Rede.

Auch wenn – bei Gefahr im Verzug – auf eine richterliche Anordnung verzichtet wird, bleibt es für den mit der Entscheidung betrauten Polizeibeamten faktisch unmöglich, die Konsequenzen seiner Entscheidung zu beurteilen. Aufgrund der technischen und organisatorischen Vorbereitungen und damit verbundenen Vorlaufzeiten, die der Einsatz einer solchen Trojanersoftware erfordert, ist die kurzfristige Anordnung einer solchen Maßnahme aber ohnehin zweifelhaft (entsprechendes gilt bei der Quellen-TKÜ).[65]

8.6. Durchsuchungsergebnisse können manipuliert werden

Die Kompromittierung eines IT-Systems ermöglicht weitgehende Manipulation bis hin zur Ablage kompromittierender Dateien. Ebenso wie die Ermittlungspersonen sind die zu überwachenden Zielpersonen technisch prinzipiell in der Lage, die Ermittlungsergebnisse in ihrem Sinne zu manipulieren.[66] Damit haben die erhobenen Daten keine forensische Beweiskraft.

---

62 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)".: Fredrik Roggan (2017), a.a.O., S. 828-829

63 Fredrik Roggan (2017), .a.a.O. S. 824

64 Zum Beispiel das Produkt FinSpy des Münchener Herstellers FinFisher, der zur Gamma Group gehört, oder Produkte der Firma DigiTask, die mittlerweile zum Konzern Rohde & Schwarz gehört, der auch mit der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITIS) kooperiert. Vgl. dazu Stefan Krempl (2018): Geheimdokumente: BKA bastelt weiter an Bundestrojaner für Online-Durchsuchungen. heise.de, 12. Juli 2018, https://www.heise.de/newsticker/meldung/Geheimdokumente-BKA-bastelt-weiter-an-Bundestrojaner-fuer-Online-Durchsuchungen-4108952.html

65 Generell ist die Eignung der Quellen-TKÜ bzw. der Online-Durchsuchung als Ermittlungsmethode bei Gefahr im Verzug aufgrund seiner langen Vorbereitungszeiten prinzipiell ungeeignet, siehe Dirk Fox (2007), a.a.O.

66 Dirk Fox (2007), a.a.O.

8.7. Die Eingriffe in die informationstechnischen Systeme müssen rechtssicher dokumentiert werden

Der Gesetzentwurf sieht geeignete Dokumentationspflichten weder für die Maßnahme selbst noch für die Herstellung bzw. Beschaffung der genutzten Spionagesoftware und die Herstellung bzw. Beschaffung der genutzten Sicherheitslücken und Exploits vor. Aufgrund des Schwarzmarktcharakters solcher Schadsoftware müssen sich staatliche Ermittlungsbehörden notwendig in einen rechtlichen Graubereich begeben, der zu seiner rechtsstaatlichen Absicherung einer akribischen Nachvollziehbarkeit und Rechtfertigung bedarf.

Auch die Eingriffe selbst müssen rechtssicher dokumentiert werden und nachvollziehbar sein. Die Möglichkeit rechtssicherer Dokumentation eines Eingriffs ist aber auf einem fremden System in der Regel sehr eingeschränkt, da dieses System, wenn es nicht vollständig durch die Ermittlungsbeamten kontrolliert wird, manipuliert werden kann.

Eine exakte Dokumentation und Nachvollziehbarkeit wäre aufgrund der weitgehenden Eingriffsmöglichkeiten aber erforderlich. Die Kompromittierung eines IT-Systems ermöglicht weitgehende Manipulation bis hin zur Ablage kompromittierender Dateien. Nur eine rechtssichere Dokumentation kann solche Manipulationen ausschließen. Auch die kryptographische Absicherung solcher Protokolle kann die Authentizität nicht gewährleisten, da die dafür benötigten Schlüssel auch durch das infiltrierte System zugreifbar wären.

8.8. Der Missbrauch der erhobenen Daten muss ausgeschlossen werden

Der Entwurf enthält keine Maßnahmen zur wirksamen Verhinderung von Missbrauch der erhobenen Daten. Die Erfahrung zeigt, dass das Risiko eines solchen Missbrauchs nicht ausgeschlossen werden kann.[67] 2012 löste ein Streit zwischen einem Vater – Beamter der Bundespolizei – und seiner Tochter einen Angriff auf Systeme der Bundespolizei aus. Der Vater hatte einen Trojaner auf dem Rechner seiner Tochter installiert, um sie überwachen zu können. Ein Freund der Tochter untersuchte daraufhin den Rechner des Beamten und erhielt dadurch Zugang zu dienstlichen E-Mails und zu den Systemen der Bundespolizei.[68] Mitarbeiter der NSA missbrauchten offenbar Spionagewerkzeuge auch regelmäßig für private Zwecke.[69]

9. Einsatz von Tasern (§ 69 Abs. 4 NPOG-E)

Die Humanistische Union hat große Bedenken gegen die standardmäßige Einführung der Elektroimpulsgeräte (Taser).

Durch die Anwendung von Tasern gegen eine Person wird deren körperliche Gesundheit massiv beeinträchtigt. Zudem hat das Antifolterkomitee der UNO im Jahr 2007 in Bezug auf das gängige Model X26 starke Bedenken geäußert, weil diese Geräte derartig intensive Schmerzen verursache, dass die Anwendung eine Art der Folter darstelle und unter Bestimmten Umständen auch den Tod

67 Stellungnahme des Chaos Computer Club zur öffentlichen mündlichen Anhörung des Hessischen Landtags am 8. Februar 2018 zum Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen: Hessischer Landtag, Ausschussvorlagen – Teil 3, S. 290-305, https://hessischer-landtag.de/sites/default/files/scald/files/INA-AV-19-63-T3-NEU.pdf

68 Patras – Vater-Tochter-Streit löst Angriff auf Bundespolizei aus, https://www.golem.de/1201/88870.html, 8. Januar 2012

69 NSA staff used spy tools on spouses, ex-lovers, https://www.reuters.com/article/us-usa-surveil- lance-watchdog/nsa-staff-used-spy-tools-on-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927, 27. September 2013

verursachen kann.[70] Zudem bestehen bei besonderen Risikogruppen (z.B. Menschen mit Herzerkrankungen und Drogenkonsumenten) bei allen Geräten gesundheitliche Risiken.[71] Hinzu kommt, dass infolge des mit dem Einsatz zwangsläufig verbundenen Sturzes des Betroffenen hohe Verletzungsfolgen bestehen.

Vor diesem Hintergrund lehnt die Humanistische Union die standardmäßige Einführung des Taser in Niedersachsen ab. Aufgrund der mit seinem Einsatz verbundenen Risiken sollte er allenfalls als Alternative für Schusswaffen fungieren. Soweit die Gesetzesbegründung darauf verweist, dass der Einsatz von Tasern per Erlass ausdrücklich auf solche Fälle beschränkt „wurde", bei denen durch den Gebrauch die Anwendung von „Waffen" vermieden werden kann, ist dies in vielfacher Hinsicht nicht ausreichend. Zum einen ist unklar, ob der Erlass sich ausschließlich auf das erwähnte Pilotprojekt beim SEK bezieht oder nach Verabschiedung des vorliegenden Gesetzentwurfs auch auf den allgemeinen Gebrauch der Taser Anwendung findet. Zum anderen ist der Taser zwar als milderes Mittel gegenüber dem letalen Schusswaffeneinsatz anzusehen, nicht jedoch gegenüber dem Gebrauch eines Schlagstocks, der ebenfalls eine Waffe i. S. d. § 69 Abs. 4 darstellt, und unter Umständen auch nicht gegenüber Schusswaffen, die nicht tödlich eingesetzt werden. Hinzukommt, dass der Gesetzgeber die mit einem Grundrechtseingriff verbundenen wesentlichen Entscheidungen aufgrund des verfassungsrechtlich verankerten Vorbehaltes des Gesetzes stets selbst zu treffen hat. Zu den wesentlichen Fragen des mit dem Tasereinsatz verbundenen Grundrechtseingriffs gehören ohne Zweifel die Voraussetzungen und Grenzen des Tasereinsatzes. Die bloße Regelung in einem Erlass wäre damit ohnehin verfassungswidrig.

10. Versammlungsgesetz: Vermummungsverbot (§ 20 Abs. 2 Nr. 5 VersG-E)

Die Humanistische Union lehnt die Pönalisierung von Verstößen gegen das Vermummungsverbot ausdrücklich ab.

10.1. Zum Vermummungsverbot allgemein

Das Vermummungsverbot entspringt einem veralteten Verständnis vom Bürger-Staat-Verhältnis und ist nicht mehr zeitgemäß. Denn Bürger*innen haben ein berechtigtes Interesse daran, bei der Teilnahme an einer Versammlung anonym bleiben zu dürfen. Ein solches Bedürfnis kann insbesondere durch Angst vor Repressionen von Andersdenkenden (z.B. Gegendemonstranten), dem Arbeitgeber oder dem persönlichen Umfeld nachvollziehbar begründet sein. Darüber hinaus sind Versammlungen vielfach auch dadurch geprägt, dass die Versammlungsteilnehmer durch kreative Aufmachungen auf ihr Anliegen aufmerksam machen. Auch diese Freiheit der Versammlungsteilnehmer*innen, selbst zu entscheiden, in welcher Art und Weise Meinungsbildung und –äußerung erfolgen sollen (sog. Gestaltungsfreiheit), ist Teil der von Art. 8 GG geschützten Versammlungsfreiheit.[72] In diese Gestaltungsfreiheit greifen § 9 Abs. 2 Nr. 1 und § 20 Abs. 2 Nr. 5 ein. Soweit § 9 Abs. 2 Nr. 1 zwar nur solche Aufmachungen verbietet, die zur Verhinderung der Feststellung der Identität nicht nur geeignet, sondern auch bestimmt sind, ist zu beachten, dass es sich bei letzterem um eine rein

70 CAT/C/PRT/CO/4 2008, S. 5

71 Prof. Dr. Clemens Arzt in seiner Stellungnahme für den Landtag Nordrhein-Westfalen (Drs. 16/4608) unter Verweis auf White, Michael D./ Ready, Justin, „The TASER as a Less Lethal Force Alternative: Findings on Use and Effectiveness in a Large Metropolitan Police Agency", Police Quarterly 2007, S. 170-191; Leitgeb, Norbert/ Niedermayr, Florian/ Loos, Gerhart/ Neubauer, Robert Cardiac fibrillation risk of TASER X-26 dart mode application, Wiener Medizinische Wochenschrift 2011, 161/23–24: 571–577; Bux, Roman/ Andresen, Dietrich/ Rothschild, Markus Alexander, „Elektrowaffe ADVANCED TASER M 26", Rechtsmedizin 2002, 207-213; Banaschak, Sibylle/ Milbradt, Horst/ Roll, Peter/ Madea, Burkhard, „Zum Nachweis der Anwendung von Elektroschockgeräten", Archiv für Kriminologie 2001, 149-158.

72 BVerfGE 69, 315 (343).

subjektive Voraussetzung handelt, die selbst im Rahmen eines gerichtlichen Verfahrens kaum rechtssicher feststellbar ist; geschweige denn von PolizistInnen im Rahmen des Versammlungsgeschehens vor Ort. Aus diesem Grund führt das Vermummungsverbot zu einer enormen Verunsicherung von VersammlungsteilnehmerInnen und dazu, dass Bürger*innen von der ihrer Versammlungsfreiheit innewohnenden Gestaltungsfreiheit im Zweifel keinen Gebrauch machen, insbesondere wenn eine strafrechtliche Verurteilung droht. Dies ist letztendlich ein enormer Schaden sowohl für den einzelnen als auch den demokratischen Rechtsstaat. Es sei an die Ausführungen des Bundesverfassungsgerichts in seinem Brokdorf-Beschluss erinnert, wonach das Gebrauchmachen der Bürger*innen von ihrer Versammlungsfreiheit ein unentbehrliches Funktionselement des demokratischen Gemeinwesens ist.[73] Soweit durch die Freiheit zur anonymen Teilnahme an Versammlungen immer auch solche Teilnehmer profitieren, die beabsichtigen im Schutz der Anonymität Straftaten zu begehen, wird darauf verwiesen, dass im öffentlichen Raum außerhalb von Versammlungen ebenfalls kein Vermummungsverbot besteht und dies weitgehend Akzeptanz findet.

10.2. Gefahren der Pönalisierung von Verstößen gegen das Vermummungsverbot

Bei vielen Einsätzen der Polizei im Rahmen von Versammlungen hat sich eine Deeskalationsstrategie bewährt (z.B. seit Jahren geübt am 1. Mai in Berlin). Die mit dem vorliegenden Gesetzentwurf beabsichtigte Pönalisierung von Verstößen gegen das Vermummungsverbot macht es der Polizei jedoch unmöglich, flexibel und deeskalierend auf einzelne Verstöße gegen das Vermummungsverbot zu reagieren, denn stellen Verstöße gegen das Vermummungsverbot Straftaten dar, ist sie aufgrund des Legalitätsprinzips (§ 163 StPO) verpflichtet gegen diese Verstöße einzuschreiten. Ein solches Einschreiten bedeutet in der Praxis, dass sich uniformierte Polizeibeamte in das Versammlungsgeschehen drängen, um der vermummten Personen habhaft zu werden. Dies führt in der Praxis nicht selten zur Eskalation eines Versammlungsgeschehens. Soweit der vorliegende Gesetzentwurf die Fälle der strafbewehrten Verstöße gegen das Vermummungsverbot auf diejenigen Fälle reduziert, bei denen gegen die unkenntlich gemachte Person zuvor eine vollziehbare Maßnahme nach § 10 Abs. 2 ergangen ist, ist dies zwar grundsätzlich zu begrüßen, birgt jedoch die geschilderte Problematik für die von der Strafvorschrift erfassten Fälle in gleichem Maße in sich. Daher sollte ein Verstoß, sofern eine Sanktionierung unbedingt gewollt ist, allenfalls eine Ordnungswidrigkeit bleiben.

Anja Heinrich, Stefan Hügel, Dr. Kirsten Wiese

73 BVerfGE 69, 315 (1. Leitsatz).