Jun.-Prof. Dr. Sebastian Golla
Massenbergstraße 11
44787 Bochum

An das
Bundesverfassungsgericht
Schlossbezirk
76131 Karlsruhe

Bochum, den 19. November 2020

Verfassungsbeschwerde

1. der Frau Britta Eder,
2. der Frau Anja Flach,
3. der Frau Emily Laquer,
4. der Frau Katharina Schipkowski,
5. der Frau Marily Stroux,
6. des Herrn Sebastian Friedrich,

gegen

§ 8 Abs. 12 Hamburgisches Verfassungsschutzgesetz (HmbVerfSchG) in der Fassung des Vierten Gesetzes zur Änderung von Vorschriften auf dem Gebiet des Verfassungsschutzrechts vom 24. Januar 2020, veröffentlicht am 11. Februar 2020 im Hamburgischen Gesetz- und Verordnungsblatt, Nr. 7, S. 99

und

§ 49 Hamburgisches Gesetz über die Datenverarbeitung der Polizei (PolDVG) in der Fassung des Gesetzes über die Datenverarbeitung der Polizei und zur Änderung weiterer polizeirechtlicher Vorschriften vom 12. Dezember 2019, veröffentlicht am 23. Dezember 2019 im Hamburgischen Gesetz- und Verordnungsblatt, Nr. 51, S. 485.

Namens und in Vollmacht der Beschwerdeführer*innen erhebe ich Verfassungsbeschwerde. Ich rüge Verletzungen von Art. 2 Abs. 1 i.V.m. Art. 1, Art. 5 Abs. 1 Satz 2, Art. 10 Abs. 1, Art. 13 Abs. 1, Art. 19 Abs. 4 GG.

INHALT

A. Vorbemerkung

Stetig schaffen die Gesetzgeber neue Befugnisse für Sicherheitsbehörden, damit diese moderne Überwachungstechniken einsetzen können. Die Verfassungsbeschwerde richtet sich gegen zwei verfassungswidrige Regelungen im Landesrecht Hamburgs.

I. Quellen-Telekommunikationsüberwachung für Hamburgs Verfassungsschutz

Erstens rügt die Beschwerde im Hamburgischen Verfassungsschutzgesetz (HmbVerfSchG) die Ermächtigung zur Telekommunikationsüberwachung an informationstechnischen Systemen (Quellen-TKÜ) in § 8 Abs. 12 HmbVerfSchG.

Die Regelung offenbart grundlegende Probleme bei den Gesetzgebungskompetenzen im Recht der Nachrichtendienste. Sie kann nicht kompetenzmäßig sein, da sie als unselbstständige Regelung an § 3 G 10 anknüpft, der seinerseits kompetenzwidrig ist.

Außerdem kann die Regelung die schwerwiegenden Eingriffe in das Telekommunikationsgeheimnis, die die Quellen-TKÜ durch den Verfassungsschutz bedeutet, nicht rechtfertigen. Die Anforderungen hierfür kann das angerufene Gericht nun näher klären. Dabei ist neben dem Telekommunikationsgeheimnis die Garantie der Pressefreiheit als ergänzender Prüfungsmaßstab zu berücksichtigen; soweit die angegriffene Norm zur sog. „kleinen Online-Durchsuchung“ ermächtigt, auch das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme.

Die Hamburgische Befugnis zur Quellen-TKÜ verfehlt zudem die Anforderungen, die an die Transparenz und Kontrolle derartiger Maßnahmen zu stellen sind. Zuletzt hat das angerufene Gericht in seinem Urteil zum BND-Gesetz vom 19. Mai 2020 (1 BvR 2835/17) Maßstäbe für die Kontrolle der Auslandsfernmeldeaufklärung aufgestellt, die mindestens auch für die Quellen-TKÜ im Inland gelten müssen.

Die Regelung führt schließlich zu nicht hinnehmbaren Risiken für die allgemeine IT-Sicherheit. Sie ermöglicht die Verwendung eines „Geheimdienstrojaners“ und schließt nicht aus, dass der Verfassungsschutz zur Überwachung unbekannte IT-Sicherheitslücken ausnutzt und diese geheim hält. Dies verletzt das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in seiner objektiv-rechtlichen Ausprägung.

II. Komplexe Datenauswertungen für Hamburgs Polizei

Zweitens rügt die Beschwerde die neue Rechtsgrundlage für eine automatisierte Anwendung zur Auswertung vorhandener Daten in § 49 Hamburgisches Gesetz über die Datenverarbeitung der Polizei (HmbPolDVG). Die Regelung ermöglicht die Zusammenführung und Auswertung großer Mengen personenbezogener Daten mit technischen Hilfsmitteln. Sie stößt das Tor für den Einsatz von komplexen Algorithmen und Anwendungen des „Predictive Policing“ auf.

Es ist dringend notwendig, die verfassungsrechtlichen Maßstäbe für den Einsatz derartiger Technologien durch Sicherheitsbehörden näher festzulegen. Dass diesbezüglich weitere gesetzliche Regelungen notwendig werden dürften, hat das angerufene Gericht in seinem Urteil zum BND-Gesetz vom 19. Mai 2020 angedeutet.

Das vorliegende Verfahren bietet dem angerufenen Gericht Gelegenheit, seine Rechtsprechung zu Eingriffen durch Datenauswertungen weiterzuentwickeln. Die Maßstäbe aus dem Beschluss zur Rasterfahndung vom 4. April 2006 (1 BvR 518/02) sind durch die heutigen technischen Möglichkeiten überholt. Selbst diese Maßstäbe hält die Hamburgische Befugnis zur komplexen Datenauswertung aber nicht ein, obwohl sie tiefere Grundrechtseingriffe ermöglicht als die überkommene Rasterfahndung.

Welche technischen Hilfsmittel § 49 HmbPolDVG im Einzelnen erlauben soll, lässt sich aus Wortlaut, Entstehungsgeschichte und Kontext der Regelung nicht genau bestimmen. Sie ist nicht präzise genug formuliert, um den Einsatz von komplexen Algorithmen und lernfähigen Systemen zu rechtfertigen. Gleichzeitig erweckt sie im Vergleich zu §§ 48 und 50 HmbPolDVG den Anschein, dass ebendies gewollt ist.

Die Schaffung einer Überwachungsbefugnis, die derart technikoffen gefasst ist, ohne sich zu ihrem Anwendungsbereich zu verhalten, überschreitet die Grenzen des gesetzgeberischen Spielraums. Eine eigene Abwägungsentscheidung des Gesetzgebers hinsichtlich Reichweite und Folgen der Befugnis ist nicht erkennbar.

Zudem fehlt es an flankierenden Verfahrensvorschriften. Die Datenauswertungen, die § 49 HmbPolDVG ermöglicht, müssten in rechtlicher und technischer Hinsicht einer kontinuierlichen unabhängigen Kontrolle unterzogen werden.

Da die Ergebnisse komplexer Auswertungen personenbezogener Daten entscheidend von der Qualität des einbezogenen Datenmaterials abhängen, müsste schließlich ein Standard für die Datenqualität gesetzlich festgelegt werden.

B. Sachverhalt

Gegenstand der Verfassungsbeschwerde sind erstens Neuregelungen im Hamburgischen Verfassungsschutzgesetz (HmbVerfSchG), die am 1. April 2020 durch das Vierte Gesetz zur Änderung von Vorschriften auf dem Gebiet des Verfassungsschutzrechts in Kraft getreten sind, und zweitens Neuregelungen des Hamburgischen Gesetzes über die Datenverarbeitung der Polizei (HmbPolDVG), die am 24. Dezember 2019 durch das Gesetz über die Datenverarbeitung der Polizei und zur Änderung weiterer polizeirechtlicher Vorschriften in Kraft getreten sind.

I. Die angegriffene Regelung im HmbVerfSchG

§ 8 Abs. 12 Satz 1 HmbVerfSchG ermächtigt das Landesamt für Verfassungsschutz (LfV), zur Durchführung einer bereits oder zugleich angeordneten Maßnahme nach § 1 Abs. 1 Nr. 1 G 10 mit technischen Mitteln auf informationstechnische Systeme zuzugreifen, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen und durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird.

Eine vergleichbare Befugnis zur Quellen-TKÜ durch den Verfassungsschutz existiert in Art. 13 Abs. 1 Bayerisches Verfassungsschutzgesetz (BayVerfSchG), gegen den seit Ende Juli 2017 eine Verfassungsbeschwerde beim Ersten Senat des angerufenen Gerichts anhängig ist (Aktenzeichen: 1 BvR 1619/17). Anders als Art. 13 Abs. 1 Satz 2 BayVerfSchG enthält § 8 HmbVerfSchG allerdings keine Regelungen über Begleitmaßnahmen, die erforderlich sind, um die Durchführung der Quellen-TKÜ zu ermöglichen.

Weiter als Art. 13 BayVerfSchG ist § 8 HmbVerfSchG insofern, als er in Abs. 12 Satz 2 eine Befugnis enthält, über laufende Kommunikationsvorgänge hinaus auch auf dem System bereits gespeicherte Inhalte und Umstände der Kommunikation überwachen und aufzeichnen zu dürfen, wenn sie auch während eines laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können. Diese Regelung ist § 100a Abs. 1 Satz 3 StPO nachempfunden. Sie erlaubt im Ergebnis eine Überwachung und Auf-

zeichnung aller seit dem Zeitpunkt der Überwachungsanordnung auf dem betroffenen System gespeicherten Kommunikationsinhalte als „kleine Online-Durchsuchung“.

II. Die angegriffene Regelung im PolDVG

§ 49 HmbPolDVG ermächtigt die Polizei zum Einsatz automatisierter Anwendungen zur Datenanalyse. Die Regelung soll komplexe Analysen bei der Polizei vorhandener Daten mit modernen technischen Hilfsmitteln ermöglichen.

Vgl. Hamburgische Bürgerschaft Drs. 21/17906, S. 70 f.

Welche Methoden und Hilfsmittel bei den Analysen zum Einsatz kommen sollen und inwiefern die Regelung die Tür für ein personenbezogenes „Predictive Policing“ öffnet, lassen Gesetzeswortlaut und -begründung allerdings offen. Nach Angaben des Hamburgischen Senats gibt es seitens der Polizei Hamburg bisher keine Planungen zur Anschaffung oder Entwicklung einer spezialisierten Software zur automatisierten Datenauswertung nach § 49 HmbPolDVG. Die Polizei Hamburg informierte sich jedoch zumindest im Jahr 2018 im Rahmen einer Veranstaltung der Polizei Hessen über die Anwendung „Hessendata“, wobei an dieser Veranstaltung auch Vertreter der US-Firma Palantir Technologies, Inc. teilnahmen.

Hamburgische Bürgerschaft Drs. 21/20061.

Zuletzt erklärte der Hamburgische Senat auf eine Kleine Anfrage, gegebenenfalls ein datenbankübergreifendes Analyse- und Recherchetool für operative Auswertungen nutzen zu wollen, das im Rahmen des bundesweiten Programmes „Polizei 2020“ entwickelt werde. Wie ein solches Tool ausgestaltet sein könnte, ist allerdings noch offen.

Hamburgische Bürgerschaft Drs. 22/1758.

Die Regelung erinnert bis in die Details ihres Wortlauts stark an § 25a HSOG, mit dem erstmals eine Befugnis für komplexe Datenabgleiche im Polizeirecht der Länder geschaffen wurde. Gegen § 25a HSOG ist seit Anfang Juli 2019 eine Verfassungsbeschwerde beim Ersten Senat des angerufenen Gerichts anhängig (Aktenzeichen: 1 BvR 1547/19).

§ 49 HmbPolDVG ermächtigt nicht zur Datenerhebung, sondern ermöglicht die gemeinsame Speicherung und den automatisierten Abgleich von Daten, die die Polizei auf Grundlage anderer Ermächtigungsgrundlagen gewonnen hat.

Aus welchen Datenquellen die Daten stammen, die in die automatisierte Datenanalyse einfließen, und insbesondere, welche externen Daten von anderen öffentlichen Stellen, privaten Unternehmen oder aus Online-Quellen einfließen, lässt sich weder dem Gesetzestext noch der Gesetzesbegründung entnehmen.

Welche Daten in die Analyse einfließen, ist nach der Gesetzesbegründung „im Hinblick auf den jeweiligen Analysezweck zu prüfen und gegebenenfalls über Zugriffsberechtigungen zu definieren."

> Hamburgische Bürgerschaft Drs. 21/17906, S. 70.

Zwar gestattet § 49 Abs. 1 HmbPolDVG nur die Auswertung von „in polizeilichen Dateisystemen gespeicherte[n] personenbezogene[n] Daten", allerdings können in diese Datensysteme auf Grundlage der allgemeinen Befugnisse zur Datenerhebung zahlreiche Daten von anderen Stellen oder aus öffentlichen Quellen gelangen.

Potentiell können in die automatisierte Datenanalyse alle Daten einfließen, die die Polizei Hamburg selbst erheben kann oder die sie sich auf Grundlage von §§ 10, 11 HmbPolDVG von anderen öffentlichen Stellen oder privaten Unternehmen übermitteln lassen kann. Soweit die Polizei begründen kann, dass die Erhebung und Speicherung der Daten zur Erfüllung ihrer Aufgaben erforderlich ist, steht ihr dabei ein weiter Spielraum zu.

Die Beschränkung auf Daten aus polizeilichen Dateisystemen, die auf intransparente Weise, in großer Zahl und mit stetig wachsendem Datenvolumen geführt werden, macht die Datenquellen damit nur scheinbar überschaubar. In Betracht kommen als auszuwertende Daten namentlich:

- Originär zu polizeilichen Zwecken etwa in Vorgangsbearbeitungssystemen oder Fallbearbeitungssystemen gespeicherte Daten.
- Der Polizei übermittelte und von dieser im Einzelfall in Dateisystemen gespeicherte Daten aus anderen behördlichen Quellen wie dem KfZ-Register.
- Von der Polizei aus sozialen Netzwerken wie Facebook und Twitter erhobene und in Dateien gespeicherte Daten („OSINT-Daten").

- Andere ursprünglich bei privaten Stellen gespeicherte Daten, die von der Polizei erhoben wurden, so etwa aus Gründen des Infektionsschutzes erhobene Daten zur Nachverfolgung von Kontaktpersonen aus der Gastronomie („Corona-Listen“).

§ 49 Abs. 1 HmbPolDVG sieht eine erhöhte Eingriffsschwelle vor, um automatisierte Analysen durchzuführen. Demnach ist die Anwendung beschränkt auf begründete Einzelfälle zur „vorbeugenden Bekämpfung von in § 100a Absatz 2 der Strafprozessordnung genannten Straftaten oder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist“.

Gerade die Kategorie der vorbeugenden Straftatenbekämpfung verlagert die Anwendung ins Vorfeld einer konkreten Gefahr. Dies entspricht auch dem Zweck der Analyse, die dazu dient, Zusammenhänge und Handlungsmuster zu erschließen und so auch zukünftige Gefahren zu erkennen.

Nicht näher benannt ist in § 49 HmbPolDVG der Kreis der Betroffenen. Aus der Natur der Datenanalyse ergibt sich jedoch zwangsläufig, dass diese nicht auf den unmittelbaren Störer beschränkt bleibt. Schließlich soll die Analyse unter anderem „Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen“ herstellen (Abs. 2). Da die Analyse Verknüpfungen, Netzwerke und Strukturen zutage fördern soll, ist von den Analysen unweigerlich ein weiter Personenkreis betroffen. Schließlich kann jede Beziehung eines Objekts mit einem anderen Objekt zur Auswertung herangezogen werden und dies führt zu weiteren Objekten, die wieder mit anderen Objekten in Beziehung stehen. Auch die genannten Datenquellen, aus denen eine Auswertung erfolgen kann, sind keinesfalls nur auf Störer beschränkt.

Als flankierende Verfahrenssicherungen sieht § 49 Abs. 3 HmbPolDVG lediglich vor, dass die Einrichtung und wesentliche Änderung einer automatisierten Anwendung zur Datenanalyse durch Anordnung der Polizeipräsidentin oder des Polizeipräsidenten oder der Vertretung im Amt erfolgen muss und vor Einrichtung oder Änderung der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit anzuhören ist. Dem Datenschutzbeauftragten fehlt es dabei sowohl faktisch als auch rechtlich an Möglich-

keiten, um die Datenauswertungen laufend zu beobachten und ggf. korrigierend einzugreifen.

Vorgaben zur Dauer der Anwendung, Erneuerung der Anwendung, Löschung der Daten einschließlich der Ergebnisse der automatisierten Auswertung, sowie zum Grundsatz der Zweckbindung trifft § 49 HmbPolDVG selbst nicht. Die Gesetzesbegründung führt dazu aus, dass in Bezug auf die Datenanalyse die allgemeinen Regelungen zur Zweckbindung (§ 34 HmbPolDVG) und besondere Verwendungsregelungen sowie der Vierte Abschnitt des HmbPolDVG zu beachten sind.

Hamburgische Bürgerschaft Drs. 21/17906, S. 70.

III. Die Beschwerdeführer*innen

1. Beschwerdeführerin zu 1 (Britta Eder)

Die Beschwerdeführerin zu 1 ist Strafverteidigerin in Hamburg. Zu ihren Mandant*innen gehören unter anderem Personen, denen vorgeworfen wird, inländischen und ausländischen terroristischen Vereinigungen anzugehören oder sie zu unterstützen. Sie vertrat etwa vor dem Landgericht Flensburg eine Gruppe von Antifaschist*innen, denen Anschläge auf Fahrzeuge der Bundeswehr und deren Zulieferunternehmen sowie die Bildung einer terroristischen Vereinigung vorgeworfen worden war. Unter anderem vor dem Oberlandesgericht Hamburg verteidigte sie mehrere Personen, die angeklagt waren, Mitglieder oder führende Kader der in Deutschland als terroristische Vereinigung im Ausland eingestuften PKK gewesen zu sein.

taz vom 11. Mai 2016, https://taz.de/!5299521/.

Ihre Mandant*innen werden dabei auch Subjekt von staatlichen Überwachungsmaßnahmen, von denen die Beschwerdeführerin zu 1 mitunter mit betroffen ist. So wurden beispielsweise im Jahr 2014 in einem Ermittlungsverfahren der Staatsanwaltschaft Braunschweig bei einer Telekommunikationsüberwachung auch Gespräche mitgehört, an denen die Beschwerdeführerin zu 1 beteiligt war.

Anlage 1.

Die Beschwerdeführerin zu 1 nutzt sowohl in ihrer privaten als auch in ihrer beruflichen Kommunikation verschlüsselte Kommunikationsdienste. Sie verwendet bei der Kommunikation mittels ihres Mobiltelefons den Ende-zu-Ende verschlüsselten Messenger-

dienst Signal. Ihre E-Mails verschlüsselt sie regelmäßig nach dem Standard PGP (Pretty Good Privacy). Dies betrifft besonders E-Mails an ihre Mandant*innen.

2. Beschwerdeführerin zu 2 (Anja Flach)

Die Beschwerdeführerin zu 2 ist Ethnologin, Journalistin und Buchautorin und lebt in Hamburg. Von 1995 bis 1997 hielt sie sich in Kurdistan auf und lebte bei Guerilla-Einheiten der PKK. Nach ihrer Rückkehr führte die Bundesanwaltschaft ein Ermittlungsverfahren wegen Verdachts der Bildung einer terroristischen Vereinigung gegen sie. Nach Hausdurchsuchungen, Beschlagnahmen und weiteren Ermittlungsmaßnahmen wurde das Verfahren am 26. März 2001 gemäß § 170 Abs. 2 StPO eingestellt. Bei den Ermittlungen kam es zu einer Beschlagnahme der Tagebücher, die die Beschwerdeführerin bei ihrem Aufenthalt in Kurdistan geführt hatte. Der Verfassungsschutz NRW gelangte an diese Aufzeichnungen und stellte ausführliche Auszüge hieraus im Internet ein und veröffentlichte sie in einer Informationsbroschüre. Die Beschwerdeführerin zu 2 erreichte durch eine verwaltungsgerichtliche Klage in einem Vergleich die Feststellung der Rechtswidrigkeit dieser Veröffentlichungen.

> VG Düsseldorf Urteil vom 9. Mai 2003, 1 K 1183/01; OVG Münster Beschluss vom 3. März 2004, 8 A 3277/03.

Im Juli 2019 verbreitete die Beschwerdeführerin zu 2 eine Fotografie eines Hamburgers, der in Kurdistan für die PKK gekämpft hatte und dort verstorben war, auf Twitter und Facebook. Im Hintergrund des Bildes war ein kleines Symbol der PKK zu erkennen. Infolgedessen durchsuchte die Hamburger Polizei die Wohnung der Beschwerdeführerin zu 2 wegen eines mutmaßlichen Verstoßes gegen das Vereinsgesetz. Durch einen mittlerweile rechtskräftigen Strafbefehl vom 15. Juli 2020 (Az. 243 Cs 176/20) setzte das Amtsgericht hierfür eine Geldstrafe von 40 Tagessätzen gegen sie fest.

> Hamburger Morgenpost vom 12. Dezember 2019, https://www.mopo.de/hamburg/polizei/polizeieinsatz-in-hamburg-frau-twittert-foto-von-hamburger-pkk-kaempfer---razzia-33601342; Anlage 2a und 2b.

Das LfV Hamburg und die Polizei Hamburg haben Daten zu der Beschwerdeführerin zu 2 in ihren Systemen gespeichert.

Auf einen Antrag auf Auskunft teilte die Behörde für Inneres und Sport der Freien und Hansestadt Hamburg der Beschwerdeführerin zu 2 im August 2020 mit, dass beim LfV Hamburg personenbezogene Daten über sie gespeichert seien. Dem LfV liegen nach der Auskunft Erkenntnisse vor, die angeblich tatsächliche Anhaltspunkte dafür begründen, dass sie sich „an Aktivitäten linksextremistischer Bestrebungen bzw. Bestrebungen mit Auslandsbezug beteiligt“ habe und „Personenzusammenschlüssen [angehöre], die der PKK zuzurechnen [seien] oder dieser nahe [stünden]“.

Anlage 3.

Der Auskunft lässt sich insbesondere entnehmen, dass das LfV seit dem Jahr 2000 zahlreiche Informationen zu Aktivitäten der Beschwerdeführerin zu 2 im „Verein freier Frauen aus Mesopotamien e.V.“ (zwischenzeitlich: Nûjiyan Frauenzentrum e.V.; heute: Rojbîn Frauenrat e.V.) gesammelt hat. Dass das LfV diesen Verein überwacht, ergibt sich zumindest bis zum Jahr 2016 auch aus dem Verfassungsschutzbericht.

LfV Hamburg, Verfassungsschutzbericht 2016, S. 74; Anlage 3.

Gespeichert hat das LfV u.a. auch, dass die Beschwerdeführerin zu 2 sich selbst zuletzt zum Jahreswechsel 2018/2019 in der Autonomen Administration von Nord- und Ostsyrien (Rojava) aufhielt, einem de facto autonomen Gebiet in Syrien. Sie war hierbei Teilnehmerin einer Delegation der feministischen Kampagne „Gemeinsam Kämpfen“.

Auf einen Antrag auf Auskunft teilte die Polizei Hamburg der Beschwerdeführerin zu 2 im August 2020 mit, dass zu ihr neben Personalien unter anderem Daten zur Einreise zu Zwecken der vorbeugenden Bekämpfung von Straftaten aus den Bereichen politisch motivierte Kriminalität Rechts und politisch motivierte Kriminalität Links gespeichert seien. Zu der Beschwerdeführerin zu 2 sind bei der Polizei Hamburg außerdem Informationen zu verschiedenen konkreten Verfahren gespeichert, in denen diese u.a. als Beschuldigte und Geschädigte geführt wird.

Anlage 4.

Die Beschwerdeführerin zu 2 nutzt sowohl in ihrer privaten als auch in ihrer beruflichen Kommunikation verschlüsselte Kommunikationsdienste. Sie verwendet bei der Kommunikation mittels ihres Mobiltelefons den Ende-zu-Ende verschlüsselten Messengerdienst Signal. Ihre E-Mails verschlüsselt sie regelmäßig nach dem Standard PGP (Pretty Good Privacy).

3. Beschwerdeführerin zu 3 (Emily Laquer)

Die Beschwerdeführerin zu 3 ist Aktivistin sowie Presseleiterin des VSA: Verlages und lebt in Hamburg. Sie tritt öffentlich für die Interventionistische Linke (IL) auf. Die IL ist eine bundesweite antikapitalistische Organisation. Hamburgs Innenbehörde beschreibt die IL als „gewaltorientierte Gruppierung“, deren Ziel es sei, „eine möglichst große Zahl nichtextremistischer Akteure zu indoktrinieren und letztendlich zu radikalisieren.“

> Behörde für Inneres und Sport Hamburg vom 11. April 2019; https://www.hamburg.de/innenbehoerde/schlagzeilen/12443512/die-interventionistische-linke-eine-gewaltorientierte-gruppierung/.

Die Innenbehörde beschreibt die Hamburger Ortsgruppe der IL dabei als besonders aktive linksextremistische Organisation und sieht die Beschwerdeführerin zu 3 als ihr „öffentliches Gesicht“ an.

> Behörde für Inneres und Sport Hamburg vom 11. April 2019; https://www.hamburg.de/innenbehoerde/schlagzeilen/12443486/wie-die-interventionistische-linke-demokratische-initiativen-instrumentalisieren-will/.

In dieser Rolle wird sie von Hamburgs Innenbehörde in mehreren öffentlichen Quellen namentlich erwähnt. Dies gilt besonders für ihre Aussagen im Zusammenhang mit dem Protest gegen den G20-Gipfel, der im Jahr 2017 in Hamburg stattfand.

> Vgl. LfV Hamburg, Verfassungsschutzbericht 2019, S. 127; LfV Hamburg, Verfassungsschutzbericht 2018, S. 73, 121 ff.; LfV Hamburg, Verfassungsschutzbericht 2017, S. 93 ff.

Die Beschwerdeführerin zu 3 nutzt sowohl in ihrer privaten als auch in ihrer beruflichen Kommunikation verschlüsselte Kommunikationsdienste. Sie verwendet bei der Kommunikation mittels ihres Mobiltelefons Ende-zu-Ende verschlüsselte Messengerdienste – unter anderem Signal, WhatsApp und Telegram. Ihre E-Mails verschlüsselt sie regelmäßig nach dem Standard PGP (Pretty Good Privacy). Sowohl per E-Mail als auch über Signal, WhatsApp und Telegram hält sie dabei Kontakt zu anderen Aktivist*innen, unter anderem zu Akteuren der radikalen Linken.

4. Beschwerdeführerin zu 4 (Katharina Schipkowski)

Die Beschwerdeführerin zu 4 lebt in Hamburg und ist als Journalistin bei der taz angestellt. Sie schreibt auch als freie Journalistin für Spiegel Online und weitere Medien. Dabei befasste sie sich unter anderem mit den G20-Protesten, der linken Szene in Hamburg und polizeilichem Handeln. Weitere Themen, zu denen die Beschwerdeführerin zu 4 schreibt, sind die bundesweiten Klimaproteste und soziale Bewegungen.

Im Rahmen ihrer journalistischen Tätigkeit ist sie in Kontakt mit Persönlichkeiten, die unter Beobachtung des LfV Hamburg stehen. So interviewte sie unter anderem die Beschwerdeführerin zu 3.

> taz vom 13. Juli 2017, https://taz.de/Emily-Laquer-ueber-Proteste-gegen-G20/!5426419/.

Im Zusammenhang mit einem Interview mit zwei Aktivisten aus Hamburg von Dezember 2016 wurde sie als Zeugin in einem Strafverfahren vorgeladen. Der Vorladung kam sie nicht nach. Den Interviewten wurde vorgeworfen, in dem Interview in strafbarer Weise Straftaten gebilligt zu haben (§ 140 Nr. 2 StGB).

> Neus Deutschland vom 29. Juni 2017, https://www.neues-deutschland.de/artikel/1055749.hausdurchsuchung-wegen-g-interview-in-hamburg.html.

In diesem Zusammenhang erfolgte eine Speicherung personenbezogener Daten der Beschwerdeführer*in zu 4 im Vorgangsverwaltungssystem der Polizei Hamburg.

> Anlage 5.

Die Beschwerdeführerin zu 4 nutzt sowohl in ihrer privaten als auch in ihrer beruflichen Kommunikation verschlüsselte Kommunikationsdienste. Sie verwendet bei der Kommunikation mittels ihres Mobiltelefons den Ende-zu-Ende verschlüsselten Messengerdienst Signal. Ihre E-Mails verschlüsselt sie regelmäßig nach dem Standard PGP (Pretty Good Privacy). Sowohl per E-Mail als auch über Signal hält sie dabei unter anderem Kontakt zu Aktivist*innen und anderen Personen, die sie im Rahmen ihrer journalistischen Tätigkeit mit Informationen versorgen. Hierzu gehört auch die Beschwerdeführerin zu 3.

5. Beschwerdeführerin zu 5 (Marily Stroux)

Die Beschwerdeführerin zu 5 ist seit Mitte der 1980er-Jahre als freie Fotografin für die taz und andere Medien tätig. Dabei fotografierte sie unter anderem auf vielen Demonstrationen und bei Polizeiaktionen.

Im Jahr 2007 beantragte die Beschwerdeführerin zu 5 beim Bundespresseamt eine Akkreditierung als Fotografin für den G8-Gipfel in Heiligendamm. Diesen Antrag lehnte das Bundespresseamt ohne inhaltliche Begründung auf Empfehlung des Bundeskriminalamts ab. In einer Entscheidung im Eilverfahren erklärte das Verwaltungsgericht Berlin die Ablehnung allerdings für rechtswidrig und verpflichtete das Bundespresseamt zur Erteilung der Akkreditierung.

VG Berlin, Beschluss vom 1. Juni 2007, VG 27 A 137.07 (nicht veröffentlicht).

Auf eine Anfrage beim LfV Hamburg (im Folgenden: LfV) erfuhr die Beschwerdeführerin zu 5 im Jahr 2016, dass sie seit 1988 unter Beobachtung des LfV stand. Dabei waren 31 Termine aufgelistet, bei denen sie beobachtet worden war – darunter zahlreiche journalistische Termine wie ein Interview mit inhaftierten RAF-Mitgliedern und Besuche von Demonstrationen als Pressefotografin.

taz vom 6. September 2016, https://taz.de/taz-Fotografin-ausgespaeht/!5337129/.

Die Beschwerdeführerin zu 5 erhob darauf vor dem Verwaltungsgericht Hamburg Klage auf Löschung der beim LfV über sie gespeicherten Daten. Der Hamburger Senat ordnete in der Folge die vorübergehende Sperrung der Daten an, gab sie jedoch im Jahr 2017 erneut zur Verwendung frei, da sie zur Erfüllung der Aufgaben des LfV notwendig seien. Dass sich die Beschwerdeführerin zu 5 unter anderem durch die Veröffentlichung einer eigenen Broschüre zu der Thematik gegen ihre Beobachtung und die Datenspeicherung zur Wehr setzte, wertete das LfV als Anhaltspunkt für ihre linksextremistische Gesinnung und die Relevanz der Daten.

taz vom 8. Mai 2019, https://taz.de/Die-seltsame-Akte-der-Marily-S/!5592674/.

Das Verfahren vor dem Verwaltungsgericht Hamburg (Az. 20 K 1543/17) wurde im Mai 2020 durch einen Vergleich abgeschlossen, mit dem sich die Innenbehörde verpflichtete, die über die Beschwerdeführerin zu 5 gespeicherten Daten zu löschen. Das LfV betonte hierbei jedoch, dass sie die Speicherung für rechtmäßig halte und nur deshalb in den Vergleich eingewilligt habe, weil aufgrund angeblich abnehmender Aktivität und

damit Relevanz der Beschwerdeführerin die Löschung kurzfristig ohnehin angestanden hätte. Die Beschwerdeführerin zu 5 ist aber weiterhin als Fotografin und in aktivistischen Kreisen tätig.

Sie nutzt sowohl in ihrer privaten als auch in ihrer beruflichen Kommunikation verschlüsselte Kommunikationsdienste. Sie verwendet bei der Kommunikation mittels ihres Mobiltelefons den Ende-zu-Ende verschlüsselten Messengerdienst Signal. Ihre E-Mails verschlüsselt sie regelmäßig nach dem Standard PGP (Pretty Good Privacy). Sowohl per E-Mail als auch über Signal hält sie dabei unter anderem Kontakt zu Personen, die aktivistischen Kreisen und Hamburgs linker Szene zuzuordnen sind.

6. Beschwerdeführer zu 6 (Sebastian Friedrich)

Der Beschwerdeführer zu 6 ist als Journalist unter anderem für den Norddeutschen Rundfunk sowie die Wochenzeitung der Freitag tätig und lebt in Hamburg.

Im Juni 2017 meldete er sich beim Presse- und Informationsamt der Bundesregierung für eine Akkreditierung als Journalist beim G20-Gipfel 2017 in Hamburg an. Nachdem ihm die Anmeldung bestätigt und ihm der Akkreditierungsausweis ausgehändigt wurde, wurde dieser ihm am 7. Juli 2017 entzogen. Dagegen erhob der Beschwerdeführer zu 6 Widerspruch und strengte ein Auskunftsersuchen beim BKA an. Dieses ergab, dass er nach Erkenntnissen des LfV Berlin Aktivist der linksextremistischen Szene Berlins sei und Kontakt zu gewaltbereiten Gruppierungen gehabt habe. Daher sei er auf die „Arbeitsliste Personenüberprüfung“ aufgenommen worden.

Im August 2017 erhob der Beschwerdeführer zu 6 Klage, um die Rechtswidrigkeit des Entzugs der Akkreditierung feststellen zu lassen. Das Verwaltungsgericht Berlin gab ihm recht. Die Voraussetzungen eines Widerrufs der Akkreditierung hätten nicht vorgelegen; zudem sei die Entscheidung ermessensfehlerhaft gewesen.

VG Berlin Urteil vom 20. November 2019, 27 K 516.17.

Am 13. Oktober 2020 beantragte der Beschwerdeführer zu 6 bei der Senatsverwaltung für Inneres und Sport Berlin Auskunft über die zu ihm beim Verfassungsschutz Berlin gespeicherten Daten. Die Senatsverwaltung teilte ihm darauf am 26.Oktober 2020 mit, dass im Rahmen der Beobachtung linksextremistischer Bestrebungen Informationen zu ihm suchfähig gemäß §§ 5 Abs. 2 Nr. 1 i.V.m. 11 Abs. 1 Nr. 1 VSG Bln gespeichert

seien. Nicht suchfähig gespeichert seien auch Informationen im Zusammenhang mit dem G20-Gipfel 2017 und dem geschilderten Entzug der Akkreditierung.

Anlage 6.

Der Beschwerdeführer zu 6 nutzt sowohl in seiner privaten als auch in seiner beruflichen Kommunikation verschlüsselte Kommunikationsdienste. Er verwendet bei der Kommunikation mittels seines Mobiltelefons den Ende-zu-Ende verschlüsselten Messengerdienst Signal. Seine E-Mails verschlüsselt er regelmäßig nach dem Standard PGP (Pretty Good Privacy). Sowohl per E-Mail als auch über Signal hält er dabei unter anderem Kontakt zu Personen, die dem aktivistischen Spektrum zuzuordnen sind.

C. Zulässigkeit

Die Verfassungsbeschwerde ist zulässig. Insbesondere sind die Beschwerdeführer*innen beschwerdebefugt (I.) sowie der Grundsatz der Subsidiarität der Verfassungsbeschwerde (II.) und die Beschwerdefrist gewahrt (III.).

I. Beschwerdebefugnis

Die Beschwerdeführer*innen sind im Sinne von § 90 Abs. 1 BVerfGG beschwerdebefugt.

1. Verfassungsrechtliche Rügen

Die Beschwerdeführer*innen rügen folgende Grundrechtsverletzungen:

Die angegriffene Überwachungsbefugnis in § 8 Abs. 12 HmbVerfSchG verletzt das Grundrecht der Beschwerdeführer*innen auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und ihr Telekommunikationsgrundrecht (Art. 10 Abs. 1 GG). Ein Grundrechtsverstoß ergibt sich auch aus der formellen Verfassungswidrigkeit der Regelung nach Art. 70 GG. Des Weiteren ist die Pressefreiheit aus Art. 5 Abs. 1 Satz 2 als ergänzender Prüfungsmaßstab zu berücksichtigen.

Die Ermächtigung zur automatisierten Datenanalyse in § 49 HmbPolDVG verletzt die Beschwerdeführer*innen in ihrem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und, soweit Daten aus der Wohnraumüberwachung oder der Telekommunikationsüberwachung analysiert werden, auch in ihrem Wohnungsgrundrecht (Art. 13 Abs. 1 GG) sowie ihrem Telekommunikationsgeheimnis (Art. 10 Abs. 1 GG). Sie verletzt die Beschwerdeführer*innen schließlich in ihrem Grundrecht auf individuellen Rechtsschutz nach Art. 19 Abs. 4 GG.

2. Eigene, gegenwärtige und unmittelbare Beschwer

Die Beschwerdeführer*innen sind auch selbst, gegenwärtig und unmittelbar von den angegriffenen Regelungen betroffen, § 90 Abs. 1 BVerfGG.

Erforderlich, aber auch ausreichend für die Darlegung einer eigenen Betroffenheit ist bei Verfassungsbeschwerden gegen Ermächtigungen zu gegen einzelne Personen gerichtete verdeckte Überwachungen und zum Umgang mit den dadurch erlangten personenbezogenen Daten, dass die/der Beschwerdeführer*in aufgrund ihres/seines Vortrags mit hinreichender Wahrscheinlichkeit als Zielperson oder Dritter von einer Überwachungsmaßnahme betroffen sein kann.

Vgl. BVerfGE 141, 220 (262), stRspr.

a) In Bezug auf die Quellen-TKÜ nach § 8 Abs. 12 HmbVerfSchG

(1) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

In Bezug auf § 8 Abs. 12 HmbVerfSchG rügen sämtliche Beschwerdeführer*innen die Verletzung ihres Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Die Beschwerdeführer*innen sind in herausgehobener Weise auf die Vertraulichkeit ihrer IT-Systeme angewiesen, dies jeweils auch zum Schutz der Rechte anderer Menschen. Die mögliche Verletzung ihres Rechts auf Gewährleistung dieser Vertraulichkeit liegt darin, dass die Freie und Hansestadt Hamburg durch die Einführung der angegriffenen Rechtsgrundlagen in § 8 Abs. 12 HmbVerfSchG ohne eine flankierende Regelung des Umgangs mit IT-Schwachstellen einen Anreiz dafür setzt, dass staatliche Behörden die IT-Sicherheit der Beschwerdeführer*innen gefährden. Denn für den Verfassungsschutz in Hamburg ist es aufgrund dieser Regelung zukünftig von Vorteil, IT-Schwachstellen geheim zu halten, um sie somit möglichst lange für Überwachungen ausnutzen zu können, statt sie den Herstellern zu melden und ihr Beheben zu ermöglichen.

Der Grundrechtschutz der Gewährleistung der Vertraulichkeit von IT-Systemen beinhaltet die staatliche Pflicht, sich für IT-Sicherheit einzusetzen und sich damit schützend vor dieses Recht zu stellen. Dem Gesetzgeber wird im Bereich der grundrechtlichen Schutzpflichten traditionell ein weiter Gestaltungsspielraum zugebilligt. Dieser wird jedoch dann verlassen, wenn das Land Hamburg seiner Schutzpflicht überhaupt nicht nachkommt oder sogar, wie vorliegend, Regelungen trifft, die Gefahren für das zu schützende Gut begründen. Die Vernachlässigung einer solchen grundrechtlichen

Schutzpflicht kann von den Betroffenen mit der Verfassungsbeschwerde geltend gemacht werden.

BVerfGE 77, 170 (214); BVerfGE 79, 174 (201 f.); BVerfGE 125, 39 (78).

Für den Schutz ihrer IT-Systeme hängen die Beschwerdeführer*innen in erster Linie von Maßnahmen der Hersteller der von ihnen verwendeten Programme und IT-Systeme ab. Der Staat spielt jedoch eine wesentliche Rolle in der Herstellung der IT-Sicherheit. Staatliche Stellen können Kenntnis von Sicherheitslücken noch vor den Herstellern der betroffenen Programme und IT-Systeme erhalten, beispielsweise über Meldungen von Firmen oder Behörden, die von Angriffen auf ihre IT-Systeme betroffen waren. Die Möglichkeit zu Maßnahmen nach § 8 Abs. 12 HmbVerfSchG begünstigt indes einen Umgang mit solchen Sicherheitslücken, der sich auf die Beschwerdeführer*innen, aber auch auf die Bürger*innen der Bundesrepublik insgesamt fatal auswirkt.

Das Ausnutzen von Schwachstellen spielt mutmaßlich bei der Umsetzung von Quellen-Telekommunikationsüberwachungen durch das LfV eine große Rolle. Diese Form des Eindringens in ein IT-System hat gegenüber den möglichen Alternativen deutliche, praktische Vorteile, da weder ein räumlicher Zugriff noch ein weiteres Fehlverhalten eines*r Nutzer*in notwendig ist. Gerade wegen dieses strategischen Vorteils werden solche Schwachstellen auf dem Schwarzmarkt für hohe Summen gehandelt.

Vgl. BR24 vom 20. Februar 2020, https://www.br.de/nachrichten/wirtschaft/zero-days-das-gefaehrliche-geschaeft-mit-it-sicherheitsluecken,Rr2DabA.

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

heise online vom 6. Juni 2018, https://heise.de/-4072578.

Es liegt daher nahe, dass auch das LfV bzw. Hamburgs Innenbehörde bestrebt sind, Informationen über IT-Sicherheitslücken und Infiltrationsmöglichkeiten zu sammeln und geheim zu halten, um diese für Maßnahmen nach § 8 Abs. 12 HmbVerfSchG zu nutzen.

Aufgrund ihrer jeweiligen beruflichen und privaten Tätigkeit sind die Beschwerdeführer*innen in besonderem Maße darauf angewiesen, dass die Vertraulichkeit ihrer IT-Systeme gewährleistet ist und Sicherheitslücken behoben werden, und sind deshalb zumindest möglicherweise betroffen. Sie sind auch selbst, gegenwärtig und unmittelbar betroffen.

Die Beschwerdeführerin zu 1 bedarf eines besonderen Schutzniveaus von IT-Systemen und IT-gestützter Kommunikation, um als Rechtsanwältin mit einem bestimmten Kreis von Mandant*innen die Vertraulichkeit der geschützten Kommunikation sicherstellen zu können. Dabei muss sie sowohl auf ein hohes Schutzniveau der eigenen IT-Systeme als auch auf ein solches Schutzniveau der IT-Systeme ihrer Mandant*innen vertrauen können. Denn nur, wenn die jeweiligen IT-Systeme und die IT-gestützte Kommunikation sicher sind, kann sie sicherstellen, dass die in ihrem IT-System gespeicherten, die Mandatsarbeit betreffenden Daten vor fremdem Zugriff geschützt sind und die Kommunikation mit ihren Mandant*innen vertraulich bleibt. Und nur bei hinreichend gewährleisteter IT-Sicherheit kann sie ihren Mandant*innen auch ein Vertrauen auf die Vertraulichkeit der Mandatsarbeit vermitteln. Gerade Schwachstellen, über welche ein Zugriff durch Dritte nicht verhindert und kaum bemerkt werden kann, bieten dafür ein Risiko.

Die Vertraulichkeit der Kommunikation ist für jede*n Anwält*in von großer Bedeutung. Bei der Beschwerdeführerin zu 1 kommt jedoch hinzu, dass ein Teil ihrer Mandant*innen und damit auch sie selbst von einer deutlich erhöhten Wahrscheinlichkeit ausgehen müssen, dass ihre IT-Systeme angegriffen werden. Diesen Mandant*innen wird die Begehung terroristischer Straftaten oder die Mitgliedschaft in ausländischen terroristischen Vereinigungen wie der PKK vorgeworfen. Es ist davon auszugehen, dass diese Personen auch von ausländischen Geheimdiensten überwacht werden.

Die Beschwerdeführer*innen zu 2, 4, 5 und 6 haben im Zusammenhang mit ihren journalistischen Tätigkeiten ein besondere Interesse an der Integrität der von ihnen und ihren Kommunikationspartner*innen genutzten IT-Systeme. Dabei besteht namentlich ein hohes Interesse am Quellenschutz. So ist die Beschwerdeführerin zu 4 im Zusammenhang mit ihrer Berichterstattung über die linke Szene in Hamburg in besonderem Maße auf eine vertrauliche Kommunikation angewiesen. Die Menschen aus der Szene, mit denen sie in Kontakt ist, stehen regelmäßig im Fokus von Polizei und Sicherheitsbehörden. Die Beschwerdeführerin zu 2 ist im Zusammenhang mit ihren Re-

cherchen und Berichten über Kurdistan in Kontakt mit Personen, die auch im Fokus ausländischer Sicherheitsbehörden stehen.

Um ihre Quellen zu schützen, sind die Beschwerdeführerinnen zu 2, 4 und 6 darauf angewiesen, dass organisierte Kriminalität, aber auch ausländische Sicherheitsbehörden nicht auf ihre IT-Systeme oder die IT-Systeme ihrer Kontaktpersonen zugreifen können. Dafür ist es wichtig, dass die genutzten IT-Systeme vor fremdem Zugriff bestmöglich geschützt sind. Gerade das Schließen von Sicherheitslücken ist dafür wesentlich.

Zusätzlich haben sämtliche Beschwerdeführer*innen auch ein privates Interesse an Datensicherheit, da sie legitimierweise eine eigene Überwachung durch kriminelle oder ausländische staatliche Akteure nicht wünschen. Zudem bieten die Sicherheitslücken ein Einfallstor für das Auslesen und die Manipulation von Daten sowie Erpressungen mittels Ransomware – also Software, die Daten auf IT-Systemen verschlüsselt und erst nach Zahlung eines Lösegeldes wieder freigibt.

> Zu der weiter steigenden Relevanz dieses Phänomens Bundeskriminalamt, Cybercrime, Bundeslagebild 2019, S. 20 ff.

§ 8 Abs. 12 HmbVerfSchG betrifft die Beschwerdeführer*innen unmittelbar in ihrem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, weil es zu ihrer Beschwer keines weiteren gegen sie gerichteten Akts bedarf. Vielmehr folgt ihre Betroffenheit gerade aus der durch staatliche Stellen erhöhten Gefahr für ihre IT-Systeme, die daraus resultiert, dass das LfV wegen § 8 Abs. 12 HmbVerfSchG ihm bekanntwerdende Sicherheitslücken unter Verletzung seiner staatlichen Schutzpflicht gegenüber den Beschwerdeführer*innen nicht an die Hersteller der betroffenen Programme und IT-Systeme meldet.

Wäre für die Unmittelbarkeit der Grundrechtsverletzung demgegenüber daran anzuknüpfen, dass das LfV eine bestimmte Schwachstelle geheim hält, um sie für Maßnahmen nach § 8 Abs. 12 HmbVerfSchG auszunutzen und genau diese durch Dritte für einen Hackerangriff auf ein IT-System der Beschwerdeführer*innen ausgenutzt würde, dann wäre der gerichtliche Rechtschutz unmöglich, da die Beschwerdeführer*innen von diesen Tatsachen, insbesondere den konkreten den Behörden bekannten Schwachstellen, keine Kenntnis erlangen würden.

Vgl. im Fall des sogenannten „Großen Lauschangriffs“ BVerfGE 109, 279 (306); BVerfGE 133, 277 (311 f.).

(2) Telekommunikationsgeheimnis

Auch hinsichtlich des durch die Quellen-TKÜ folgenden Eingriffs in das Telekommunikationsgrundrecht sind die Beschwerdeführer*innen selbst, gegenwärtig und unmittelbar betroffen.

Dies gilt besonders für die Beschwerdeführer*innen zu 2, 3, 5 und 6, die bereits nachweislich von Datenspeicherungen durch den Verfassungsschutz betroffen und Subjekt von Überwachungsmaßnahmen waren. Auch die übrigen Beschwerdeführerinnen stehen zumindest in Kontakt zu Personen, deren Überwachung durch den Verfassungsschutz als naheliegend erscheint. Namentlich bei der Beschwerdeführerin zu 3 wird unter anderem aus den Verfassungsschutzberichten deutlich, dass sie vom LfV Hamburg als eine besonders relevante und gefährliche Akteurin angesehen wird.

Insofern erscheint es wahrscheinlich, dass die Beschwerdeführer*innen Betroffene einer Quellen-TKÜ werden.

Zwar bedürfen Ermächtigungen zu Überwachungsmaßnahmen wie § 8 Abs. 12 HmbVerfSchG der behördlichen Umsetzung. Von einer unmittelbaren Betroffenheit durch ein Gesetz ist jedoch auch dann auszugehen, wenn Beschwerdeführer*innen den Rechtsweg nicht beschreiten können, weil sie keine Kenntnis von der betreffenden Vollziehungsmaßnahme erhalten. In solchen Fällen steht ihnen die Verfassungsbeschwerde unmittelbar gegen das Gesetz zu.

BVerfGE 133, 277 (311); BVerfGE 141, 220 (261).

Ein solcher Fall liegt hinsichtlich der Befugnis zur Quellen-TKÜ vor. Es handelt sich um eine Maßnahme, deren Kenntnis sich den Betroffenen entzieht. Eine Benachrichtigung der einzelnen Betroffenen erfolgt in vielen Fällen nicht. § 8 Abs. 12 Satz 8 HmbVerfSchG verweist zwar auf die Benachrichtigungsregelung des § 12 Abs. 1 G 10. Diese Regelung enthält jedoch weit gefasste Ausschlusstatbestände, die die Benachrichtigung oftmals entfallen lassen oder langfristig aufschieben.

b) In Bezug auf die automatisierte Datenanalyse nach § 49 HmbPolDVG

Die Beschwerdeführer*innen sind auch selbst, gegenwärtig und unmittelbar durch die Befugnis zur automatisierten Datenanalyse gemäß § 49 HmbPolDVG beschwert. Sie werden mit einiger Wahrscheinlichkeit durch die automatisierte Datenanalyse in ihren Grundrechten berührt.

Vgl. zu diesem Erfordernis BVerfGE 109, 279 (307 f.).

Die eigene und gegenwärtige Betroffenheit der Beschwerdeführer*innen folgt aus der Weite des Adressatenkreises der Ermächtigung. Für den geforderten Grad der Wahrscheinlichkeit ist bedeutsam, ob die angegriffene Maßnahme auf einen tatbestandlich eng umgrenzten Personenkreis zielt oder eine große Streubreite hat und Dritte auch zufällig erfassen kann.

Vgl. BVerfGE 109, 279 (307 f.).

Durch den Einsatz zur vorbeugenden Bekämpfung von Straftaten nach § 100a Abs. 2 StPO greift die automatisierte Datenanalyse schon in Bezug auf die unmittelbaren Zielpersonen im Vorfeld einer konkreten Gefahr. Für die vorbeugende Straftatbekämpfung reichen schon abstrakte Gefahrenlagen.

Vgl. nur Denninger, in: Lisken/ders., Handbuch des Polizeirechts, 6. Aufl. 2018, Rn. D 1 ff., m.w.N.

Zudem finden sich in dem Straftatkatalog des § 100a StPO neben Erfolgsdelikten auch Gefährdungstatbestände wie §§ 129 ff. StGB, die Handlungen im Vorfeld einer Rechtsgutsverletzung kriminalisieren, und auf deren Grundlage in der Vergangenheit immer wieder auch in angeblich linksextremistischen Strukturen ermittelt wurde.

Nimmt man die von der automatisierten Datenanalyse auch unvermeidlich betroffenen Dritten oder im Zusammenhang mit der Zielperson stehenden Personen hinzu, ergibt sich eine so hohe Streubreite der Eingriffe, dass die Beschwerdeführer*innen zu 2 bis 6 deutlich mit hinreichender Wahrscheinlichkeit von diesen Maßnahmen betroffen sein können. Sie alle stehen in Kontakt mit Personen, die von Polizei oder Verfassungsschutz linksextremen Kreisen zugeordnet wurden, oder werden sogar selbst als Teil dieser Szenen eingeordnet. Die Beschwerdeführer*innen zu 2, 3, 5 und 6 waren nachweislich bereits von nachrichtendienstlichen Datenverarbeitungen betroffen. Es ist davon auszugehen, dass Informationen über sie auch von polizeilicher Seite als für die vorbeugende Bekämpfung von Staatsschutzdelikten relevant angesehen werden.

Informationen über die Beschwerdeführerin zu 4 erscheinen polizeilich jedenfalls aufgrund ihrer Stellung als Kontakt von Personen im linksextremen Spektrum relevant. Dies zeigt unter anderem ihre jüngst erfolgte Vorladung als Zeugin in einem Strafverfahren aufgrund eines von ihr geführten Interviews, in dem ihre Interviewpartner Aussagen trafen, in denen die Strafverfolgungsbehörde eine Billigung von Straftaten sah. Auch die Beschwerdeführerin zu 1 steht im Rahmen ihrer beruflichen Tätigkeit als Strafverteidigerin in Kontakt mit Personen, deren Daten mit hoher Wahrscheinlichkeit polizeilich verarbeitet werden. Durch eine Auswertung der Daten ihrer Mandant*innen könnten sogar Verknüpfungen dieser untereinander sowie mit der Beschwerdeführerin selbst hergestellt werden.

Insofern erscheint es wahrscheinlich, dass die Beschwerdeführer*innen jedenfalls im Zusammenhang mit dem Ziel, „Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen“ herzustellen (§ 49 Abs. 2 HmbPolDVG), Gegenstand einer Datenanalyse nach § 49 HmbPolDVG werden.

Aufgrund dieser Zielrichtung ist anzunehmen, dass Gegenstand der Analyse nicht nur Daten der unmittelbaren Zielperson werden, sondern auch Daten von Menschen aus dem Umfeld der Zielperson und darüber hinaus auch von vollkommen unbeteiligten Menschen, die beispielsweise mit einem Ort oder einem Ereignis in Verbindung stehen. Schließlich kann jede Beziehung eines Objekts mit einem anderen Objekt zur Auswertung herangezogen werden und dies führt zu weiteren Objekten, die wieder mit anderen Objekten in Beziehung stehen. So beispielsweise bei einer Datenauswertung zur Bekämpfung eines kriminellen Netzwerks, dessen Mitglieder weitgehend polizeilich unbekannt sind. A wird dem Netzwerk zugeordnet. Da ihm regelmäßige Verbindungen zu B nachgewiesen sind, die im Zusammenhang mit Netzwerkaktivitäten stehen könnten, wird auch B als für die Datenauswertung relevant betrachtet. Die Kontakte und Beziehungen von B könnten nach einem ähnlichen Muster mit einbezogen werden. Diese Form der Analyse kann buchstäblich jeden treffen, bei Berücksichtigung von Melderegister- oder Fahrzeughalterdaten auch Menschen, die noch nie anlassbezogen polizeilich erfasst wurden.

Sämtliche Beschwerdeführer*innen sind jedenfalls aufgrund ihrer „politischen, beruflichen und privaten Verbindungen zu potentiellen Zielpersonen“ von den angegriffenen Maßnahmen mit hinreichender Wahrscheinlichkeit betroffen, sofern sie nicht schon

selbst als potentielle Zielpersonen eingestuft werden, was insbesondere für die Beschwerdeführer*innen zu 2, 3, 5 und 6 gilt.

> Vgl. BVerfGE 141, 220 (262). Siehe auch BVerfGE 109, 279 (307 f.); BVerfGE 113, 348 (363 f.); BVerfGE 133, 277 (312 f.).

Die Beschwerdeführer*innen sind durch die angegriffenen Regelungen auch unmittelbar betroffen.

Zwar bedürfen die Ermächtigungen zu Überwachungsmaßnahmen der behördlichen Umsetzung. Von einer unmittelbaren Betroffenheit durch ein Gesetz ist jedoch auch dann auszugehen, wenn Beschwerdeführer*innen den Rechtsweg nicht beschreiten können, weil sie keine Kenntnis von der betreffenden Vollziehungsmaßnahme erhalten. In solchen Fällen steht ihnen die Verfassungsbeschwerde unmittelbar gegen das Gesetz zu.

> BVerfGE 133, 277 (311); BVerfGE 141, 220 (261).

Ein solcher Fall liegt hinsichtlich der Befugnis zur automatisierten Datenanalyse nach § 49 HmbPolDVG vor. Die Datenauswertung ist für die Betroffenen zunächst nicht spürbar oder nachvollziehbar. Eine Benachrichtigung der einzelnen Betroffenen ist hierbei nicht vorgesehen.

II. Subsidiarität der Verfassungsbeschwerde

Ein Rechtsweg unmittelbar gegen die angegriffenen Regelungen ist nicht eröffnet und muss daher auch nicht gemäß § 90 Abs. 2 Satz 1 BVerfGG erschöpft werden.

Darüber hinaus steht der Grundsatz der Subsidiarität der Verfassungsbeschwerde der Zulässigkeit der vorliegenden Verfassungsbeschwerde nicht entgegen. Es ist den Beschwerdeführer*innen nicht möglich oder zumindest nicht zumutbar, gegen den Vollzug der angegriffenen Normen durch das LfV und die Polizei vorzugehen und sich so einen indirekten Rechtsschutz gegen diese Normen zu verschaffen.

Die Beschwerdeführer*innen erhalten von den angegriffenen Maßnahmen keine Kenntnis. Auch ein vorbeugender Rechtsschutz in Gestalt einer vorbeugenden Unterlassungs- oder Feststellungsklage ist den Beschwerdeführer*innen nicht eröffnet. Solche Klagen setzen nach gefestigter Rechtsprechung voraus, dass sich ein drohendes Verwaltungshandeln bzw. ein zukünftiges Rechtsverhältnis bereits hinreichend konk-

ret abzeichnet und die für eine Rechtmäßigkeitsprüfung erforderliche Bestimmtheit aufweist.

> Vgl. zur vorbeugenden Unterlassungsklage BVerwGE 45, 99 (105); BVerwG BeckRS 1981, 31248115; BVerwG NVwZ 2018, 731 (732 Rn. 12); Pietzcker/Marsch, in: Schoch/Schneider/Bier, VwGO, Bearbeitungsstand 2020, § 42 Abs. 1 Rn. 163; zur Feststellungsklage BVerwGE 59, 310 (318); BVerwG NVwZ 1988, 430 (431); BVerwG NVwZ 2018, 1476 (1482 Rn. 53 f.); Pietzcker, in: Schoch/Schneider/Bier, VwGO, Bearbeitungsstand 2008, § 43 Rn. 21.

Eine konkrete Bestimmung drohender Überwachungsmaßnahmen und Datenanalysen ist den Beschwerdeführer*innen jedoch nicht möglich. Hierzu müssten die Beschwerdeführer*innen ein konkretes behördliches Verfahren bezeichnen können, in dessen Rahmen ihnen eine Überwachung – sei es als Kontaktpersonen oder als Drittbetroffene – droht. Aus ihrer Betroffenenperspektive lassen sich solche Verfahren im Voraus aber nicht absehen.

Kenntnis von einem laufenden Verfahren können die Betroffenen bezüglich der Datenanalyse frühestens erlangen, wenn die Hamburgische Polizei offene Gefahrenabwehrmaßnahmen durchführt oder das Verfahren in ein offenes strafrechtliches Ermittlungsverfahren überleitet. Dies wird allerdings zum einen keineswegs in jedem Fall geschehen. Zum anderen werden zu diesem Zeitpunkt die verdeckten Maßnahmen bereits abgeschlossen sein, so dass ein vorbeugender Rechtsschutz zu spät käme. Bei einer Quellen-TKÜ durch das in seiner Aufgabe auf die Sammlung und Auswertung von Informationen begrenzte LfV erscheint eine Kenntnisnahme der Maßnahme durch die Betroffenen noch unwahrscheinlicher.

Um Rechtsschutz gegen die Maßnahmen zu erlangen, bliebe den Beschwerdeführer*innen regelmäßig lediglich eine vorbeugende Klage gegen unbestimmte Überwachungsmaßnahmen in unbestimmten Verfahren. Eine solche Klage „ins Blaue hinein“ sprengte jedoch den in langjähriger Rechtsprechung entwickelten Rahmen des vorbeugenden Rechtsschutzes und wäre aller Voraussicht nach unzulässig. Selbst wenn dies anders zu sehen wäre, wäre ein solcher Rechtsschutz so inadäquat, dass der Subsidiaritätsgrundsatz nicht dazu zwänge, ihn vorrangig zu ergreifen. Soweit nämlich die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft, die das Bundesverfassungsgericht zu beantworten hat, ohne dass von einer vorausge-

gangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären, bedarf es einer vorangehenden fachgerichtlichen Entscheidung nicht.

BVerfG NJW 2019, 842 (843 Rn. 44); BVerfG NJW 2020, 2699 (2702 Rn. 77).

So läge der Fall bei einer vorbeugenden Unterlassungs- oder Feststellungsklage gegen verdeckte Überwachungsmaßnahmen nach den angegriffenen Regelungen. Da die Beschwerdeführer*innen konkrete Überwachungsanlässe im Voraus nicht absehen und nicht benennen können, müsste eine solche Klage darauf gerichtet sein, eine Überwachung der Beschwerdeführer*innen nach den angegriffenen Regelungen generell zu unterlassen. Diese Klage wäre nur begründet, wenn es keinen denkbaren Sachverhalt gäbe, in dessen Rahmen die Beschwerdeführer*innen einer solchen Überwachung ausgesetzt werden dürfen. Dies ließe sich nur annehmen, wenn die angegriffenen Regelungen auch bei restriktiver Interpretation und unabhängig von ihrer tatsächlichen Handhabung verfassungswidrig wären. Ausführungen zur Auslegung und Anwendung der Normen könnten die Fachgerichte daher allenfalls als obiter dicta machen, zu denen sie nicht gehalten sind und deren bloße Möglichkeit unter Subsidiaritätsgesichtspunkten keinen fachgerichtlichen Rechtsschutz gebieten kann. Vielmehr wäre eine Aufklärung der einfachrechtlichen Rechtslage und der tatsächlichen Gegebenheiten im Verwaltungsprozess nicht angezeigt. Das verwaltungsgerichtliche Verfahren wäre vielmehr materiell als reiner Verfassungsprozess zu führen, was der Subsidiaritätsgrundsatz gerade nicht verlangt.

Vgl. BVerfG, NJW 2019, 842 (843 Rn. 44); BVerfGE 123, 148 (172 f.); BVerfGE 143, 246 (322); stRspr.

Daneben können die Beschwerdeführer*innen unter dem Gesichtspunkt der Subsidiarität der Verfassungsbeschwerde nicht darauf verwiesen werden, ihre Auskunftsansprüche aus § 23 HmbVerfSchG und § 69 HmbPolDVG gegen das LfV und die Polizei geltend zu machen und gegebenenfalls in einem verwaltungsgerichtlichen Verfahren um die Auskunftserteilung ihre verfassungsrechtlichen Argumente gegen die angegriffenen Ausschlusstatbestände des § 23 Abs. 2 HmbVerfSchG und §§ 69 Abs. 4 i.V.m. 68 Abs. 2 HmbPolDVG vorzubringen. Ein solches Vorgehen ist den Beschwerdeführer*innen nicht zumutbar, weil ein wirksamer fachgerichtlicher Rechtsschutz gegen eine Auskunftsverweigerung im Einzelfall nicht durchweg gewährleistet ist.

Grund hierfür ist, dass das LfV gemäß § 23 Abs. 4 HmbVerfSchG und die Polizei gemäß § 69 Abs. 6 Satz 2 HmbPolDVG nicht verpflichtet sind, eine Auskunftsverweige-

rung zu begründen, wenn hierdurch der Zweck der Auskunftsverweigerung gefährdet würde. Fehlt eine Begründung, so kann der Auskunftspetent vor Gericht nicht umfassend darlegen, weshalb die vom LfV oder von der Polizei für die Auskunftsverweigerung herangezogenen Gründe unzureichend sind. Auch Bedenken gegen einen der gesetzlichen Ausschlusstatbestände kann der Petent dann allenfalls pauschal und nicht in Bezug auf den konkreten Einzelfall und den in diesem Fall maßgeblichen Ausschlusstatbestand vorbringen. Die Gründe für die Auskunftsverweigerung können gerichtlich (zunächst) nur in einem In-Camera-Verfahren gemäß § 99 Abs. 2 VwGO überprüft werden. Vom Prozessstoff dieses Verfahrens erhält der Auskunftspetent jedoch wiederum keine umfassende Kenntnis, so dass er sich auch in diesem Rahmen nicht detailliert zu der Auskunftsverweigerung und den für sie herangezogenen Gründen äußern kann.

Schließlich ist es den von polizeilichen und sicherheitsbehördlichen Datenverarbeitungen betroffenen Personen nicht zumutbar, laufend neue Auskunftsansprüche geltend zu machen, um die Rechtmäßigkeit von Datenverarbeitungen zu überprüfen

III. Frist

Die Jahresfrist des § 93 Abs. 3 BVerfGG ist gewahrt.

§ 8 Abs. 12 HmbVerfSchG ist gemäß Art. 7 Abs .1 des Vierten Gesetzes zur Änderung von Vorschriften auf dem Gebiet des Verfassungsschutzrechts am 1. April 2020 in Kraft getreten.

§ 49 HmbPolDVG ist gemäß Art. 54 Satz 1 Verfassung der Freien und Hansestadt Hamburg am 24. Dezember 2019 in Kraft getreten.

D. Begründetheit

Die Verfassungsbeschwerde ist begründet.

I. Hinsichtlich § 8 Abs. 12 HmbVerfSchG

Die Ermächtigung zur Quellen-TKÜ in § 8 Abs. 12 HmbVerfSchG ist verfassungswidrig. Sie verletzt die Kompetenzordnung. Zudem verletzt sie die objektivrechtlichen Anforderungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Schließlich sind die gesetzlichen Eingriffsschwellen dieser Ermächtigung zu weit gefasst und es fehlt ihr an notwendigen Verfahrenssicherungen.

1. Kompetenzverstoß

Die Befugnis zur Quellen-TKÜ in § 8 Abs. 12 HmbVerfSchG steht nicht mit der Ordnung der Gesetzgebungskompetenzen in Einklang und verletzt damit Art. 10 Abs. 1 sowie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Der durch die Befugnis vorgenommene Eingriff in die Freiheitsrechte der Betroffenen kann nicht gerechtfertigt werden, da sie wegen eines Verstoßes gegen Art. 70 GG nicht verfassungsgemäß ist. Der Kompetenzverstoß begründet damit den Grundrechtsverstoß.

BVerfGE 98, 106 (117); BVerfGE 109, 96 (109).

§ 8 Abs. 12 HmbVerfSchG verletzt die Kompetenzordnung, indem diese Regelung lediglich ergänzend zu einer Telekommunikationsüberwachung nach dem G 10 hinzutreten soll. Die damit in Bezug genommene bundesrechtliche Eingriffsermächtigung des § 3 G 10 wurde jedoch ihrerseits unter Verstoß gegen Art. 70 GG kompetenzwidrig erlassen, soweit sie, wie sich aus § 1 Abs. 1 Nr. 1 G 10 ergibt, Telekommunikationsüberwachungen durch Landesverfassungsschutzbehörden zum Gegenstand hat. Die darauf bezugnehmende Ergänzungsregelung in § 8 Abs. 12 HmbVerfSchG nimmt an diesem Kompetenzverstoß teil.

Sollte das angerufene Gericht hingegen § 3 G 10 insoweit für kompetenzgemäß halten, so ist § 8 Abs. 12 HmbVerfSchG gleichwohl als kompetenzwidrig anzusehen. Denn in diesem Fall ist neben der bundesrechtlichen Überwachungsermächtigung für eine landesrechtliche Ergänzungsregelung kein Raum.

§ 8 Abs. 12 HmbVerfSchG ist nur dann als kompetenzgemäß anzusehen, wenn erstens § 3 G 10 kompetenzwidrig ist und zweitens § 8 Abs. 12 HmbVerfSchG entgegen der Gesetzesbegründung nicht als bloße Ergänzungsregelung zu § 3 G 10, sondern als eigenständige Überwachungsermächtigung anzusehen ist. Da es für die kompetenzrechtliche Beurteilung von § 8 Abs. 12 HmbVerfSchG in jedem Fall darauf ankommt, ob § 3 G 10 kompetenzgemäß erlassen wurde, soweit diese Norm Telekommunikationsüberwachungen durch Landesverfassungsschutzbehörden regelt, ist diese Frage im vorliegenden Verfahren zwingend als Vorfrage zu klären.

Es liegt nahe, § 8 Abs. 12 HmbVerfSchG – ähnlich wie den fast gleichlautenden Art. 13 Abs. 1 BayVSG – nicht als originäre Überwachungsermächtigung zu verstehen, sondern als eine unselbstständige Ergänzungsregelung, welche lediglich eine bestimmte technische Vorgehensweise bei einer Telekommunikationsüberwachung nach § 3 G 10 ermöglicht. Hierfür spricht zum einen die Gesetzesbegründung, die die Quellen-TKÜ als „Begleitmaßnahme zur eigentlichen TKÜ, die nach den Vorschriften des Artikel 10-Gesetzes durchzuführen ist“ und „zu dieser akzessorisch“ beschreibt.

Hamburgische Bürgerschaft Drs. 21/18578, S. 42.

Zum anderen sind §§ 3 ff. G 10 darauf angelegt, die Voraussetzungen und weitgehend auch das Verfahren für Telekommunikationsüberwachungen durch alle Nachrichtendienste – also einschließlich der Landesverfassungsschutzbehörden – bundesweit verbindlich und abschließend zu regeln. Dies ergibt sich aus § 1 Abs. 1 Nr. 1 G 10. Es ist nicht ersichtlich, dass sich der Hamburgische Gesetzgeber durch Erlass von § 8 Abs. 12 HmbVerfSchG hierüber hinwegsetzen wollte.

Jedoch verletzt § 3 G 10 die Kompetenzordnung jedenfalls insoweit, als er eine Vollregelung für Telekommunikationsüberwachungen für Landesverfassungsschutzbehörden enthält. An diesem Kompetenzverstoß nimmt § 8 Abs. 12 HmbVerfSchG teil.

a) Keine Gesetzgebungskompetenz des Bundes für Überwachungsermächtigungen der Landesverfassungsschutzbehörden

§ 3 G 10 verletzt die Kompetenzordnung zumindest insoweit, als er eine Ermächtigung für Telekommunikationsüberwachungen durch Landesverfassungsschutzbehörden enthält. Für eine solche Ermächtigung fehlt dem Bund die Gesetzgebungskompetenz.

Näher hierzu Bäcker, DÖV 2011, S. 840 ff.

Allerdings hat das angerufene Gericht in seinem ersten G 10-Urteil aus dem Jahr 1970 die Vorgängerregelung des heutigen § 3 G 10, den damaligen Art. 1 § 2 G 10, kompetenzrechtlich gebilligt. Als maßgeblichen Kompetenztitel für die Überwachungsermächtigung hat das Gericht Art. 74 (heute: Abs. 1) Nr. 1 GG angeführt, nach dem der Bund das gerichtliche Verfahren regeln darf. Dazu heißt es in dem Urteil:

> „Art. 1 § 2 G 10 dient der Abwehr verfassungsfeindlicher Bestrebungen im Vorfeld strafprozessualer Ermittlungen. Die zulässigen Beschränkungsmaßnahmen sind begrenzt auf die Fälle, in denen tatsächliche Anhaltspunkte für den Verdacht bestehen, daß bestimmte strafbare Handlungen geplant, begangen werden oder begangen worden sind. Die Beschränkungsmaßnahmen nach Art. 1 § 2 G 10 dienen also (wenigstens mittelbar) der Verhinderung, Aufklärung und Verfolgung von Straftaten.“ BVerfGE 30, 1 (29).

Diese Begründung ist jedoch jedenfalls nach dem heutigen Stand der Verfassungsauslegung unhaltbar. Träfe die darin vertretene Interpretation von Art. 74 Abs. 1 Nr. 1 GG zu, so könnte der Bund neben dem Verfassungsschutzrecht auch das allgemeine Polizeirecht, das anerkanntermaßen in die alleinige Gesetzgebungskompetenz der Länder fällt, weitgehend an sich ziehen. Denn das allgemeine Polizeirecht hat maßgeblich die Verhinderung von Straftaten zum Gegenstand.

Demgegenüber ist zu den von dem angerufenen Gericht seinerzeit herausgearbeiteten Zwecken des Gesetzes Folgendes einzuwenden: Die Aufklärung von Straftaten ist kompetenzrechtlich unergiebig, da für die Verteilung der Gesetzgebungskompetenzen das Ziel einer Aufklärungsmaßnahme maßgeblich ist. Die Verfolgung von Straftaten unterfällt in der Tat Art. 74 Abs. 1 Nr. 1 GG, ist aber nicht das Ziel von Überwachungsmaßnahmen der Verfassungsschutzbehörden.

> Näher zu den Aufgaben der Nachrichtendienste in Abgrenzung zu Polizei- und Strafverfolgungsbehörden BVerfGE 133, 277 (325 ff.).

Die Verhinderung von Straftaten ist unmittelbar nicht Gegenstand der Aufgabe der Verfassungsschutzbehörden, die sich auf Beobachtung und Bewertung beschränkt. Selbst wenn sie aber als mittelbares Ziel von Überwachungen nach § 3 G 10 anzusehen sein sollte, lässt sich die Verhinderung von Straftaten jedoch nicht unter Art. 74 Abs. 1 Nr. 1 GG subsumieren. Eine allgemeine Gesetzgebungskompetenz des Bundes für präventiv ausgerichtete Überwachungsmaßnahmen besteht gerade nicht. Nur bereichsspezifisch lässt sich eine Gesetzgebungskompetenz des Bundes begründen,

wenn bestimmte Überwachungsmaßnahmen notwendig mit einem Sachbereich zusammenhängen, für den eine Bundeskompetenz besteht.

> BVerfGE 113, 348 (369), unter Verweis auf BVerfGE 109, 190 (215); ähnlich BVerfGE 110, 33 (48).

Als Kompetenztitel für Überwachungsermächtigungen im Verfassungsschutzrecht kommt daher allein Art. 73 Abs. 1 Nr. 10 lit. b und c GG in Betracht. Danach ist der Bund ausschließlich dafür zuständig, die Zusammenarbeit des Bundes und der Länder zum Verfassungsschutz und zum Schutz gegen gewaltbereite inländische Bestrebungen, die auswärtige Belange der Bundesrepublik gefährden, zu regeln. Der Begriff der Zusammenarbeit verdeutlicht, dass es hierbei um ein Kooperationsrecht für Bundes- und Landesbehörden mit parallelen Aufgaben und in den Grenzen ihrer je eigenen Befugnisse geht.

> Vgl. BVerfGE 133, 277 (317 f.).

Im Übrigen sind die Länder zum Erlass von Gesetzen zur Abwehr von Bestrebungen gegen die freiheitliche demokratische Grundordnung befugt, soweit sich diese im jeweiligen Land auswirken und damit dort Gefahren hervorrufen können.

> BVerfGE 113, 63 (79).

In extensiver Interpretation mag zu der Gesetzgebungskompetenz des Bundes für die Zusammenarbeit des Bundes und der Länder im Verfassungsschutz noch gehören, dass der Bund den Ländern Mindeststandards für die Aufgaben und möglicherweise auch für bestimmte Befugnisse der Landesverfassungsschutzbehörden auferlegt, um eine hinreichend effektive Kooperation zu gewährleisten.

> Hierfür etwa BVerwG, Beschluss vom 9. Januar 1995 – 1 B 231.94 u.a., DÖV 1995, 692 (693); Uhle, in: Maunz/Dürig, GG, Bearbeitungsstand 2010, Art. 73 Rn. 233.

Dabei kann es sich jedoch allenfalls um rahmenartige Vorgaben handeln. Innerhalb dieses Rahmens muss den Ländern freistehen, zu welchen Maßnahmen sie ihre Verfassungsschutzbehörden unter welchen Voraussetzungen ermächtigen. Der Bund kann dementsprechend nicht selbst Eingriffsermächtigungen für die Landesverfassungsschutzbehörden schaffen, besonders dann nicht, wenn diese Ermächtigungen nicht unmittelbar der Zusammenarbeit von Bund und Ländern dienen. Gerade eine solche eigenständige Eingriffsermächtigung enthält jedoch § 3 G 10, soweit die Norm

auch für die Landesverfassungsschutzbehörden gilt. Diese Regelung lässt sich daher auf Art. 73 Abs. 1 Nr. 10 GG auch bei extensivster Auslegung nicht mehr stützen.

b) Auswirkung auf die landesrechtliche Ergänzungsregelung des § 8 Abs. 12 HmbVerfSchG

An dem Kompetenzverstoß von § 3 G 10 nimmt § 8 Abs. 12 HmbVerfSchG teil. Zwar ist der Hamburgische Landesgesetzgeber gemäß Art. 70 GG befugt, Ermächtigungen zu Telekommunikationsüberwachungen durch das LfV zu schaffen. Die kompetenzwidrigen Regelungen in §§ 3 ff. G 10 stehen dem nicht entgegen.

Jedoch enthält § 8 Abs. 12 HmbVerfSchG gerade keine eigenständige Überwachungsermächtigung, sondern lediglich eine unselbstständige Regelung bestimmter technischer Vorbereitungsmaßnahmen. § 8 Abs. 12 HmbVerfSchG geht offenkundig von der Geltung von § 3 G 10 aus und stützt sich insbesondere auf dessen Eingriffsvoraussetzungen. § 3 G 10 ist aber kompetenzwidrig zustande gekommen und daher unbeachtlich. Allein taugt § 8 Abs. 12 HmbVerfSchG nicht als Rechtsgrundlage für die Quellen-TKÜ, weil er eben keine eigenen Voraussetzungen für einen Eingriff regelt. Ohne den in Bezug genommenen § 3 G 10 läuft die Befugnis ins Leere. Daran ändert sich auch nichts dadurch, dass § 8 Abs. 12 Satz 8 HmbVerfSchG die entsprechende Geltung von § 3 G 10 anordnet. Hiermit sollen nach der Gesetzesbegründung die Anforderungen für eine Anordnung nach dem G 10 entsprechend gelten, nicht aber die Kompetenzwidrigkeit der Norm aufgefangen werden.

> Hamburgische Bürgerschaft Drs. 21/18578, S. 44.

Im Ergebnis wird § 8 Abs. 12 HmbVerfSchG durch die Kompetenzwidrigkeit seiner Bezugsnorm nicht nur gegenstandslos. Wird § 8 Abs. 12 HmbVerfSchG vielmehr als eine unselbstständige Regelung bestimmter technischer Vorbereitungsmaßnahmen für Telekommunikationsüberwachungen nach § 3 G 10 verstanden, so erzeugt diese Regelung den Rechtsschein der Verfassungskonformität und Wirksamkeit der kompetenzwidrigen bundesrechtlichen Norm. Der hamburgische Gesetzgeber ist jedoch nicht dazu befugt, einen solchen Rechtsschein zu setzen. Denn die Kompetenzordnung steht nicht zur Disposition der Länder. Landesgesetzliche Regelungen können daher dem Bund keine Gesetzgebungsbefugnisse einräumen, die er nach dem Grundgesetz nicht hat.

BVerfGE 1, 14 (35); Uhle, in: Maunz/Dürig, GG, Bearbeitungsstand 2008, Art. 70 Rn. 154 m.w.N.

Rechtsstaatlich ist es daher geboten, den von § 8 Abs. 12 HmbVerfSchG erzeugten Rechtsschein zu beseitigen, indem die Verfassungswidrigkeit der Norm als bloßer Ergänzungsregelung festgestellt wird. Anschließend mag der Hamburgische Landesgesetzgeber eine kompetenzgemäße originäre Überwachungsermächtigung schaffen.

c) Hilfsweise: Kompetenzwidrigkeit von § 8 Abs. 12 HmbVerfSchG, falls das G 10 kompetenzgemäß ergangen ist

Wird entgegen der oben begründeten Auffassung davon ausgegangen, dass der Bund die Gesetzgebungskompetenz für Überwachungsermächtigungen der Landesverfassungsschutzbehörden hat, so ist § 8 Abs. 12 HmbVerfSchG selbst kompetenzwidrig. Denn in diesem Fall ist für eine landesrechtliche Regelung zu Telekommunikationsüberwachungen durch das Landesamt auch dann kein Raum, wenn § 8 Abs. 12 HmbVerfSchG lediglich als unselbstständige Ergänzungsregelung zu § 3 G 10 begriffen wird.

Die Gesetzgebungskompetenz des Bundes für § 3 G 10 lässt sich, soweit es um Überwachungsmaßnahmen durch Landesverfassungsschutzbehörden geht, allenfalls auf Art. 73 Abs. 1 Nr. 10 GG stützen. Der von dem angerufenen Gericht 1970 beschrittene Weg über Art. 74 Abs. 1 Nr. 1 GG ist jedenfalls heute nicht mehr gangbar, will man nicht fundamental mit der jüngeren Rechtsprechung zu diesem Kompetenztitel brechen.

Art. 73 Abs. 1 Nr. 10 GG begründet eine ausschließliche Gesetzgebungskompetenz des Bundes. In ihrem Anwendungsbereich sind die Länder gemäß Art. 71 GG zur Gesetzgebung nur dann berufen, wenn und soweit der Bund sie hierzu ausdrücklich gesetzlich ermächtigt hat. Eine solche Ermächtigung der Länder findet sich weder im G 10, das in § 16 G 10 lediglich für die parlamentarische Kontrolle von Überwachungen auf das Landesrecht verweist, noch in einem anderen Bundesgesetz.

2. Objektivrechtliche Anforderungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

§ 8 Abs. 12 HmbVerfSchG verletzt sämtliche Beschwerdeführer*innen in ihrem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

Das Land Hamburg hätte die genannte Befugnis mit einem effektiven Schwachstellen-Management verbinden müssen, welches insbesondere die Verwendung von Sicherheitslücken verhindert, die dem Hersteller des betreffenden Systems noch nicht bekannt sind.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme leitet sich nach der Rechtsprechung des angerufenen Gerichts aus dem allgemeinen Persönlichkeitsrecht ab (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

BVerfGE 120, 274 (302 ff.).

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

BVerfGE 120, 274 (314).

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ist aber nicht nur ein subjektives Abwehrrecht gegen staatliche Eingriffe. Es begründet – wie schon der Begriff der Gewährleistung zeigt – auch eine staatliche Pflicht dazu beizutragen, dass die Sicherheit der informationstechnischen Infrastruktur der Bundesrepublik ein hohes Niveau erreicht. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme trägt so einerseits der hohen Bedeutung der Informationstechnik für die Funktionsfähigkeit von Staat und Gesellschaft, andererseits der erheblichen Verwundbarkeit dieser Technologie Rechnung.

Vgl. nur Kutscha, NJW 2008, 1042 (1044); Roßnagel/Schnabel, NJW 2008, 3534 (3535); Hoffmann-Riem, JZ 2009, 165 ff.; ders., JZ 2014, 53 ff.; Becker, NVwZ 2015, 1335 (1339 f.).

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

Vgl. zu aus unterschiedlichen Grundrechten hergeleiteten staatlichen Schutzpflichten etwa BVerfGE 49, 89 (142); BVerfGE 77, 17 (214 f.); BVerfGE 88, 203 (251 ff.); BVerfGE 92, 26 (46); BVerfGE 106, 28 (37); BVerfGE 125, 39 (78 f.); BVerfGE 143, 313 (337 f.).

Der grundrechtliche Mindeststandard wird allerdings zumindest dann unterschritten, wenn eine staatliche Stelle ohne zureichenden Grund eine Gefährdungslage für die Vertraulichkeit und Integrität der informationstechnischen Infrastruktur in der Bundesrepublik bewusst aufrechterhält oder sogar selbst schafft. Eine solche Situation kann im Zusammenhang mit Quellen-Telekommunikationsüberwachungen auftreten.

Um die von den informationstechnischen Systemen ausgehende Kommunikation zu überwachen ist es notwendig, eine Software auf den Systemen zu installieren, die dies ermöglicht. Da die Zielpersonen der Überwachung dies nicht freiwillig tun werden und auch eine Implementierung der Software bei Auslieferung sämtlicher in Frage kommender Systeme nicht als praktisch umsetzbar erscheint, wird es regelmäßig notwen-

dig sein, die Software durch einen verdeckten hoheitlichen Zugriff auf das System einzuschleusen.

Weitgehend ungeklärt ist bislang, auf welchem Weg dies technisch erfolgen soll. Denkbar sind verschiedene Arten physischer Zugriffe und Fernzugriffe auf das Zielsystem. Ein physischer Zugriff kann etwa dadurch erfolgen, dass Ermittler heimlich eine Wohnung betreten und dort eine Spionagesoftware auf einem PC installieren. Außerhalb von Wohnungen könnten Behörden zudem im Rahmen von Maßnahmen wie Zoll- oder Verkehrskontrollen vorübergehend die Sachherrschaft über mobile Endgeräte erlangen. Fernzugriffe sind über das Ausnutzen von Sicherheitslücken eines IT-Systems denkbar. Schließlich bietet die Manipulation des Nutzers eines Systems verschiedene Optionen zur Herbeiführung einer Infektion. Die Installation eines Programmes kann etwa in „Phishing“-Manier erfolgen, indem einem Nutzer unter falschem Absender E-Mails mit infizierten Anhängen zugeschickt werden, die der Nutzer nur noch öffnen muss.

Da es in den meisten Fällen praktisch schwierig sein wird, physischen Zugriff auf das Zielsystem zu erlangen, ist davon auszugehen, dass die Infektion per Fernzugriff regelmäßig notwendig sein wird, um Quellen-Telekommunikationsüberwachungen durchzuführen. Ein solcher Fernzugriff kann dadurch erfolgen, dass das LfV oder andere Behörden Sicherheitslücken in Soft- und Hardware des Zielsystems ausnutzen. Hierfür geeignet sind namentlich Sicherheitslücken, die Softwareherstellern und Nutzer*innen noch nicht bekannt sind. Informationen über derartige Sicherheitslücken werden auf dem internationalen Schwarzmarkt für hohe Summen verkauft und spielen eine zentrale Rolle sowohl für Überwachungsmaßnahmen staatlicher Stellen als auch für die organisierte Kriminalität. Es ist davon auszugehen, dass sie auch bei der Umsetzung von Maßnahmen nach § 8 Abs. 12 Satz 1 HmbVerfSchG von herausgehobener Bedeutung sind.

Die Möglichkeit für das LfV, Quellen-Telekommunikationsüberwachungen durch das Ausnutzen von Sicherheitslücken durchzuführen, führt zu Fehlanreizen und gefährdet im Ergebnis die kollektive IT-Sicherheit: Wenn der Verfassungsschutz solche Lücken ausnutzen darf, so entsteht ein Interesse daran, ein „Arsenal“ von Sicherheitslücken aufzubauen, um im Falle des Falles auf Zielsysteme zugreifen zu können. Dieses Interesse kann Behörden davon abhalten, eine entdeckte oder gar auf dem Schwarzmarkt angekaufte Sicherheitslücke den Herstellern der IT-Systeme oder dem Bundes-

amt für Sicherheit in der Informationstechnik mitzuteilen, damit sie geschlossen werden kann.

Im Sinne der Effektivität der Überwachungsmaßnahme muss die Sicherheitslücke möglichst lange geheim gehalten werden. Wird die Sicherheitslücke bekannt, besteht die Gefahr, dass sie geschlossen wird und darum die Infiltration von vornherein misslingt oder die Maßnahme vorzeitig abgebrochen werden muss. Selbst nach Beendigung der einzelnen Überwachungsmaßnahme besteht ein Interesse daran, eine Sicherheitslücke weiterhin geheim zu halten, um sie für weitere Maßnahmen nutzen zu können.

Die Ausnutzung von Sicherheitslücken durch staatliche Stellen kann zugleich in mehrfacher Hinsicht die Bedrohungslage für die informationstechnische Infrastruktur in der Bundesrepublik aufrechterhalten oder sogar noch verschärfen. Wird eine Sicherheitslücke aus den eben genannten Gründen geheim gehalten, so trägt die handelnde Behörde durch ihr Unterlassen dazu bei, dass diese Sicherheitslücke nicht geschlossen wird. Da sich aus technischer Sicht die Infiltration informationstechnischer Systeme durch staatliche Stellen und durch Kriminelle nicht unterscheiden, perpetuiert dieses Unterlassen das Risiko krimineller Übergriffe auf die informationstechnische Infrastruktur.

Zusätzlich hat das Ausnutzen von IT-Sicherheitslücken durch staatliche Stellen zur Folge, dass der Markt für derartige Sicherheitslücken befeuert wird. Es ist derzeit nicht davon auszugehen, dass staatliche Behörden Sicherheitslücken in einem für die Überwachung ausreichenden Umfang selbst aufdecken können.

> So auch Wilfried Karl, der Präsident der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS); https://heise.de/-3976587.

Dementsprechend werden die notwendigen Informationen am Markt beschafft werden müssen, wobei staatliche Behörden in einen Bieterwettbewerb mit Kriminellen und anderen fragwürdigen Akteuren treten würden. Dies würde die Preise für derartige Informationen steigern und Sicherheitsforscher*innen vermeidbare Anreize verschaffen, Erkenntnisse über Sicherheitslücken nicht den Herstellern zur Verfügung zu stellen, sondern sie auf dem Schwarzmarkt zu verkaufen. Die staatliche Unterstützung dieses Marktes birgt zusätzlich das erhebliche Risiko, Straftaten zu begünstigen – etwa den unbefugten Zugriff auf Daten (§ 202a StGB) und Vorbereitungshandlungen (§ 202c StGB).

Eine staatliche Stelle, die über einen geheim gehaltenen Bestand von Informationen über Sicherheitslücken verfügt, die selbst dem Hersteller der Soft- oder Hardware nicht bekannt sind, ist schließlich selbst ein lohnendes Angriffsziel für Kriminelle, die sich diese Informationen beschaffen und für eigene Zwecke nutzen können. Hierbei handelt es sich nicht um ein hypothetisches Szenario, das als Restrisiko der staatlichen Aufklärung außer Acht bleiben könnte. Solche Angriffe liegen vielmehr ausgesprochen nahe und sind schon vorgekommen.

So hat im Mai 2017 das Schadprogramm „WannaCry“ weltweit erhebliche Schäden verursacht. In Deutschland war davon etwa die Deutsche Bahn betroffen. Besonders schwer traf es das Gesundheitssystem in Großbritannien. Zahlreiche Rechner des National Health Service waren befallen. Die Daten von Krebs- und Herzpatient*innen standen nicht mehr zur Verfügung. Viele Kranke mussten in andere Kliniken umgeleitet werden. „WannaCry“ nutzte eine Sicherheitslücke in Windows-Betriebssystemen aus, welche die kriminellen Angreifer nach verbreiteter Einschätzung mitsamt der zugehörigen Angriffswerkzeuge bei der US-amerikanischen National Security Agency (NSA) ausgespäht hatten, die ihrerseits diese Sicherheitslücke für eigene Zwecke eingesetzt und geheim gehalten hatte.

> Vgl. Zeit Online vom 15. Mai 2017, https://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung.

Es ist unwahrscheinlich, dass deutsche Sicherheitsbehörden die bei ihnen vorhandenen Informationen über Sicherheitslücken bedeutend besser schützen können als die NSA. Vielmehr ist anzunehmen, dass ein Verlust sich nie ausschließen lässt.

Werden die Risiken und die möglichen Erträge der staatlichen Infiltration informationstechnischer Systeme mithilfe von unbekannten Sicherheitslücken einander gegenübergestellt, so ergibt sich, dass dieser Infiltrationsweg ausgeschlossen werden muss. Die durch die Nutzung und Geheimhaltung solcher Sicherheitslücken eröffneten oder zumindest erhöhten Risiken wiegen äußerst schwer.

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

stört, so kann dies zu Leistungsausfällen oder Schadensereignissen führen, die schlimmstenfalls den Verlust von Menschenleben zur Folge haben können. So verstarb im September 2020 eine Patientin eines Wuppertaler Krankenhauses nach erfolgloser Behandlung. Sie hätte eigentlich in der Uniklinik Düsseldorf sein sollen, wo ihre Behandlung bereits eine Stunde früher als in Wuppertal hätte stattfinden können. Die Uniklinik war jedoch zu diesem Zeitpunkt aufgrund eines Ausfalls ihrer IT-Systeme von der Notfallversorgung abgemeldet. Hacker hatten eine Sicherheitslücke in der IT des Klinikums ausgenutzt, um 30 Server zu verschlüsseln und ein Lösegeld für deren Freigabe zu erpressen.

heise online vom 17. September 2020, https://heise.de/-4904134.

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

Hingegen wiegt der Effektivitätsverlust, der durch ein Verbot der Ausnutzung von IT-Sicherheitslücken für die Aufgabenerfüllung der Sicherheitsbehörden droht, weniger schwer. Dies gilt besonders für das LfV, das die Quellen-TKÜ im Gegensatz zur Polizei nicht zur Abwehr konkreter Gefahren oder in deren unmittelbaren Vorfeld einsetzt.

Zwar haben die Belange, denen Quellen-Telekommunikationsüberwachungen des LfV dienen, schon wegen der grundrechtlich gebotenen restriktiven Fassung des Eingriffstatbestands durchweg ein hohes Gewicht. Jedoch können diese Belange zumeist auch auf weniger riskanten Wegen erreicht werden. So ist es aus objektiv-rechtlicher Sicht beispielsweise unbedenklich, wenn zur Infiltration des Zielsystems einer Quellen-TKÜ eine physische Zugriffsmöglichkeit (etwa im Rahmen einer Durchsuchung) oder eine bereits bekannte, auf diesem System jedoch noch nicht geschlossene Sicherheitslücke ausgenutzt werden. Soweit im Einzelfall eine Infiltration auf solchen Wegen nicht möglich sein sollte, ist der damit verbundene Ausfall dieser Überwachungsmaßnahmen hinzunehmen und auf andere, gegebenenfalls aufwändigere Maßnahmen auszuweichen.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verpflichtet die staatliche Gewalt mithin dazu, auf die Nutzung und Geheimhaltung von Sicherheitslücken zum Zweck der Infiltration informationstechnischer Systeme zu verzichten. Es ist Sache des Gesetzgebers, diese Pflicht durch ein ausdrückliches gesetzliches Verbot umzusetzen. Nur durch ein ausdrückliches Verbot erhalten die Sicherheitsbehörden eine eindeutige Vorgabe, die das durch die Befugnisse zu Quellen-TKÜ und „Online-Dursuchung“ geschaffene Risiko für die Sicherheit der informationstechnischen Infrastruktur der Bundesrepublik sicher ausschließt. Dass es einer solchen Vorgabe bedarf, illustriert beispielhaft die Antwort der Bundesregierung auf eine parlamentarische Kleine Anfrage, in der die Bundesregierung eine Nutzung von unbekannten IT-Sicherheitslücken („Zero-Day-Exploits“) zumindest nicht ausgeschlossen hat:

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

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

- die Verbreitung der Sicherheitslücke
    - in quantitativer Hinsicht: Zahl der betroffenen Nutzerinnen und Nutzer,

    - in qualitativer Hinsicht: Art der betroffenen Nutzerinnen und Nutzer,
- das Gewicht der Sicherheitslücke
    - zur Ausnutzung erforderlicher Aufwand,
    - aus der Ausnutzung resultierender Schaden,
- die Wahrscheinlichkeit, dass Betroffene die Ausnutzung der Lücke bemerken und im Einzelfall Gegenmaßnahmen einleiten,
- die Wahrscheinlichkeit einer technischen Lösung für die Lücke,
- die Wahrscheinlichkeit einer Verbreitung der technischen Lösung,
- Möglichkeiten zur Linderung der Folgen bei einer (zeitweisen) Geheimhaltung der Lücke,
- die Wahrscheinlichkeit, dass Dritte die Lücke finden.

Vgl. Herpig, Schwachstellen-Management für mehr Sicherheit, 2018, https://www.stiftung-nv.de/de/publikation/schwachstellen-management-fuer-mehr-sicherheit.

Da § 8 Abs. 12 HmbVerfSchG kein ausdrückliches Verbot einer Nutzung und Geheimhaltung von unbekannten Sicherheitslücken zum Zweck der Infiltration enthält und auch keine Vorgaben für ein behördliches Schwachstellen-Management errichtet, ist die Vorschrift in diesem Punkt verfassungswidrig.

3. Unverhältnismäßigkeit und Weite

Schließlich ist § 8 Abs. 12 HmbVerfSchG auch hinsichtlich seiner materiellen Eingriffsschwellen verfassungswidrig und verfehlt die aus dem Grundsatz der Verhältnismäßigkeit folgenden Anforderungen an Transparenz und Kontrolle.

a) Maßstab

Die verfassungsrechtlichen Maßstäbe, denen die Tatbestände von Überwachungsermächtigungen im Verfassungsschutzrecht genügen müssen, lassen sich aus der Rechtsprechung des angerufenen Gerichts zum Sicherheitsrecht ableiten. Ausgangspunkt ist der Verhältnismäßigkeitsgrundsatz und insbesondere das Gebot der Verhält-

nismäßigkeit im engeren Sinne. Danach sind an die gesetzlichen Eingriffsschwellen desto höhere Anforderungen zu stellen, je schwerer der geregelte Überwachungseingriff wiegt. Dies kann dazu führen, dass eine bestimmte Überwachungsmaßnahme nicht zur Durchsetzung bestimmter Allgemeininteressen angewandt werden darf, weil die davon ausgehenden Grundrechtsbeeinträchtigungen schwerer wiegen als die durchzusetzenden Belange.

Vgl. BVerfGE 120, 274 (322).

Im Einzelnen knüpfen die verfassungsrechtlichen Anforderungen an die gesetzliche Eingriffsschwelle an zwei Parameter an: Erstens muss das Gesetz einen hinreichend gewichtigen Anlass für die jeweilige Überwachungsmaßnahme in normenklarer Weise regeln. Zweitens muss das Gesetz gewährleisten, dass die Zielperson der Überwachungsmaßnahme in einem hinreichenden Näheverhältnis zu dem Anlass der Maßnahme steht.

Für die Konkretisierung der verfassungsrechtlichen Maßstäbe ist insbesondere bedeutsam, ob und inwieweit auf die Rechtsprechung des angerufenen Gerichts zu präventivpolizeilichen Überwachungsmaßnahmen zurückgegriffen werden kann, um Ermächtigungen im Verfassungsschutzrecht zu beurteilen.

Im Ausgangspunkt hat das angerufene Gericht wiederholt anerkannt, dass die unterschiedlichen Aufgaben und Befugnisse von Polizeibehörden und Nachrichtendiensten es grundsätzlich rechtfertigen, an Überwachungsermächtigungen im Nachrichtendienstrecht weniger strenge Anforderungen zu stellen als an entsprechende Ermächtigungen im Polizeirecht.

Vgl. BVerfGE 100, 313 (383); BVerfGE 120, 274 (330); BVerfGE 133, 277 (325 ff.); kritisch mit der Forderung nach einer partiellen „Deprivilegierung der Geheimdienste“ Wegener, VVDStRL 75 (2016), S. 293 (312 ff.).

Allerdings ist zugleich seit geraumer Zeit in der Rechtsprechung anerkannt, dass sich die verfassungsrechtlichen Anforderungen an die gesetzlichen Eingriffsschwellen auch im Nachrichtendienstrecht mit zunehmender Eingriffsintensität der jeweiligen Überwachungsmaßnahme verschärfen.

Vgl. beispielhaft zu Eingriffen in das Fernmeldegeheimnis BVerfGE 120, 274 (342 f.); BVerfG NJW 2020, 2699 (2710 Rn. 145).

Bereits mehrfach hat zudem das angerufene Gericht deutlich gemacht, dass die Anforderungen an Überwachungsermächtigungen des Nachrichtendienstrechts bei besonders eingriffsintensiven Maßnahmen mit den Anforderungen an polizeirechtliche Ermächtigungen konvergieren. Für solche Maßnahmen hat das angerufene Gericht ausdrücklich ausgeführt, dass die verfassungsrechtliche Mindesteingriffsschwelle auch nicht deshalb abzusenken ist, weil die Nachrichtendienste aufgrund ihres spezifischen Auftrags zur Vorfeldaufklärung nicht dazu berufen sind, konkrete Gefahren mit imperativen Mitteln abzuwehren.

> Vgl. zur Online-Durchsuchung BVerfGE 120, 274 (329 ff.); zum Abruf bevorrateter Telekommunikations-Verkehrsdaten BVerfGE 125, 260 (331 f.).

Im Gegenteil hat das angerufene Gericht die Aktivitäten der Nachrichtendienste als besonders belastend bewertet, weil die gesamte Tätigkeit geheim erfolgt und „das Gefühl des unkontrollierbaren Beobachtetwerdens“ befördert.

> BVerfGE 125, 260 (332).

Auf der Grundlage des Urteils zum BKA-Gesetz, das die verfassungsrechtlichen Anforderungen an präventivpolizeiliche Überwachungsermächtigungen präzisiert und konsolidiert hat, lassen sich die Maßstäbe auch für Ermächtigungen im Nachrichtendienstrecht weiter schärfen. In diesem Urteil hat das angerufene Gericht eingriffsintensive Überwachungsmaßnahmen an das Erfordernis einer konkreten Gefahr als einheitliche Mindesteingriffsschwelle gebunden. Zugleich hat das Gericht den verfassungsrechtlichen Begriff der konkreten Gefahr von dem polizeirechtlichen Gefahrbegriff entkoppelt und im Verhältnis zu diesem erweitert.

Eine konkrete Gefahr im verfassungsrechtlichen Sinne liegt danach nicht nur dann vor, wenn situationsbezogen ein Schaden mit hinreichender Wahrscheinlichkeit droht, wie es der polizeirechtliche Gefahrbegriff verlangt. Daneben könne eine „hinreichend konkretisierte Gefahr“ auch schon bestehen, „wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen.“ Diese Tatsachen müssten „zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden

kann.“ In Bezug auf terroristische Straftaten hat das angerufene Gericht es darüber hinaus für ausreichend gehalten, „wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird“.

BVerfGE 141, 220 (272).

Insbesondere die zweite Formulierung zielt erkennbar auf eine Ergänzung der situationsbezogenen Schadensprognose des hergebrachten polizeirechtlichen Gefahrbegriffs um eine personenbezogene Gefährlichkeitsprognose, die allerdings auf hinreichend aussagekräftigen Tatsachen beruhen muss.

Vgl. für einen Ansatz zur rechtsdogmatischen Erfassung und Rationalisierung personenbezogener Prognoseurteile Bäcker, Kriminalpräventionsrecht, 2015, S. 205 ff.

Ob diese Erweiterung des verfassungsrechtlichen Gefahrbegriffs durchweg eine tragfähige Grundlage für eine rechtsstaatskonforme Konsolidierung des Polizeirechts darstellt, oder ob es sich um eine konzeptionell problematische Verwischung unterschiedlicher Tatbestandskategorien und hinsichtlich von höchst eingriffsintensiven Überwachungsmaßnahmen wie Wohnraumüberwachung und „Online-Durchsuchung“ um eine bedenkliche Aufweichung rechtsstaatlicher Grundsätze handelt, mag hier offenbleiben. Jedenfalls ist der erweiterte verfassungsrechtliche Gefahrbegriff für das Nachrichtendienstrecht anschlussfähig.

Einerseits ermöglicht der erweiterte verfassungsrechtliche Gefahrbegriff Überwachungsmaßnahmen bereits im Vorfeld akuter Krisenlagen, das in besonderem Maße die Domäne der nachrichtendienstlichen Aufklärung darstellt. Insbesondere ein personenbezogener Prognosetatbestand kommt dem spezifischen Aufklärungsauftrag des Verfassungsschutzes entgegen, indem er Überwachungsmaßnahmen gegen „Gefährder“ bereits im Vorfeld klar konturierter schadensträchtiger Situationen ermöglicht.

Andererseits schirmt der erweiterte verfassungsrechtliche Gefahrbegriff das Risiko ab, dass gerade die Nachrichtendienste Überwachungsmaßnahmen von hoher Eingriffsintensität im Wesentlichen auf allgemeine Erfahrungssätze stützen könnten, deren Gebrauch rechtlich nicht näher angeleitet wird und die möglicherweise nur sehr grobe Prognosen zulassen. Denn der erweiterte verfassungsrechtliche Gefahrbegriff ermög-

licht Überwachungsmaßnahmen gerade nur gegenüber Personen, die aufgrund ihres Vorverhaltens belastbar als „gefährlich“ gekennzeichnet werden können.

Die von dem angerufenen Gericht umrissene personenbezogene Gefährlichkeitsprognose eignet sich daher besonders dazu, personengerichtete Überwachungsmaßnahmen der Nachrichtendienste im benötigten Umfang zu ermöglichen und sie zugleich hinreichend trennscharf zu begrenzen.

Damit ist nach der partiellen Neukonzeption der verfassungsrechtlichen Anforderungen an das Polizeirecht im Urteil zum BKA-Gesetz nunmehr auch eine Anpassung der verfassungsrechtlichen Anforderungen an das Nachrichtendienstrecht angezeigt. Personengerichtete Überwachungsmaßnahmen hoher Eingriffsintensität sind auch im Nachrichtendienstrecht an eine situationsbezogene Schadens- oder eine personenbezogene Gefährlichkeitsprognose zu binden, wie sie das angerufene Gericht für das Polizeirecht entwickelt hat. Eine Absenkung der verfassungsrechtlichen Mindesteingriffsschwelle ist für solche Überwachungsmaßnahmen nach der Erweiterung des verfassungsrechtlichen Gefahrbegriffs nicht (mehr) angezeigt.

> Vgl. andeutungsweise bereits BVerfGE 141, 220 (340): danach bedürfen „ungeachtet ihres im Wesentlichen auf das Vorfeld von Gefahren beschränkten Handlungsauftrags“ auch Datenerhebungen von Verfassungsschutzbehörden grundsätzlich einer „konkretisierten Gefahrenlage“.

Die Absenkung ist auch nicht sachgerecht, da Nachrichtendienste bei der Aufklärung nicht mit einer geringeren Eingriffsintensität agieren als Polizeibehörden, die im Vorfeld einer Gefahr Informationen erheben. Auch im Fall polizeilicher Ermittlungen sind imperative Folgemaßnahmen keine notwendige Konsequenz. Sofern ihre Möglichkeit eine erhöhte Eingriffsintensität begründet, steht dem bei den Nachrichtendiensten ein im höheren Maße heimliches Agieren gegenüber, welches die Eingriffsintensität ebenso erhöht.

Zur Einstufung der Eingriffsintensität der Aufklärungsmaßnahmen kommt es bei personengerichteten Maßnahmen ohne besondere Streubreite vor allem darauf an, ob sie in besondere Rückzugsbereiche der Privatheit eindringen, auf einem Bruch schutzwürdigen personengebundenen Vertrauens beruhen, Wahrnehmungsschranken insbesondere durch technische Mittel oder ein planvoll verdecktes Vorgehen überwinden oder Eigenschaften, Verhalten oder Sozialkontakte der betroffenen Person in besonderem Maße für die Überwachungsbehörde verfügbar machen.

b) Anwendung des Maßstabs auf den vorliegenden Fall

Falls die Regelung zu Quellen-TKÜ in § 8 Abs. 12 HmbVerfSchG nicht lediglich als (kompetenzwidrige) Ergänzungsregelung zu § 3 G 10 interpretiert wird, ist sie als eigenständige Überwachungsermächtigung an den für solche Ermächtigungen geltenden verfassungsrechtlichen Anforderungen zu messen. Diese Anforderungen verfehlt sie. Zum einen verletzt sie das Gebot der Normenklarheit sowie das Demokratieprinzip, da sie Anlass und Ziel der Überwachung nicht selbst, sondern durch eine dynamische Verweisung auf die bundesrechtliche Vorschrift des § 3 Abs. 1 G 10 regelt. Zum anderen genügt der in Bezug genommene § 3 Abs. 1 G 10 seinerseits nicht den verfassungsrechtlichen Anforderungen an Ermächtigungen zu Telekommunikationsüberwachungen. Schließlich verfehlt die Befugnis zur „kleinen Online-Durchsuchung“ in § 8 Abs. 12 Satz 2 HmbVerfSchG die verfassungsrechtlichen Anforderungen, da sie nicht an Art. 10 Abs. 1 GG, sondern dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu messen ist.

Des Weiteren ist für die Beschwerdeführer*innen zu 2 sowie 4 bis 6 die Pressefreiheit aus Art. 5 Abs. 1 Satz 2 als ergänzender Prüfungsmaßstab neben dem Fernmeldegeheimnis zu berücksichtigen. Die drohende Überwachung beeinträchtigt ihre Tätigkeit im Pressewesen, insbesondere hinsichtlich der notwendigen Vertraulichkeit im Verhältnis zu Informant*innen sowie in der Redaktionsarbeit.

Ebenso wie das angerufene Gericht jüngst in den Befugnissen zur Ausland-Ausland-Fernmeldeaufklärung des BND einen Verstoß gegen die Pressefreiheit festgestellt hat,

BVerfG NJW 2020, 2235 (2247 Rn. 141 ff.),

ist dies auch hier anzunehmen, soweit sich die Quellen-TKÜ gegen Journalist*innen richten kann.

(1) Unzulässige dynamische Verweisung auf § 3 Abs. 1 G 10

Nach § 8 Abs. 12 Satz 8 HmbVerfSchG gilt für die Durchführung einer Quellen-TKÜ § 3 Abs. 1 G 10 entsprechend. Hiermit erfolgt hinsichtlich der Voraussetzungen des Eingriffs eine dynamische Verweisung auf diese Regelung. Auch aus der Gesetzesbegründung geht der Wille des Gesetzgebers hervor, die Quellen-TKÜ unter densel-

ben Voraussetzungen und im selben Verfahren wie eine herkömmliche Beschränkung im Einzelfall nach dem G 10 zuzulassen.

> Hamburgische Bürgerschaft Drs. 21/18578, 44.

Dieses Ziel lässt sich nur im Wege einer dynamischen Verweisung auf das G 10 erreichen, da ansonsten im Zuge der – durchaus häufigen – Änderungen des G 10 Eingriffstatbestand und Verfahrensvorgaben der landesrechtlichen und der bundesrechtlichen Überwachungsermächtigungen im Laufe der Zeit immer weiter voneinander abweichen würden. Demgegenüber lassen sich weder dem Wortlaut noch der Begründung des Gesetzes Anhaltspunkte dafür entnehmen, dass § 8 Abs. 12 Satz 8 HmbVerfSchG als bloß statische Verweisung auf das G 10 zu interpretieren sein könnte.

Soweit § 8 Abs. 12 Satz 8 HmbVerfSchG Anlass und Ziel der Quellen-TKÜ durch eine dynamische Verweisung auf § 3 Abs. 1 G 10 bestimmt, verfehlt die Norm die Anforderungen des rechtsstaatlichen Gebots der Normenklarheit und des Demokratieprinzips.

Dynamische Verweisungen insbesondere zwischen Regelungen unterschiedlicher Gesetzgeber sind nach der Rechtsprechung des angerufenen Gerichts zwar nicht generell ausgeschlossen. Sie sind aber nur in dem Rahmen zulässig, den die Prinzipien der Rechtsstaatlichkeit, der Demokratie und der Bundesstaatlichkeit ziehen. Grundrechtliche Gesetzesvorbehalte können diesen Rahmen zusätzlich einengen.

> BVerfGE 47, 285 (312); BVerfGE 67, 348 (363); ferner zu Verweisen aus Gesetzen auf außerstaatliche Regelungswerke BVerfGE 64, 208 (214); BVerfGE 78, 32 (36).

Aus den Grundrechten, ferner auch aus dem Demokratieprinzip ergeben sich besonders hohe Anforderungen an die gesetzliche Regulierung verdeckter Überwachungsmaßnahmen der Sicherheitsbehörden. Insbesondere die gesetzlichen Eingriffsschwellen sind in der Eingriffsermächtigung hinreichend bestimmt anzugeben, um die Kontrollierbarkeit und Vorhersehbarkeit des behördlichen Handelns zu gewährleisten.

> Vgl. etwa BVerfGE 110, 33 (53 ff.); BVerfGE 113, 348 (375 ff.); BVerfGE 120, 378 (407 ff.).

Darüber hinaus hat die Gestaltung der gesetzlichen Eingriffsschwellen bei verdeckten Überwachungsmaßnahmen eine wesentliche demokratische Funktion. Da Art und Ausmaß solcher Überwachungen im Einzelfall auch im Nachhinein nicht flächendeckend bekanntwerden, muss die öffentliche Auseinandersetzung über die Befugnisse

der Sicherheitsbehörden zwangsläufig zu erheblichen Teilen anhand der abstrakt-generellen Eingriffsermächtigungen geführt werden. Dies setzt eine hinreichend gehaltvolle Fassung der Eingriffsvoraussetzungen voraus.

Den spezifischen Funktionen des formellen Gesetzes für sicherheitsbehördliche Überwachungsermächtigungen entspricht eine grundrechtliche und demokratische Regelungsverantwortung des Gesetzgebers. Er muss die Voraussetzungen einer Überwachung selbst möglichst trennscharf beschreiben, um so Überwachungen im Einzelfall voraussehbar und kontrollierbar zu machen und eine generelle Diskussion über die jeweilige Überwachungsmaßnahme zu ermöglichen. Durch die dynamische Verweisung auf das G 10 hat sich der Hamburgische Gesetzgeber dieser Regelungsverantwortung partiell entzogen. Die Gestaltung des gesetzlichen Eingriffstatbestands ist aufgrund dieser Verweisung zukünftig nicht mehr Sache des Landesgesetzgebers, sondern er gibt sie aus der Hand. Für denkbare Erweiterungen der Ermächtigung und die damit verbundenen grundrechtlichen Probleme muss er dann nicht mehr einstehen. Auch eine spezifisch auf das LfV bezogene demokratische Diskussion wird anlässlich solcher Änderungen nicht mehr zu führen sein. In einem so sensiblen Regelungsfeld wie dem sicherheitsbehördlichen Eingriffsrecht ist eine derartige Delegation grundrechtlicher Regelungsverantwortung nicht hinnehmbar.

Generell ist zu rügen, dass das System der fragmentarischen Verweise auf Regelungen des G 10 in § 8 Abs. 12 Satz 8 HmbVerfSchG für die Betroffenen von Überwachungsmaßnahmen kaum zu durchschauen ist. Das Gesamtsystem der Schutzmechanismen zugunsten der Betroffenen ergibt sich erst aus einer aufwändigen Zusammenschau der beiden Regelungskomplexe, die allenfalls durch spezialisierte Jurist*innen zu leisten ist. Daher ist auch anzunehmen, dass auch die die Überwachungsmaßnahme flankierenden Vorschriften durch den Hamburgischen Gesetzgeber selbst zu regeln sind.

(2) Defizite der Eingriffstatbestände in § 3 Abs. 1 G 10

Darüber hinaus genügen die in § 3 Abs. 1 G 10 enthaltenen Eingriffstatbestände ihrerseits nicht den verfassungsrechtlichen Anforderungen an Ermächtigungen zu eingriffsintensiven Überwachungsmaßnahmen. Da § 8 Abs. 12 HmbVerfSchG keine eigenen Anlassschwellen für die Quellen-TKÜ aufstellt, schlagen die hier angeführten Mängel der Eingriffstatbestände unmittelbar auf diese Regelung durch.

§ 3 Abs. 1 G 10 enthält zwei alternative Eingriffstatbestände: Nach § 3 Abs. 1 Satz 1 G 10 darf die Telekommunikation überwacht werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine Straftat aus einem Straftatkatalog plant, begeht oder begangen hat. Nach § 3 Abs. 1 Satz 2 G 10 ist eine Überwachung zulässig, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Mitglied einer Vereinigung ist, die auf Straftaten gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes ausgerichtet ist.

Gemäß § 3 Abs. 1 Satz 1 i.V.m. § 1 Abs. 1 Nr. 1 G 10 muss die Überwachung zudem dazu dienen, Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes, eines Landes oder der in Deutschland stationierten NATO-Truppen abzuwehren. Dieses weitere Erfordernis begrenzt allerdings den Ermächtigungstatbestand kaum. Insbesondere kann § 1 Abs. 1 Nr. 1 G 10 angesichts der Aufgabe der Nachrichtendienste, Bedrohungslagen im Vorfeld akuter Krisen aufzuklären, nicht so verstanden werden, dass bereits eine konkrete Gefahr im polizeirechtlichen Sinne vorliegen müsste.

> So die allgemeine Auffassung, etwa Günther, in Münchener Kommentar zur StPO, 2018, § 1 G 10 Rn. 14; Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 1 G 10 Rn. 33.

Die Ermächtigungen in § 3 Abs. 1 G 10 sind sehr weit gefasst und ermöglichen Telekommunikationsüberwachungen bereits in diffusen Bedrohungslagen mit teils nur geringem Schadenspotential. Sie verfehlen daher zumindest in weitem Umfang die auch für die Nachrichtendienste zu beachtende verfassungsrechtliche Mindesteingriffsschwelle einer (verfassungsrechtlichen) konkreten Gefahr für ein besonders bedeutsames Rechtsgut.

Bei § 3 Abs. 1 Satz 1 G 10 beruht dies auf drei Defiziten, die einander zudem noch wechselseitig verstärken:

Erstens knüpft dieser Eingriffstatbestand nicht nur an die gegenwärtige Begehung einer Straftat an, die zumindest in der Regel auf eine Rechtsgutsgefahr schließen lässt, sondern ermöglicht Übermittlungen bereits im Planungsstadium. Der Umstand allein, dass jemand eine Straftat plant, begründet jedoch noch nicht zwangsläufig eine Gefahr für die Rechtsgüter, die durch diese Straftat verletzt würden. Die Planungen können sich noch in einem so frühen Stadium befinden und es können vor der Tatbegehung

noch so erhebliche Hürden zu überwinden sein, dass eine konkrete Straftat nicht einmal grob konturiert absehbar oder ihre Begehung sehr unwahrscheinlich sein kann.

Vgl. BVerfGE 110, 33 (58 ff.).

§ 3 Abs. 1 Satz 1 G 10 enthält keine präzisierenden Tatbestandsmerkmale, um das potentiell fast uferlose Planungsstadium einzugrenzen.

Kritisch auch Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 3 G 10 Rn. 13.

Zweitens ermöglicht § 3 Abs. 1 Satz 1 G 10 Telekommunikationsüberwachungen auch, um dem Verdacht der Planung oder Begehung minderschwerer Straftaten nachzugehen, die keine besonders bedeutsamen Rechtsgüter schädigen. Zu nennen sind mindestens das Verbreiten von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 3 G 10), die Zuwiderhandlung gegen ein Vereinsverbot (§ 20 Abs. 1 Nr. 1 bis 4 VereinsG, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 3 G 10) und die Zugehörigkeit zu einer geheim gehaltenen Vereinigung von Ausländern (§ 95 Abs. 1 Nr. 8 AufenthG, Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 7 G 10).

Drittens finden sich in dem Straftatkatalog des § 3 Abs. 1 Satz 1 G 10 neben Erfolgsdelikten auch Gefährdungstatbestände, die Handlungen im Vorfeld einer Rechtsgutsverletzung kriminalisieren. Teilweise verlagern diese Tatbestände die Strafbarkeit erheblich vor.

Beispielhaft sei auf § 129a StGB (Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 6 lit. a G 10) verwiesen, der bereits die Gründung oder Beteiligung an einer terroristischen Vereinigung bei Strafe verbietet, also eine Tathandlung weit im Vorfeld konkreter Schädigungshandlungen beschreibt. Sogar noch weiter von einer konkreten Schädigungshandlung entfernt ist die nach § 129a Abs. 5 strafbare Unterstützung entsprechender Vereinigungen, die ebenfalls eine taugliche Katalogtat darstellt. Eine sehr weitreichende Vorverlagerung der Strafbarkeit sieht auch etwa § 89a StGB vor (Katalogtat nach § 3 Abs. 1 Satz 1 Nr. 2 G 10). Diese Norm stellt die Vorbereitung eines terroristischen Anschlags bereits in einem sehr frühen Stadium unter Strafe, wenn noch kaum absehbar ist, ob der Täter sein Vorhaben letztlich in die Tat umsetzen können wird. Die Rechtsprechung begrenzt die sehr weit gefasste Norm vor allem, indem sie hohe Anforderungen an den subjektiven Tatbestand stellt.

Vgl. BGH NJW 2014, 3459 (3465 f. Rn. 45); BGH NJW 2016, 260 (Rn. 10).

Diese Begrenzung wirkt sich jedoch im präventiven behördlichen Handlungsfeld, dem § 3 Abs. 1 Satz 1 G 10 angehört, allenfalls schwach aus. Denn im Voraus lassen sich die genauen Absichten und die Motivation des Betroffenen kaum erschließen. Eine präventiv ausgerichtete Überwachung muss darum ganz überwiegend an äußerliche, klar erkennbare Tatsachen anknüpfen. Vorfeldtatbestände wie § 129a oder § 89a StGB, die auf der objektiven Seite sehr weit gefasst sind, bieten deshalb kaum Anknüpfungspunkte, um die von § 3 Abs. 1 Satz 1 G 10 geforderte Prognoseentscheidung normativ anzuleiten. Diese Entscheidung kann vielmehr in weitem Umfang an hoch ambivalente und vage Erkenntnisse anknüpfen.

In diesem Sinne hat das angerufene Gericht jüngst ausgeführt, dass ein Verweis auf Straftaten, die Vorbereitungshandlungen oder andere Gefährdungen im Vorfeld erfassen, dem Erfordernis einer konkreten Gefahrenlage nicht genügt.

BVerfG NJW 2020, 2235 (2255 f. Rn. 211 ff., 221).

Ungeachtet der Einstufung der von § 3 Abs. 1 Satz 1 G 10 in Bezug genommenen Vorfeldtatbestände als Erscheinungsformen der Schwerkriminalität, die sich im gesetzlichen Strafrahmen zeigt, sind diese Straftatbestände daher nicht geeignet, den Anlass präventiv ausgerichteter Eingriffsmaßnahmen trennscharf zu beschreiben.

Die Defizite des gesetzlichen Übermittlungsanlasses verschärfen sich, wenn sie miteinander verbunden werden. § 3 Abs. 1 Satz 1 G 10 ermöglicht eine Überwachung auch, wenn der Verdacht besteht, dass jemand eine Vorfeldstraftat plant. Materiell-strafrechtliche und prozedural-nachrichtendienstrechtliche Vorverlagerung verstärken dann einander, so dass sich der Übermittlungstatbestand nahezu vollständig auflöst und Überwachungen weitgehend nach Belieben ermöglicht.

Dies lässt sich an einem Beispiel illustrieren: Nach § 89a Abs. 1, Abs. 2 Nr. 3 StGB macht sich unter anderem strafbar, wer sich Stoffe beschafft, um daraus Mittel für einen terroristischen Anschlag herzustellen. Erfasst sind insbesondere auch vielfältig nutzbare Stoffe, deren deliktischer Bezug sich erst aus den Vorstellungen des Handelnden ergibt. Den Straftatbestand erfüllt beispielsweise der Kauf von Unkrautvernichtungsmittel mit dem Ziel, daraus Sprengstoff herzustellen. In der Folge kann das LfV gemäß § 3 Abs. 1 Satz 1 Nr. 2 G 10 die Telekommunikation einer Person bereits überwachen, wenn der Verdacht besteht, dass diese Person plant, mit entsprechendem Vorbereitungsvorsatz Unkrautvernichtungsmittel zu kaufen. Auf welcher Grundlage ein solcher Verdacht fußen könnte, bleibt offen. Fast zwangsläufig wird es sich

hierbei vor allem um vage und wenig aussagekräftige Faktoren wie die persönlichen Überzeugungen und sozialen Beziehungen des Betroffenen handeln, die für eine verfassungsrechtlich tragfähige Schadensprognose jedoch nicht ausreichen.

BVerfGE 141, 220 (273).

Auch § 3 Abs. 1 Satz 2 G 10 ermöglicht eine Telekommunikationsüberwachung bereits weit im Vorfeld konkreter Gefahren. Der Verdacht der Mitgliedschaft in einer Vereinigung kann bereits bestehen, wenn die genauen Ziele und das Gefährdungspotential der Vereinigung noch weitgehend unbekannt sind. Bedeutsam ist hierbei auch, dass die Regelung bereits einen strafrechtlich relevanten Zweck der Vereinigung ausreichen lässt. Anhaltspunkte für bereits begangene Straftaten sind danach nicht erforderlich. Schließlich schränkt der in § 3 Abs. 1 Satz 2 G 10 enthaltene Eingriffstatbestand den Kreis der Straftaten nicht ein, auf welche die Zwecke oder die Tätigkeit der mutmaßlichen Vereinigung gerichtet sein müssen. Eine Überwachung könnte daher auch an den Verdacht der Mitgliedschaft in einer Vereinigung anknüpfen, von der lediglich minder schwere Straftaten wie Beleidigungen oder einfache Sachbeschädigungen erwartet werden, wenn diesen Straftaten eine verfassungsfeindliche Motivation zugrunde liegt. Eine Gefahr für besonders bedeutsame Rechtsgüter geht von einer solchen Vereinigung nicht aus.

(3) „Kleine Online-Durchsuchung“

§ 8 Abs. 12 Satz 2 HmbVerfSchG erlaubt die Überwachung und Aufzeichnung bereits auf einem IT-System gespeicherter Inhalte und Umstände der Kommunikation. Da die Regelung sich nicht auf laufende Kommunikationsvorgänge bezieht, ist sie nicht an Art. 10 Abs. 1 GG, sondern an dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu messen.

Vgl. BVerfGE 120, 274 (308).

Die Ausführungen in der Gesetzesbegründung dazu, dass lediglich der Maßstab des Fernmeldegeheimnisses gelte, überzeugen nicht. Die Begründung verweist darauf, dass „die Gefahr des Auslesens des gesamten Systems oder auch nur der gesamten gespeicherten Kommunikation nicht“ bestünde, wenn die Überwachung auch technisch „auf neu ankommende oder abgesendete Messenger-Nachrichten auf dem Endgerät begrenzt“ werde.

Hamburgische Bürgerschaft Drs. 21/18578, S. 43.

§ 8 Abs. 12 Satz 2 HmbVerfSchG bedeutet aber gerade keine Begrenzung auf eingehende oder abgesetzte Kommunikation, sondern eine Erweiterung der Überwachungsbefugnis auf hypothetische Fälle, in denen Kommunikation auch bei Eingang oder Absetzen hätte überwacht werden können. Dies überdehnt die Grenzen der Figur der Quellen-TKÜ. Dass eine Überwachung laufender Kommunikation durch eine Überwachung an der Quelle nach Art. 10 GG zu messen ist, stellt bereits eine Ausnahme von der Regel dar, dass Trojaner-Einsätze einen Eingriff in das IT-Grundrecht darstellen. Dazu kommt, dass es nicht nachvollziehbar ist, wie § 8 Abs. 12 Satz 2 HmbVerfSchG es gleichzeitig erlauben soll „auf dem informationstechnischen System gespeicherte Inhalte und Umstände der Kommunikation“ zu überwachen und technisch auf laufende Kommunikation beschränkt zu werden. Dies erscheint als unauflösbarer Widerspruch.

Hinzu kommt noch, dass es technisch notwendig wäre, zunächst sämtliche auf einem Gerät gespeicherten Kommunikationsinhalte auszulesen, um überhaupt festzustellen, welche Inhalte nach dem Beginn der Überwachung gespeichert wurden. Diese logisch erforderliche Vor-Auswertung würde als eine Form der „Online-Durchsuchung“ aber bereits einen rechtfertigungsbedürftigen Eingriff in das IT-Grundrecht bedeuten, der von § 8 Abs. 12 Satz 2 HmbVerfSchG nicht abgedeckt ist.

Im Ergebnis ist damit der Maßstab des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auf § 8 Abs. 12 Satz 2 HmbVerfSchG anzuwenden. Diesem Maßstab genügt die angegriffene Regelung nicht. So beschränkt § 8 Abs. 12 Satz 2 HmbVerfSchG die Möglichkeit der „kleinen Online-Durchsuchung“ nicht – wie verfassungsrechtlich notwendig –

BVerfGE 120, 274 (328).

auf Fälle, in denen tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Die Befugnis ermöglicht „kleine Online-Durchsuchungen“ unter Verweis auf die Voraussetzungen von § 3 G 10 – wie bereits ausgeführt – vielmehr auch, um dem Verdacht der Planung oder Begehung minderschwerer Straftaten nachzugehen, die keine besonders bedeutsamen Rechtsgüter schädigen

c) Transparenz und Kontrolle

Aus dem Grundsatz der Verhältnismäßigkeit folgen auch Anforderungen an die Transparenz und Kontrolle von Überwachungsmaßnahmen, die § 8 Abs. 12 HmbVerfSchG verfehlt.

(1) Transparenzschaffende Regelungen

Ermächtigungen zu eingriffsintensiven verdeckten Überwachungsmaßnahmen müssen durch transparenzschaffende Regelungen flankiert werden, um dem Betroffenen eine Orientierung über ihn betreffende Eingriffsmaßnahmen sowie einen effektiven Rechtsschutz zu ermöglichen.

Der Gesetzgeber muss nach der Rechtsprechung des angerufenen Gerichts Ermächtigungen zu eingriffsintensiven verdeckten Überwachungsmaßnahmen unter anderem durch Benachrichtigungspflichten flankieren. Das Gesetz kann Ausnahmen von der Benachrichtigungspflicht vorsehen, um bedeutsame Allgemeininteressen oder Rechtsgüter Dritter zu schützen. Solche Ausnahmen sind jedoch auf das unbedingt Erforderliche zu beschränken und müssen dem Gebot der Normenklarheit und Bestimmtheit genügen.

BVerfGE 141, 220 (282 f.); BVerfG NJW 2020, 2235 (2262 Rn. 267).

§ 8 Abs. 12 HmbVerfSchG verfehlt diese Anforderungen. § 8 Abs. 12 Satz 8 HmbVerfSchG verweist auf die Benachrichtigungsregelung des § 12 Abs. 1 G 10. Diese Regelung enthält jedoch viel zu weit gefasste Ausschlusstatbestände und verfehlt daher die verfassungsrechtlichen Anforderungen.

Bereits sehr weit geht der Ausnahmetatbestand in § 12 Abs. 1 Satz 2 Alt. 1 G 10, nach dem die Benachrichtigung unterbleibt, solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann. Zwar ist die Sicherung des Überwachungszwecks grundsätzlich ein verfassungsrechtlich tragfähiger Grund, die Benachrichtigung zurückzustellen.

BVerfGE 129, 208 (254); BVerfGE 141, 220 (283).

Indem jedoch § 12 Abs. 1 Satz 2 Alt. 1 G 10 die Benachrichtigung generell sperrt, solange eine Gefährdung des Überwachungszwecks lediglich nicht auszuschließen ist, lässt die Norm ihrem Wortlaut nach bereits entfernte Risiken ausreichen, damit der

Ausnahmetatbestand greift. Angesichts des weit gefassten Aufklärungsauftrags der Verfassungsschutzbehörden wird sich kaum je mit Sicherheit ausschließen lassen, dass eine Benachrichtigung solche Risiken birgt. § 12 Abs. 1 Satz 2 Alt. 1 G 10 beschränkt die Benachrichtigungspflicht daher unverhältnismäßig stark. Zumindest bedarf die Norm einer verfassungskonformen Auslegung, nach der die Benachrichtigung nur ausgeschlossen ist, wenn konkrete Tatsachen für eine Gefährdung des Überwachungszwecks sprechen.

> Vgl. die einschränkende Auslegung des (deutlich restriktiver gefassten) Ausnahmetatbestands in § 20w Abs. 2 Satz 1 Hs. 2 BKAG durch BVerfGE 141, 220 (320); ferner zu der Vorgängerregelung des heutigen § 12 G 10 BVerfGE 100, 313 (397 f.).

Unverhältnismäßig und auch keiner verfassungskonformen Auslegung zugänglich ist § 12 Abs. 1 Satz 2 Alt. 2 G 10, der die Benachrichtigung ausschließt, solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist.

Sowohl der Begriff des Bundes- oder Landeswohls als auch der Begriff der übergreifenden Nachteile sind weitgehend unbestimmt und grenzen den Grund für eine Zurückstellung der Benachrichtigung praktisch nicht ein. Letztlich lässt sich unter das Wohl des Bundes oder eines Landes – anders als unter den etwa in § 20w Abs. 2 Satz 1 BKAG genannten Bestand des Staates – der gesamte Aufgabenkreis des LfV oder auch jeder anderen Behörde subsumieren.

Zudem müssen die befürchteten Nachteile nach dem Wortlaut von § 12 Abs. 1 Satz 2 Alt. 2 G 10 in keinem Zusammenhang mit dem Überwachungszweck stehen, so dass der Ausnahmetatbestand auch hierdurch nicht konkretisiert wird.

Für die Zurückstellung und – auf der Grundlage von § 12 Abs. 1 Satz 5 G 10 – den endgültigen Ausschluss der Benachrichtigung reichen damit annähernd beliebige behördliche Opportunitätserwägungen aus, solange diese aufgrund einer normativ nicht angeleiteten Abwägung wichtiger erscheinen als die Benachrichtigung.

Für die Verfassungsmäßigkeit von § 12 Abs. 1 Satz 2 Alt. 2 G 10 lässt sich nicht anführen, dass dieser Ausschlusstatbestand weitgehend wörtlich dem Urteil des angerufenen Gerichts zur strategischen Telekommunikationsüberwachung nach dem G 10 vom 14. Juli 1999 entnommen ist.

Vgl. BVerfGE 100, 313 (398).

Das Bundesverfassungsgericht ist keine Rechtsetzungsinstanz, sondern dazu berufen, grundrechtliche Grenzen der Rechtsetzung zu bestimmen. Es kann sinnvoll oder sogar angezeigt sein, im Rahmen verfassungsgerichtlicher Entscheidungen allgemeine, nicht notwendigerweise unmittelbar subsumtionsfähige Formulierungen zu wählen, um so gesetzgeberische Regelungsspielräume offenzuhalten. Hingegen besteht die Aufgabe des Gesetzgebers darin, diese Regelungsspielräume durch einfaches Recht auszufüllen und so die Verfassung zu konkretisieren. Er kann sich dieser Aufgabe zumindest nicht in jedem Fall dadurch entziehen, dass er Formulierungen aus der Rechtsprechung des Bundesverfassungsgerichts schlicht abschreibt.

Insbesondere wäre es sowohl möglich als auch geboten gewesen, den Ausnahmetatbestand zum Schutz des Staatswohls näher zu spezifizieren und auf hinreichend gewichtige Ausnahmegründe zu beschränken. Hierbei hätten auch spezifisch nachrichtendienstliche Belange wie etwa der Quellenschutz oder die Erhaltung von Austauschbeziehungen mit ausländischen Diensten benannt werden können, soweit diese eine Ausnahme von der Benachrichtigungspflicht rechtfertigen können.

(2) Kontrolle

§ 8 Abs. 12 HmbVerfSchG erweist sich weiter als unverhältnismäßig, weil es an einem ausreichenden objektiv-rechtlichen Kontrollregime für die Quellen-TKÜ fehlt. Nach § 8 Abs. 12 Satz 8 HmbVerfSchG ist hierfür das Anordnungsverfahren nach §§ 9 ff. G 10 durchzuführen. Aufgrund der hohen Eingriffsintensität der Quellen-TKÜ verbunden mit ihrer Intransparenz ist hierfür allerdings eine kontinuierliche gerichtsähnliche Rechtskontrolle notwendig.

Entsprechendes hat das angerufene Gericht jüngst für die Auslandsfernmeldeaufklärung aufgrund ihrer Intransparenz und der Schwäche der individuellen Rechtsschutzmöglichkeiten diesbezüglich verlangt.

BVerfG NJW 2020, 2235 (2263 Rn. 272 ff.).

Zwar ist bei der Quellen-TKÜ durch das LfV der Rechtsschutz nicht automatisch durch einen Auslandsbezug erschwert. Allerdings ist die Quellen-TKÜ von einer ähnlichen Intransparenz geprägt und greift noch intensiver in die Grundrechte der Betroffenen ein als die strategische Auslandsaufklärung. Es handelt sich um eine heimliche Über-

wachung von Telekommunikation, die sich im Gegensatz zur strategischen Aufklärung zielgenau auf ein Individuum richtet und die von ihm ausgehende Kommunikation über ein Endgerät vollständig erfassen kann. Wenn aber das angerufene Gericht es für verfassungsrechtlich geboten hält, dass die zielgenaue Überwachung eines Ausländers im Ausland, der als möglicher Verursacher von Gefahren interessant ist, einer „gerichtsähnlichen ex ante-Kontrolle“ bedarf,

BVerfG NJW 2020, 2235 (2253 Rn. 188),

so muss dies erst recht für eine gegen Inländer gerichtete heimliche Überwachungsmaßnahme gelten, die den Betroffenen zudem stärker belastet.

Aufgrund sozio-technischer Entwicklungen ist dabei auch die Bedeutung der ausgehenden Kommunikation von besonders mobilen Endgeräten in den letzten Jahren noch einmal deutlich gestiegen. Eine Quellen-TKÜ durch das LfV kann auch eher zu operativen Konsequenzen führen als eine strategische Auslandsüberwachung.

Vgl. zu dem im Vergleich geringeren Eingriffsgewicht strategischer Auslandsüberwachung BVerfG NJW 2020, 2235 (2248 Rn. 146 ff.).

Darauf hinzuweisen ist in diesem Zusammenhang auch, dass die Parallelbefugnis des Bundeskriminalamts nach § 51 Abs. 2 BKAG selbstverständlich eine gerichtliche Anordnung der Quellen-TKÜ verlangt (§ 51 Abs. 3 Satz 1 BKAG). Dies insbesondere auch für den Fall ihrer Anordnung im Vorfeld einer konkreten Gefahr (§ 51 Abs. 1 Satz 1 Nr. 2 und 3 BKAG). Im Gefahrenvorfeld unterscheidet sich die Aufklärungsarbeit des Bundeskriminalamts aber kaum von der nachrichtendienstlichen Tätigkeit. Würde nur in einem Fall eine gerichtliche Anordnung für notwendig gehalten, bedeutete das einen nicht auflösbaren Wertungswiderspruch. Soweit die Tätigkeit der Nachrichtendienste einer höheren Geheimhaltung bedürfte, lässt sich dem auf eine Weise begegnen, wie sie das angerufene Gericht auch für die Fernmeldeaufklärung des Bundesnachrichtendienstes entwickelt hat.

BVerfG NJW 2020, 2235 (2263 Rn. 272 ff.).

Insofern ist auch für die Quellen-TKÜ durch das LfV zumindest eine gerichtsähnliche Ex-ante-Kontrolle zu fordern, um die Defizite der individuellen Möglichkeiten der Kenntnisnahme und des Rechtsschutzes auszugleichen. Eine solche wird aufgrund der geringen Zahl der aufwändigen Überwachungsmaßnahmen nach § 8 Abs. 12

HmbVerfSchG und in Anbetracht des ohnehin bereits erforderlichen Anordnungsverfahren nach §§ 8 f. G 10 auch nicht zu einem Effektivitätsverlust dieser führen.

II. Hinsichtlich § 49 HmbPolDVG

Auch § 49 HmbPolDVG ist verfassungswidrig. Die Eingriffsschwellen der Befugnis sind zu weit gefasst. Die zugehörigen Verfahrensregelungen verfehlen in weitem Umfang die verfassungsrechtlichen Anforderungen.

1. Verfassungsrechtliche Maßstäbe

Die verfassungsrechtlichen Grenzen der automatisierten Datenanalyse mit Hilfe komplexer informationstechnischer Programme wurden in der Rechtsprechung des angerufenen Gerichts bislang nicht abschließend geklärt. Als Maßstab für die komplexe Datenauswertung unzureichend ist der Grundsatz der hypothetischen Datenneuerhebung (a). Die Maßstäbe zur Rasterfahndung sind nicht vollends auf die neuartige Datenauswertung übertragbar, sie dürfen aber jedenfalls nicht unterschritten werden (b).

a) Unzulänglichkeit der hypothetischen Datenneuerhebung

Das angerufene Gericht hat in seinem Urteil zum BKA-Gesetz zwischen zwei Weiterverarbeitungskonstellationen unterschieden, für die es unterschiedlich strenge verfassungsrechtliche Maßstäbe entwickelt hat. Eine Weiterverarbeitung erhobener Daten in einem Verfahren derselben Behörde im Rahmen derselben Aufgabe zum Schutz gleichwertiger Rechtsgüter wie im Ausgangsverfahren hält sich als weitere Nutzung im Rahmen der verfassungsrechtlichen Zweckbindung der Daten. Der Gesetzgeber darf eine solche weitere Nutzung unabhängig von weiteren gesetzlichen Voraussetzungen als bloßen Spurenansatz zulassen, der den Ausgangspunkt weiterer Ermittlungen bildet.

Vgl. BVerfGE 141, 220 (325 f.).

Hingegen ist eine Weiterverarbeitung durch eine andere Behörde oder durch dieselbe Behörde im Rahmen einer anderen Aufgabe als Zweckänderung besonders rechtfertigungsbedürftig. Der Gesetzgeber darf die zweckändernde Weiterverarbeitung nach dem Kriterium einer hypothetischen Datenneuerhebung zulassen, wenn der neue Ver-

arbeitungszweck dem Erhebungszweck gleichwertig ist. In tatsächlicher Hinsicht setzt die Zweckänderung einen konkreten Ermittlungsansatz voraus.

Vgl. BVerfGE 141, 220 (327 ff.).

Diese verfassungsrechtlichen Maßstäbe sind nicht ohne weiteres auf die spätere Analyse dieser Daten mit Hilfe einer komplexen Analysesoftware übertragbar. Die automatisierte Datenanalyse stellt keinen einfachen Fall der weiteren Nutzung dar, der lediglich den Anforderungen der Zweckbindung unterliegt.

Die Feststellungen des angerufenen Gerichts im Urteil zum BKA-Gesetz hatten nicht die Generierung von Spurenansätzen mit Hilfe komplexer automatisierter Datenanalyseprogramme zum Gegenstand. Diese Art der Datennutzung unterscheidet sich auch in wesentlichen Punkten von einer einfachen Weiternutzung.

Die herkömmliche Weiternutzung, bei der einmal erhobene Daten in einem zeitlichen Zusammenhang mit dem Erhebungsanlass, beispielsweise aufgrund eines Zufallsfundes, für neue Ermittlungen weitergenutzt werden, hat eine ganz andere Qualität als der automatisierte Zugriff auf alle verfügbaren Datenbestände. Bei Letzterem werden diese Daten gemeinsam in einem umfassenden Datenpool gespeichert und einer automatisierten Analyse unterzogen, um Ermittlungsansätze zu generieren. Im Unterschied zur herkömmlichen Weiternutzung erhobener Daten ermöglicht die Datenverknüpfung unter Einsatz komplexer Analyseprogramme die Erzeugung umfassender Sozialprofile verdächtiger Milieus und weitreichender Persönlichkeitsprofile von Einzelpersonen. Diese Art der Weiternutzung kann durch die ursprüngliche Datenerhebung nicht ohne Weiteres legitimiert und in ihren Voraussetzungen auch nicht an diese angelehnt werden.

b) Maßstäbe der Rasterfahndung und Eingriffsintensität

Vor diesem Hintergrund ist die automatisierte Datenanalyse vielmehr mindestens an den im Urteil des angerufenen Gerichts entwickelten Maßstäben für die Rasterfahndung zu messen. Zwar ist die komplexe Datenauswertung aus § 49 Abs. 1 HmbPolDVG nicht direkt mit der Rasterfahndung vergleichbar. Sie erweist sich aber im Ergebnis als noch eingriffsintensiver. Sie stellt einen äußerst schwerwiegenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Beschwerdeführer*innen zu 1 bis 6 dar. Soweit personenbezogene Daten aus der Wohnraum- oder

Telekommunikationsüberwachung in die Analyse einfließen, sind auch das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG und das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG betroffen.

Für die Rasterfahndung ist charakteristisch, dass aus mehreren außerpolizeilichen Datenbeständen erhobene Daten miteinander oder mit polizeilichen Datenbeständen abgeglichen werden, um aus einer Fahndungshypothese ein Persönlichkeitsprofil zu erstellen und anhand dessen eine oder mehrere gesuchte Personen zu ermitteln. § 49 Abs. 1 HmbPolDVG geht es um komplexe Verknüpfungen zwischen in polizeilichen Dateisystemen gespeicherten Daten.

(1) Menge und Vielfalt einbezogener Daten

Den Grundrechtseingriff, der durch die Rasterfahndung erfolgt, hat das angerufene Gericht unter anderem aufgrund der Menge und Vielfalt der in den Abgleich einbezogenen personenbezogenen Daten als besonders intensiv bewertet. Diese würden mit Hilfe von Informationstechnologie gegeneinander abgeglichen und dadurch in der Verarbeitung und Verknüpfung einen neuen Stellenwert bekommen.

Vgl. BVerfGE 115, 320 (350).

Die Einschränkung auf Daten aus polizeilichen Dateisystemen lässt § 49 Abs. 1 HmbPolDVG hinsichtlich der Menge der einbezogenen Daten zunächst enger wirken als Befugnisse zur Rasterfahndung. Allerdings bestehen weitgehende Möglichkeiten der Polizei, Daten zunächst aus verschiedenen Quellen zu erheben und in Dateisystemen zu speichern, um sie im nächsten Schritt auszuwerten. Dies betrifft private und behördliche Datenbestände ebenso wie Daten aus öffentlichen Quellen. Im Unterschied zu den Befugnissen zur Rasterfahndung (vgl. § 50 HmbPolDVG) ergibt sich die Möglichkeit zur Erhebung der Daten dabei aus den allgemeinen Regelungen (§§ 10 ff. HmbPolDVG) und nicht aus § 49 HmbPolDVG selbst.

Potentiell können in die automatische Datenanalyse alle Daten einfließen, die die Polizei legal erheben oder sich von anderen öffentlichen Stellen oder privaten Unternehmen übermitteln lassen und dann in ihren Systemen speichern kann. Nach §§ 10 ff. HmbPolDVG hat die Polizei Hamburg weitreichende Datenerhebungsbefugnisse und kann sich im Rahmen ihrer Aufgaben Daten von öffentlichen und privaten Stellen übermitteln lassen. Beispielsweise kann sich die Polizei nach §§ 10, 11 HmbPolDVG Daten

zur Zielperson vom LfV, der Ausländerbehörde, der Meldebehörde, den Sozialämtern und weiteren öffentlichen Stellen übermitteln lassen, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. Von privaten Stellen wie Banken, Verkehrsunternehmen oder Telekommunikationsanbietern kann sich die Polizei Kreditkarteninformationen, Reiserouten oder Verkehrs- und Verbindungsdaten übermitteln lassen. Daten aus allgemein zugänglichen Quellen wie den sozialen Netzwerken Facebook und Twitter darf die Polizei nach § 11 Abs. 1 Nr. 2 HmbPolDVG erheben.

Auf eine Kleine Anfrage hat die Hamburgische Bürgerschaft zuletzt für die Anwendung von § 49 HmbPolDVG keine der genannten Datenquellen ausgeschlossen.

> Hamburgische Bürgerschaft Drs. 22/1758.

(2) Einbezogener Personenkreis

Im Zusammenhang mit der Rasterfahndung wertete das angerufene Gericht weiter die große Menge der betroffenen Menschen, die für den Eingriff keinen Anlass gegeben haben, als eingriffsintensivierend.

> Vgl. BVerfGE 115, 320 (354 ff.).

Maßnahmen, bei denen zahlreiche Personen in den Wirkungsbereich einbezogen werden, die den Eingriff durch ihr Verhalten nicht veranlasst haben, sind grundsätzlich von hoher Eingriffsintensität.

> Vgl. BVerfGE 100, 313 (376, 392); BVerfGE 120, 378 (402); BVerfG NJW 2019, 827 (834 Rn. 98).

Wie bei der Rasterfahndung, die über die unmittelbaren Zielpersonen hinaus eine fast unbegrenzte Zahl unbeteiligter Personen treffen kann, begründet auch die Anwendung zur automatisierten Datenanalyse Eingriffsbefugnisse gegenüber Nichtstörern und ermöglicht es anhand der Daten einen Verdacht zu generieren. Die Datenauswertung nach § 49 Abs. 1 HmbPolDVG hat eine große Streubreite und kann über die Verknüpfung von Ereignissen, Orten, Objekten und Menschen auch Bürger*innen, die keinen Anlass hierzu gegeben haben, als „Beifang“ erfassen.

Das aus § 49 Abs. 2 HmbPolDVG ablesbare Ziel der neuen Befugnis, zur vorbeugenden Bekämpfung von Straftaten Beziehungen oder Zusammenhänge zwischen Personen herzustellen, legt es gerade nahe, dass Personen mit in die Maßnahme einbe-

zogen werden, die hierfür keinen eigenen Anlass gegeben haben, aber nach Datenlage in einer Beziehung zu relevanten Personen stehen.

Mithin kann die Analyse auch Daten von Menschen aus dem Umfeld der Zielperson und darüber hinaus auch von vollkommen unbeteiligten Menschen einbeziehen, die beispielsweise mit einem Ort oder einem Ereignis in Verbindung stehen. Diese Form der Analyse kann buchstäblich jeden treffen, bei Berücksichtigung von Melderegistern oder Fahrzeughalterdaten auch Menschen, die noch nie anlassbezogen polizeilich erfasst wurden.

Zwar kann ein Eingriff in das informationelle Selbstbestimmungsrecht der miterfassten Personen ausgeschlossen sein, sofern Daten ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden ausgesondert werden.

BVerfGE 115, 320 (343).

Dies gilt aber nicht, wenn die Datenerfassung eines größeren Datenbestands letztlich nur der Verkleinerung der Treffermenge dient und sich bereits ein behördliches Interesse an den betroffenen Daten verdichtet hat.

BVerfG NJW 2019, 827 (829 Rn. 43, 48)

Dies ist bei Ausübung der Befugnis nach § 49 HmbPolDVG der Fall. Hier ist davon auszugehen, dass Daten aufgrund zuvor ausgewählter Kriterien und nicht rein zufällig miterfasst werden. Nach der erstmaligen automatisierten Erfassung wird es erst nach näherer Betrachtung möglich sein, die Relevanz im engeren Sinne von miterfassten Daten zu beurteilen. Zu diesem Zeitpunkt hat sich das polizeiliche Interesse hieran bereits verdichtet.

In manchen Fällen können durch die Analysesoftware generierte Verdachtsmomente gegenüber Drittbetroffenen vermutlich erst durch weitere, datenintensive Analysen oder gar durch weitere Folgemaßnahmen wie Telekommunikationsüberwachung oder Observation ausgeräumt werden.

(3) Besondere Persönlichkeitsrelevanz der Daten

Das Gewicht des Eingriffs durch die Auswertung verstärkt sich, wenn die einbezogenen Daten eine besondere Persönlichkeitsrelevanz aufweisen, für sich und in Verknüp-

fung mit anderen Daten. Besonders hoch ist die Eingriffsintensität, „wenn Informationen betroffen sind, bei deren Erlangung Vertraulichkeitserwartungen verletzt werden, vor allem solche, die unter besonderem Grundrechtsschutz stehen, wie etwa bei Eingriffen in das Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 GG oder das Fernmeldegeheimnis nach Art. 10 GG“.

BVerfGE 115, 320 (348).

In den Polizeidatenbanken, die in Analysen nach § 49 HmbPolDVG einfließen, können sich besonders persönlichkeitsrelevante Daten befinden. Dies betrifft etwa Informationen über politische Meinungen oder religiöse Überzeugungen, die sich in den Datenbeständen befinden können. Dazu ist es möglich, dass die Polizei (Meta-) Daten aus Maßnahmen wie der Wohnraumüberwachung und der Telekommunikationsüberwachung in Dateien speichert und in die Analyse mit einbezieht.

(4) Komplexität der Verarbeitung

Eine neue Qualität und erhöhte Eingriffsintensität der Rasterfahndung sah das Gericht des Weiteren in der Nutzung automatisierter, rechnergestützter Operationen zur Verarbeitung nahezu beliebig großer und komplexer Informationsbestände in großer Schnelligkeit, wodurch Ermittlungstätigkeiten mit einer bislang unbekannten Durchschlagskraft versehen würden.

BVerfGE 115, 320 (356 f.).

Durch die komplexen softwarebasierten Verarbeitungs- und Verknüpfungsmöglichkeiten gewinnen zuvor möglicherweise belanglose Informationen einen neuen Gehalt.

Vgl. BVerfGE 115, 320 (350).

Die Zuordnung des KfZ-Kennzeichens HH-QX 999 zu einer Person kann beispielsweise durch eine Verknüpfung mit der Information, dass eine Kontaktperson eines Drogenhändlers ein Fahrzeug, dessen Kennzeichen auf X 999 endet, im Rahmen einer komplexen Auswertung eine völlig neue und für den Betroffenen belastende Bedeutung gewinnen.

Hinsichtlich der ermöglichten Komplexität der Datenverarbeitung geht § 49 Abs. 1 HmbPolDVG deutlich weiter und ist damit eingriffsintensiver als die Befugnisse zur Rasterfahndung. Dies ist nicht nur den technischen Entwicklungen geschuldet, die

mittlerweile eine „intelligente“ Auswertung von Datensystemen mittels lernfähiger Systeme bzw. Algorithmen ermöglichen. Die Befugnis geht auch vom Wortlaut her weiter als jene zur Rasterfahndung, da sie die Verarbeitung mittels automatisierter Anwendungen zur Datenauswertung und nicht einen bloßen Abgleich gestattet. Der Abgleich ist als suchender Vergleich von Daten zu verstehen, um Übereinstimmungen festzustellen.

> Bäuerle, in: BeckOK Polizei- und Ordnungsrecht Hessen, Bearbeitungsstand 2020, § 25 Rn. 9 f.

Es handelt sich damit um einen vergleichsweise beschränkten Vorgang, von dem komplexere Verknüpfungen von Daten nicht gedeckt sind. Der Begriff der Auswertung geht hierbei weiter, was sich nicht nur aus dem Wortlaut, sondern auch aus einem systematischen Vergleich von § 49 mit § 48 HmbPolDVG ergibt, der für den einfachen Datenabgleich deutlich niedrigere Anforderungen festlegt.

Unter dem offenen Begriff der Auswertung erscheinen unter anderem komplexere suchende Vergleiche, die Herstellung von Verknüpfungen sowie die Erzeugung neuer Informationen denkbar. Dass im Gesetzgebungsverfahren der Begriff „Analyse“ in § 49 Abs. 1 HmbPolDVG durch den Begriff der „Auswertung“ ersetzt wurde, macht hierbei keinen Unterschied. Anders als in dem Gesetzgebungsverfahren vorgebracht, lässt sich der Begriff der Auswertung keinesfalls so verstehen, dass Datenverarbeitungen nicht automatisiert, sondern manuell vorgenommen werden. Der mit dem Begriff der Analyse weitgehend synonyme Begriff der Auswertung wird auch in anderen Regelungskontexten so verwendet, dass er den Einsatz komplexer automatisierter Anwendungen erfasst.

> Vgl. etwa § 21 Abs. 4 PolG Baden-Württemberg, § 60d Abs. 1 UrhG, § 15a AsylG.

(5) Gefahr der Profilbildung

Das angerufene Gericht beschrieb die Datenverarbeitung durch die Rasterfahndung zudem als Annäherung an die verfassungsrechtlich verbotene Erstellung umfassender Persönlichkeitsprofile.

> Vgl. BVerfGE 115, 320 (351).

Schon im Volkszählungsurteil ging das angerufene Gericht auf die Möglichkeiten der Datenverknüpfung ein und sah die Gefahr eines Persönlichkeitsabbilds, wenn neu erhobene Daten mit den bei den Verwaltungsbehörden vorhandenen Daten verknüpft werden oder Lebens- und Personaldaten in einem Datenverbund erschlossen werden.

> „Das Erhebungsprogramm vermag zwar einzelne Lebensbereiche, zum Beispiel den Wohnbereich des Bürgers, jedoch nicht dessen Persönlichkeit abzubilden. Etwas anderes würde nur gelten, soweit eine unbeschränkte Verknüpfung der erhobenen Daten mit den bei den Verwaltungsbehörden vorhandenen, zum Teil sehr sensitiven Datenbeständen oder gar die Erschließung eines derartigen Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal möglich wäre“ BVerfGE 65, 1 (53).

Auch in jüngeren Jahren hat das angerufene Gericht bestätigt, dass es mit der Menschenwürde unvereinbar ist, „wenn eine hoheitliche Überwachung sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können“.

> BVerfGE 141, 220 (280).

Im Urteil zur Rasterfahndung etabliert das angerufene Gericht dementsprechend für Eingriffe, die der Erstellung umfassender Persönlichkeitsbilder nahekommen, hohe Eingriffsschwellen. Ein solcher Eingriff ist danach nur dann angemessen, wenn er an eine hinreichend konkrete Gefahr für hochrangige Verfassungsgüter anknüpft.

> Vgl. BVerfGE 115, 320 (362).

Die Gefahr der Profilbildung geht aus § 49 HmbPolDVG noch deutlicher hervor als aus den Befugnissen zur Rasterfahndung. Dafür spricht der im Vergleich zum Begriff des Abgleichs weitere Begriff der Auswertung. Auch das Ziel, Beziehungen oder Zusammenhänge zwischen Personen herzustellen, geht noch weiter als das Ziel der Rasterfahndung, potentielle Straftäter zu identifizieren, und ermöglicht weitergehende Profilbildungen.

Die Verknüpfung polizeilicher Datenbanken, die über die Erhebung und Speicherung von Informationen aus sozialen Medien und anderen öffentlichen und nicht-öffentlichen Quellen angereichert werden können, ermöglicht einen weitreichenden Einblick in das Leben, die Beziehungen und Netzwerke betroffener Personen. Je größer und

je leichter verknüpfbar die zugrundeliegenden Datenbestände sind, desto umfassender sind die Einblicke in die private Lebensführung der Betroffenen.

Dabei sind auch aktuelle Entwicklungen der polizeilichen (und allgemein sicherheitsbehördlichen) Informationsordnung zu betrachten, die die Verknüpfbarkeit vorhandener Datenbestände verbessern sollen. So soll im Rahmen des Programmes „Polizei 2020“ ein neues „gemeinsames Datenhaus der Polizei“ geschaffen werden, in dem Daten nicht mehr in getrennten Dateien, sondern thematisch geordnet werden. Zentrale Ziele der Umstellung sind die Verbesserung der Verfügbarkeit und Verknüpfbarkeit polizeilicher Informationen. Diese strukturelle Änderung der Informationsordnung soll auch die Landespolizeien erfassen.

Bundesministerium des Inneren, Polizei 2020 – White Paper, S. 8 ff.

Bei der Verknüpfung der Informationen zu Persönlichkeits- oder Sozialprofilen sind auch neue technologische Möglichkeiten, insbesondere der Einsatz lernfähiger Systeme, zu berücksichtigen, die in der Entscheidung des angerufenen Gerichts zur Rasterfahndung noch nicht vorhanden waren. § 49 HmbPolDVG ist so offen formuliert, dass jede der aufgeführten Auswertungsmöglichkeiten denkbar erscheint.

(6) Mögliche Folgemaßnahmen

Auf die Intensität des Eingriffs wirken sich zudem daraus resultierende mögliche Folgemaßnahmen aus. Im Rasterfahndungsurteil wies das angerufene Gericht auf das Risiko für Betroffene hin, Gegenstand weiterer staatlicher Ermittlungsmaßnahmen zu werden.

BVerfGE 115, 320 (351).

Ähnlich wie die Rasterfahndung begründet auch die automatisierte Anwendung zur Datenanalyse für betroffene Personen ein erhöhtes Risiko, Ziel weiterer behördlicher Ermittlungsmaßnahmen zu werden. Ergibt sich aus einer mit Hilfe der Datenanalyse generierten Hypothese ein Ermittlungsansatz, führt dies zu weiteren Ermittlungsmaßnahmen, sei es offenen Charakters wie Befragungen oder verdeckten Charakters wie Observationen oder Telekommunikationsüberwachung.

Die Einbeziehung in die Datenanalyse kann aus diesem Grund eine stigmatisierende Wirkung auf die Betroffenen haben. Dies gilt nicht nur, wenn dieser Umstand öffentlich

bekannt wird. Auch dass eine Person durch diese Einbeziehung stärker ins Visier von polizeilichen Ermittlungen gerät, kann ihre Identität im Sinne einer Stigmatisierung beschädigen, da sie sich in der Folge möglicherweise vermehrt Kontrollen und Folgeermittlungen ausgesetzt sieht.

(7) Zusammenhang mit der Erhebung

Die Intensität des Grundrechtseingriffs ist nicht dadurch gemindert, dass die Analyse auf Daten beruht, die zuvor auf Grundlage anderer Befugnisse erhoben wurden. Die Auswertung der Daten ist aufgrund des damit verbundenen Informationsgewinns ein eigener Grundrechtseingriff von erheblicher Qualität. Durch die komplexen Verarbeitungs- und Verknüpfungsmöglichkeiten, die moderne Software-Tools zur Datenanalyse bieten, gewinnen zuvor möglicherweise belanglose Informationen einen neuen Gehalt.

An § 49 HmbPolDVG und andere Befugnisse zur Auswertung von Daten sind im Gegenteil gerade deshalb hohe Anforderungen zu stellen, weil die Befugnisse zur Speicherung von Daten kaum wirksame Grenzen enthalten. Die Rechtsgrundlagen für die Speicherung und Auswertung von Informationen stehen in einem direkten Zusammenhang. Dürfen Daten unter geringen Voraussetzungen gespeichert werden, müssen riskante Formen ihrer Weiterverarbeitung umso genauer geregelt werden. Dass hohe Schwellen für den Zugang zu Daten und deren Auswertung in einem gewissen Maße fehlende Einschränkungen bei der Speicherung kompensieren können und müssen, hat auch das angerufene Gericht anerkannt.

BVerfGE 125, 260 (327 f.).

(8) Verdeckter Eingriff

Schließlich steigert der Umstand, dass die Datenanalysen verdeckt vorgenommen werden, die Intensität des Eingriffs, da die Möglichkeiten des Betroffenen, hiergegen Rechtsschutz zu erlangen, stark eingeschränkt sind.

Vgl. BVerfGE 124, 43 (62).

2. Grundrechtswidrigkeit

Gemessen an der Eingriffsintensität ist die Eingriffsermächtigung unverhältnismäßig, insbesondere ist sie hinsichtlich der Gefahrenschwelle und der geschützten Rechtsgüter zu weit (dazu unter a)). Dazu hat es der Gesetzgeber versäumt, hinsichtlich der einzusetzenden Überwachungsmittel eine eigeständige Abwägungsentscheidung zu treffen (dazu unter b)). Schließlich fehlt es an den erforderlichen Verfahrenssicherungen (dazu unter c)).

a) Eingriffsschwelle nicht hinreichend qualifiziert

Gemessen an der Intensität des Eingriffs genügt die Eingriffsermächtigung nicht dem Grundsatz der Verhältnismäßigkeit. Erstens fehlt es in Bezug auf die vorbeugende Straftatenbekämpfung in § 49 Abs. 1 HmbPolDVG an der erforderlichen konkreten Gefahr für gewichtige Rechtsgüter (1), zweitens ist das in § 49 Abs. 1 HmbPolDVG normierte Rechtsgut der Sachen von bedeutendem Wert zu unbestimmt (2).

(1) Fehlen einer konkreten Gefahr

Erforderlich ist eine konkrete Gefahr für hochrangige Rechtsgüter. Diesen Anforderungen genügt § 49 HmbPolDVG nicht, denn die vorbeugende Bekämpfung der in § 100a Abs. 2 StPO genannten Straftaten ermöglicht den Einsatz der automatisierten Datenanalyse weit im Vorfeld einer konkreten Gefahr und zum Schutz von Rechtsgütern geringen Gewichts. Besonders der unscharfe Begriff der vorbeugenden Bekämpfung von Straftaten gewährleistet nicht, dass die Datenübermittlung an eine konkrete Gefahr im verfassungsrechtlichen Sinne gebunden wird, wie dies geboten ist.

Der Grundsatz der Verhältnismäßigkeit führt dazu, dass der Gesetzgeber intensive Grundrechtseingriffe erst von bestimmten Verdachts- oder Gefahrenstufen an vorsehen darf.

> Vgl. BVerfGE 100, 313 (383 f.); BVerfGE 109, 279 (350 ff.).

Verzichtet der Gesetzgeber auf begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe der Betroffenen zur abzuwehrenden Bedrohung und sieht er gleichwohl eine Befugnis zu Eingriffen von erheblichem Gewicht vor, genügt dies dem Verfassungsrecht nicht.

BVerfGE 115, 320 (362).

Aufgrund des intensiven Persönlichkeitsbezugs und der hohen Streubreite des Grundrechtseingriffs verlangt das angerufene Gericht für die Rasterfahndung eine konkrete Gefahr für hochrangige Rechtsgüter.

Vgl. BVerfGE 115, 320 (362).

Auch die automatisierte Datenanalyse erfordert angesichts der hohen Eingriffsintensität mindestens eine konkrete Gefahr für hochrangige Rechtsgüter. Dem genügt die vorbeugende Straftatenbekämpfung von in § 100a Abs. 2 StPO genannten Straftaten nicht.

Erstens knüpft der Eingriffstatbestand nicht an die gegenwärtige Begehung einer Straftat an, die zumindest in der Regel auf eine Rechtsgutsgefahr schließen lässt. Vielmehr wird der äußerst unbestimmte Begriff der vorbeugenden Bekämpfung genutzt. Danach bedarf es keiner tatsächlichen Anhaltspunkte für die bevorstehende Begehung einer Straftat, sondern es reichen im Zweifel abstrakte Gefahrenlagen. Dieses Begriffsverständnis deckt sich mit weiten Teilen der Gesetzgebungspraxis, Rechtsprechung und Literatur zum Polizeirecht.

Vgl. nur Denninger, in: Lisken/ders., Handbuch des Polizeirechts, 6. Aufl. 2018, Rn. D 1 ff., m.w.N.

Auf welcher Grundlage der Einsatz der automatisierten Datenanalyse fußen könnte, bleibt offen. Fast zwangsläufig wird es sich hierbei vor allem um vage und wenig aussagekräftige Faktoren wie die persönlichen Überzeugungen und sozialen Beziehungen des Betroffenen handeln, die für eine verfassungsrechtlich tragfähige Schadensprognose jedoch nicht ausreichen,

> „Eine Anknüpfung der Einschreitschwelle an das Vorfeldstadium ist verfassungsrechtlich angesichts der Schwere des Eingriffs nicht hinnehmbar, wenn nur relativ diffuse Anhaltspunkte für mögliche Gefahren bestehen. Die Tatsachenlage ist dann häufig durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet. Die Geschehnisse können in harmlosen Zusammenhängen verbleiben, aber auch den Beginn eines Vorgangs bilden, der in eine Gefahr mündet.“ BVerfGE 141, 220 (273).

Zweitens enthält der Straftatkatalog des § 100a Abs. 2 StPO auch Straftaten, deren Schutzgüter keineswegs äquivalent zu den in § 49 HmbPolDVG genannten Schutzgü-

tern sind. Zu nennen sind mindestens das Verbreiten von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB), Geldfälschung (§ 146 Abs. 1 StGB), Vorteilsgewährung (§ 333 Abs. 1 StGB) und Verleitung zur missbräuchlichen Asylantragsstellung (§ 84 AsylG). § 100a StPO begrenzt den Anwendungsbereich der Telekommunikationsüberwachung über den Straftatenkatalog hinaus im Abs. 1 auf Straftaten, die auch im Einzelfall schwer wiegen. Durch den unmittelbaren Verweis des § 49 Abs. 1 HmbPolDVG auf den Straftatenkatalog des § 100a Abs. 2 StPO fehlt diese Begrenzung.

Drittens enthält § 100a Abs. 2 StPO strafrechtliche Vorfeldtatbestände, deren bevorstehende Verwirklichung nicht zwingend auf eine konkrete Gefahr für ein besonders bedeutsames Rechtsgut schließen lässt. Im Straftatenkatalog des § 100a StPO finden sich neben Erfolgsdelikten auch Gefährdungstatbestände, die Handlungen im Vorfeld einer Rechtsgutsverletzung kriminalisieren. Teilweise verlagern diese Tatbestände die Strafbarkeit erheblich vor. Beispielhaft sei auf § 129a StGB und § 89a StGB verwiesen.

Siehe dazu bereits oben I. 3. b) (2).

Die Rechtsprechung begrenzt etwa § 89a StGB vor allem, indem sie hohe Anforderungen an den subjektiven Tatbestand stellt. Diese Begrenzung wirkt sich jedoch im präventiven Handlungsfeld allenfalls schwach aus. Denn im Voraus lassen sich die genauen Absichten und die Motivation des Betroffenen kaum erschließen. Eine präventiv ausgerichtete Überwachung muss darum ganz überwiegend an äußerliche, klar erkennbare Tatsachen anknüpfen. Vorfeldtatbestände wie § 129a oder § 89a StGB, die auf der objektiven Seite sehr weit gefasst sind, bieten deshalb kaum Anknüpfungspunkte, um die von § 49 HmbPolDVG geforderte Prognoseentscheidung normativ anzuleiten. Diese Entscheidung kann vielmehr in weitem Umfang an hoch ambivalente und vage Erkenntnisse anknüpfen.

(2) Unbestimmte Rechtsgüter

Ein Eingriff der beschriebenen Intensität ist mit der Verfassung nur vereinbar, wenn er dem Schutz oder der Bewahrung von hinreichend gewichtigen Rechtsgütern dient, für deren Gefährdung oder Verletzung im Einzelfall belastbare tatsächliche Anhaltspunkte bestehen. Die Einbeziehung von Sachen von bedeutendem Wert, deren Erhaltung im

öffentlichen Interesse geboten ist, bedarf zumindest einer verfassungskonformen Auslegung.

Im Urteil zur Vorratsdatenspeicherung sowie im Urteil zur Rasterfahndung sah das angerufene Gericht den Abruf der betroffenen Daten nur zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes als zulässig an.

Vgl. BVerfGE 125, 260 (330); BVerfGE 115, 320 (357).

Für die Datenerhebung im Wege verdeckter Überwachungsmaßnahmen hat das angerufene Gericht „[e]inen uneingeschränkten Sachwertschutz“ insoweit „nicht als ausreichend gewichtig [...] angesehen“.

BVerfGE 141, 220 (270).

Das angerufene Gericht hat daher festgehalten, dass mit Blick auf den Einsatz besonderer Mittel der Datenerhebung nach § 20g Abs. 1 BKAG a.F. das dortige Merkmal des Schutzes von „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist“ bei „verständiger Auslegung“ eng zu verstehen sei und – (nur) so verstanden – die Überwachungsmaßnahmen auf den Schutz hinreichend gewichtiger Rechtsgüter begrenze:

> „Bei verständiger Auslegung kann hierunter nicht schon allein der Schutz von bedeutsamen Sachwerten verstanden werden. Gemeint sind hier im gesetzlichen Zusammenhang mit der Terrorismusabwehr vielmehr etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen.“ BVerfGE 141, 220 (287).

Insofern kann das Merkmal „Sachen von bedeutendem Wert“ in § 49 HmbPolDVG ebenfalls allenfalls bei einer sehr engen Auslegung als verfassungskonform angesehen werden. Legt man die vorherrschende Interpretation dieses Merkmals in anderen Zusammenhängen zugrunde, ist eine Verfassungskonformität nicht gegeben. So wird eine Sache von bedeutendem Wert im Sinne des § 315b Abs. 1 StGB nach ständiger Rechtsprechung des BGH schon ab einem Wert von 750 Euro angenommen.

BGH NJW 2003, 836 (837); BGH NStZ 2011, 215.

Als Sachen von bedeutendem Wert kämen demnach etwa eine öffentliche Sitzbank, eine Torwand auf einem Bolzplatz, Werbeträger oder andere im Visier von Sprayern

stehende Gegenstände in Betracht. Nach diesem Verständnis könnte § 49 Abs. 1 HmbPolDVG zum Beispiel eine automatisierte Datenanalyse zur Durchleuchtung der Sprayerszene ermöglichen.

Angesichts der beschriebenen Intensität der Datenanalyse sind die in § 49 Abs. 1 HmbPolDVG normierten Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse liegt, zumindest im Sinne des Urteils zum BKA-Gesetz so auszulegen, dass nur wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen gemeint sind.

Der Unbestimmtheit des Rechtsguts vermag auch nicht abzuhelfen, dass bei gebotener Berücksichtigung des Zweckbindungsgrundsatzes gemäß § 34 HmbPolDVG die Daten aus besonders schweren Grundrechtseingriffen (wie beispielsweise der Wohnraumüberwachung) nicht für eine Datenanalyse zum Schutz von bedeutsamen Sachwerten oder der Umwelt herangezogen werden können. Schließlich sind auch in den nutzbaren Datenbeständen große Datenmengen vorhanden, die bei Verknüpfung neue, weitreichende Erkenntnisse über die Zielperson zutage fördern können.

b) Fehlende eigene Abwägungsentscheidung und mangelnde Bestimmtheit

§ 49 Abs. 1 HmbPolDVG ist auch deshalb verfassungswidrig, weil die Regelung den Einsatz von komplexen Algorithmen nicht stützen kann und der Gesetzgeber es versäumt hat, eine eigene Abwägungsentscheidung darüber zu treffen, welchen Einsatz von Überwachungstechnologien er zulassen will. Die Regelung ist daher unverhältnismäßig und genügt nicht den rechtsstaatlichen Anforderungen an die Bestimmtheit von Eingriffsbefugnissen.

Im Gesetzgebungsverfahren ist weitgehend unklar geblieben, welche Methoden der Datenauswertung § 49 Abs. 1 HmbPolDVG im Einzelnen rechtfertigen soll und wie die Regelung zu den bereits bestehenden Befugnissen für Datenabgleich (§ 48 HmbPolDVG) und Rasterfahndung (§ 50 HmbPolDVG) abzugrenzen ist.

Vgl. Hamburgische Bürgerschaft, Ausschussprotokoll 21/38, S. 42.

Vieles deutet dabei darauf hin, dass die neue Befugnis den Einsatz von Methoden künstlicher Intelligenz und komplexen Algorithmen ermöglichen soll. Dies wird aber aus der Befugnis nicht hinreichend klar. Weder aus der Regelung selbst noch aus den Gesetzgebungsmaterialien ergibt sich aber letztlich ein eindeutiges Ziel, an dem sich

die Verhältnismäßigkeit der Regelung messen lässt. Sie leidet damit an einem Mangel der Bestimmtheit, der sich auch in der Unverhältnismäßigkeit der Regelung niederschlägt.

> Vgl. zu der Beeinträchtigung der Verhältnismäßigkeit durch Mängel in der Bestimmtheit BVerfGE 110, 33 (55).

Das rechtsstaatliche Bestimmtheitsgebot verlangt vom Gesetzgeber bezogen auf Eingriffsbefugnisse nach dem angerufenen Gericht, „dass er technische Eingriffsinstrumente genau bezeichnet und dadurch sicherstellt, dass der Adressat den Inhalt der Norm jeweils erkennen kann."

> BVerfGE 112, 304 (316).

Zwar sind keine gesetzlichen Formulierungen notwendig, die jede Einbeziehung kriminaltechnischer Neuerungen ausschließen, und eine gewisse Dynamik technologisch geprägter Befugnisse erweist sich als unvermeidbar.

> BVerfGE 112, 304 (316).

Jedenfalls eine Grundentscheidung darüber, ob eine Eingriffsbefugnis den Einsatz von Künstlicher Intelligenz oder komplexer Algorithmen erlauben soll, muss aber durch den Gesetzgeber getroffen und in der betreffenden Vorschrift festgelegt werden.

> Vgl. BVerfG NJW 2020, 2235 (2253 Rn. 192).

Der Einsatz entsprechender Techniken bringt aufgrund ihrer besonderen Dynamik, ihrer eigenständigen Entwicklungsfähigkeit, ihrer immanenten Intransparenz und den Implikationen einer komplexen und teilautonomen Datenverarbeitung für die Eingriffsintensität einen besonderen Bedarf klarer Regelung und sorgfältiger gesetzgeberischer Abwägung mit sich.

In § 49 Abs. 1 HmbPolDVG genügt namentlich das Merkmal einer „automatisierten Anwendung zur Datenauswertung" den Anforderungen einer hinreichend spezifischen Regelung nicht.

> Vgl. Albers, Stellungnahme im Rahmen der öffentlichen Anhörung des Innenausschusses am 19. September 2019 zu dem Gesetzentwurf des Senats der Freien und Hansestadt Hamburg, Drittes Gesetz zur Änderung polizeirechtlicher Vorschriften, S. 4.

Als automatisierte Anwendungen zur Datenauswertung lassen sich von vergleichsweise banalen technischen Mitteln (wie z.B. Textdokumenten und Tabellen, die elektronisch gespeichert sind) bis hin zu hochkomplexen Machine-Learning-Programmen Anwendungen unterschiedlichster Art einordnen.

> Vgl. zu dem Merkmal „automatisierte Verfahren“ im datenschutzrechtlichen Zusammenhang Schild, in: BeckOK Datenschutzrecht, Bearbeitungsstand 2020, Art. 4 Rn. 34.

Das Merkmal hat keine Unterscheidungskraft dahingehend, ob es gerade auch den Einsatz komplexerer Verfahren wie eigenständig lernfähiger Systeme zulässt. Dies macht § 49 HmbPolDVG zunächst untauglich, entsprechende Anwendungen zu rechtfertigen.

Die Regelung ist aus diesem Grund allerdings nicht nur nutzlos, sondern auch verfassungswidrig. Der Gesetzgeber hat es versäumt, eine eigenständige Abwägungsentscheidung zur Reichweite der Befugnis zu treffen und den Zweck der Regelung klar festzulegen. Schon im Gesetzgebungsverfahren und auch weiterhin erscheint unklar, mit welchen technischen Mitteln die Befugnis umgesetzt werden soll.

> Vgl. Hamburgische Bürgerschaft Drs. 21/20061; Hamburgische Bürgerschaft Drs. 22/1758.

Zwar ist eine Regelung, die technisch zum Zeitpunkt ihrer Verabschiedung noch nicht umsetzbar ist, nach dem angerufenen Gericht nicht zwangsläufig widersprüchlich und unverhältnismäßig. Es darf aber nicht ausgeschlossen sein, dass die technischen Voraussetzungen zur Anwendung der Regelung in absehbarer Zukunft geschaffen werden können.

> BVerfGE 141, 220 (311).

Die Schaffung einer in hohem Maße technologisch geprägten Befugnis ohne das genaue Bewusstsein ihrer Zielrichtung dürfte allerdings die Grenzen der gesetzgeberischen Entscheidungsbefugnis überschreiten. Der Gesetzgeber schien im Zusammenhang keiner Einordnung und Bewertung der technischen Mittel, deren Einsatz § 49 HmbPolDVG rechtfertigen soll, fähig. Eine eigene Abwägungsentscheidung war damit nicht möglich.

> Vgl. LVerfG Sachsen-Anhalt, DVBl. 2015, 38.

Zudem erweckt die Regelung den falschen Anschein, sie könne den Einsatz komplexer und lernfähiger Anwendungen zur Datenauswertung rechtfertigen. Dies führt einerseits zu Einschüchterungseffekten bei den betroffenen Grundrechtsträger*innen und andererseits zu reellen Anreizen bei der Polizei, entsprechende Analysen technisch zu ermöglichen und durchzuführen.

c) Verfahrenssicherungen

Es fehlt der Regelung schließlich an ausreichenden begleitenden Verfahrenssicherungen. Bei der Speicherung und Nutzung personenbezogener Daten für die behördliche Aufgabenwahrnehmung hat der Gesetzgeber unter Verhältnismäßigkeitsgesichtspunkten auch Anforderungen an Transparenz, Rechtsschutz und Kontrolle zu beachten.

BVerfGE 133, 277 (366).

Speziell im Zusammenhang mit dem Einsatz komplexer Algorithmen hat das angerufene Gericht ausgeführt, dass ihre grundsätzliche Nachvollziehbarkeit im Hinblick auf eine unabhängige Kontrolle sicherzustellen ist.

BVerfG NJW 2020, 2235 (2253 Rn. 192).

§ 49 HmbPolDVG erfüllt keine dieser Anforderungen und verletzt damit nicht nur das Grundrecht der Beschwerdeführer*innen auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, sondern auch das Grundrecht auf individuellen Rechtsschutz nach Art. 19 Abs. 4 GG.

(1) Transparenzschaffende Regelungen

§ 49 HmbPolDVG enthält keine ausreichenden transparenzschaffenden Regelungen.

Nach §§ 68 f. HmbPolDVG existieren Benachrichtigungspflichten und Auskunftsrechte in Bezug auf die bei der Polizei Hamburg gespeicherten personenbezogenen Daten einer Person. Während die Benachrichtigungspflicht aus § 68 HmbPolDVG sich nicht auf die Verarbeitung von Daten nach § 49 HmbPolDVG bezieht, können Betroffene über das Auskunftsrecht nach § 68 Abs. 1 Nr. 1 i.V.m. § 68 Abs. 1 Satz 1 Nr. 2 HmbPolDVG zumindest Auskunft darüber verlangen, ob Daten über sie auf der Grundlage von § 49 HmbPolDVG verarbeitet wurden.

Angesichts der Schwere des Eingriffs, der über die bereits vorhandenen personenbezogenen Daten einer Person weitergehende Erkenntnisse bis hin zu weitreichenden Persönlichkeitsbildern generieren kann, wäre zumindest eine Benachrichtigung der Betroffenen nach Abschluss des Einsatzes einer Anwendung zur automatisierten Datenanalyse verfassungsrechtlich geboten.

(2) Kontrolle und Aufsicht

Auch in Bezug auf die Gewährleistung einer wirksamen Aufsicht verfehlt § 49 HmbPolDVG die verfassungsrechtlichen Anforderungen. Die Anordnung der Datenanalyse erfolgt nach § 49 Abs. 3 HmbPolDVG durch die Polizeipräsidentin oder den Polizeipräsidenten oder die Vertretung im Amt. Zudem ist die oder der Datenschutzbeauftragte vor der Einrichtung oder wesentlichen Änderung anzuhören, bei Gefahr im Verzug ist die Anhörung nachzuholen. Im Wesentlichen kann jede beauftragte Person bei der Polizei die automatisierte Analyse anordnen, bei Gefahr auch ohne Anhörung der*s Datenschutzbeauftragten. Erfolgt eine Anhörung des*r Datenschutzbeauftragten, folgen hieraus keine zwingenden Konsequenzen.

Zudem fehlen der*m Datenschutzbeauftragten die Zugriffsrechte auf die Datenanalyse, um die Reichweite im Einzelfall umfassend beurteilen zu können. Er hat auch keine wirksamen Möglichkeiten, um auf deren rechtmäßige Durchführung hinzuwirken. Der Hamburgische Beauftragte für den Datenschutz verfügt nach § 72 Abs. 1 HmbPolDVG gegenüber der Polizei nur über sehr schwache Befugnisse. Er ist bei der Feststellung von Datenschutzverstößen darauf beschränkt, diese zu beanstanden und ggf. den Rechtsweg zur Feststellung der Rechtswidrigkeit zu beschreiten.

Die Schwere des Eingriffs erfordert zur Durchführung von Maßnahmen nach § 49 Abs. 1 HmbPolDVG als rechtliche Kontrollmechanismen zunächst einen Richtervorbehalt, zumindest jedoch die Zustimmung eines*r mit Zugriffs- und Anordnungsbefugnissen ausgestatteten Datenschutzbeauftragten.

Des Weiteren ist eine technische Kontrolle der bei der Anwendung der Befugnis aus § 49 Abs. 1 HmbPolDVG eingesetzten Verfahren verfassungsrechtlich notwendig. Es ist anzunehmen, dass die Befugnis auch den Einsatz komplexer Algorithmen und lernfähiger Systeme ermöglichen soll. Diese sind für die Betroffenen und auch für juristische Expert*innen kaum überprüfbar und nachvollziehbar. Um den nach Art. 19 Abs. 4

GG gebotenen effektiven Rechtsschutz gegen Maßnahmen erlangen zu können, bei denen derartige technische Hilfsmittel zum Einsatz kommen, bedarf es institutioneller Vorkehrungen, um die Maßnahmen auf tatsächlicher Ebene überprüfbar zu machen.

Gerade der Einsatz (teil-)autonomer Systeme verleiht Maßnahmen zur Gefahrenabwehr einen gänzlich neuen Charakter und eine Intransparenz, die über das übliche Maß der Intransparenz beim Einsatz technischer Hilfsmittel hinausgeht. Die Funktionsweisen derartiger Hilfsmittel sind technisch besonders komplex und entwickeln sich dynamisch weiter, so dass es einer kontinuierlichen Überprüfung bedarf, die weder dem Betroffenen noch den sicherheitsbehördlichen Endanwender*innen allein ohne Weiteres möglich ist.

Es ist daher eine unabhängige Instanz einzusetzen, um die technische Dimension zur Umsetzung von § 49 HmbPolDVG zu kontrollieren und die eingesetzte Software ggf. im Vorfeld zu zertifizieren.

Zur effektiven Kontrolle ist weiterhin erforderlich, dass die jeweiligen Anwendungen zur automatisierten Datenanalyse vollständig protokolliert werden. Diese prozessualen Vorgaben müssen zur Wahrung der Verhältnismäßigkeit auch gesetzlich verankert sein.

Zudem fehlt es in § 49 HmbPolDVG an eingrenzenden Vorgaben zur Dauer der Maßnahme, zur Löschung der durch die automatisierte Datenanalyse generierten Erkenntnisse und zur Anwendung der aus den Grundsätzen der Zweckbindung und Zweckänderung resultierenden Beschränkungen.

Zwar mögen die allgemeinen Regelungen zur Dauer der Datenspeicherung (§ 35 HmbPolDVG), sowie zur Zweckbindung (§ 34 HmbPolDVG) anwendbar sein, aufgrund der Besonderheiten der automatisierten Datenanalyse lassen diese Regelungen gleichwohl wesentliche Fragen unbeantwortet. Fraglich ist beispielweise, ob die Löschfristen nach § 35 Abs. 2 HmbPolDVG sich jeweils verlängern, wenn Daten innerhalb der automatisierten Datenanalyse generiert und diese Verknüpfungen dort gespeichert werden. Unklar ist auch, wie lang die Speicherung der Datenanalysen selbst und ihrer Ergebnisse erfolgen soll. Wie lange dies in der Regel erforderlich ist (vgl. § 35 Abs.1 HmbPolDVG), sollte weiter konkretisiert werden. Die Maßgaben der Zweckbindung nach § 34 HmbPolDVG lassen sich nicht ohne Weiteres auf die automatisierte Datenanalyse übertragen, vielmehr bedarf es angesichts der Schwere des Eingriffs eines konkreten Ermittlungsanlasses.

(3) Anforderungen an die Art und Qualität der einbezogenen Daten

Schließlich fehlt es § 49 HmbPolDVG an einer Eingrenzung der einzubeziehenden Daten und Vorkehrungen zur Sicherung ihrer Qualität. Dadurch ist die Regelung unverhältnismäßig, da sie ohne entsprechende Absicherung keine komplexen Analysen ermöglicht, die wirksam zum Zweck der Gefahrenabwehr beitragen.

Eine komplexe Datenanalyse ist neben der Leistungsfähigkeit der Analysemethoden vor allem von der Art und Qualität der zugrunde liegenden Daten abhängig. Ohne eine ausreichend gesicherte Datenbasis kann sie keine validen Ergebnisse liefern und letztlich nicht zum Zweck der Gefahrenabwehr beitragen.

Vgl. Härtel, LKV 2019, 49 (54).

Werden komplexe, insbesondere auf lernfähigen Systemen beruhende Datenanalysen ohne weitere Überprüfung mit Informationen aus polizeilichen Datenbeständen gespeist, besteht erstens die Gefahr, dass sie den Kontext der ursprünglichen Erhebung der Daten vernachlässigen. Die konkrete Aussagekraft personenbezogener Daten erschließt sich nur aus dem sozialen Kontext ihrer Ergebung. Zweitens kann eine ungeprüfte Einbeziehung vorhandener Datenbestände dazu führen, dass sich menschliche Vorurteile oder Fehlwahrnehmungen, die in den Datenbeständen festgehalten sind, in der Anwendung zur Auswertung perpetuieren. Hieraus ergeben sich schwerwiegende Diskriminierungsrisiken, die einerseits die Eingriffsintensität der Datenverarbeitung steigern und andererseits eine prozedurale Absicherung erfordern.

Vgl. Härtel, LKV 2019, 49; Singelnstein, NStZ 2018, 1 (6).

Dass sich neuartige Risiken der Diskriminierung durch moderne Überwachungstechnologien auf internationaler Ebene bereits realisieren, ist beispielsweise anhand des Einsatzes von Software zur intelligenten Gesichtserkennung

Vgl. Süddeutsche Zeitung vom 12. Juni 2020; https://www.sueddeutsche.de/digital/microsoft-gesichtserkennung-rassismus-1.4934730.

oder zur Vorhersage von Bandenkriminalität nachvollziehen.

Vgl. Golem.de vom 30. September 2020; https://www.golem.de/news/predictive-policing-amnesty-kritisiert-polizei-fuer-diskriminierende-algorithmen-2009-151209.html.

Derartigen Risiken ist bei der komplexen Datenauswertung unter anderem durch Anforderungen an die Qualität von Daten, die in die Analysen einbezogen werden, vorzubeugen. § 49 HmbPolDVG sieht hierzu allerdings keine solche Regelung vor. Der Gesetzgeber wäre verpflichtet gewesen, den Mindeststandard der Qualität der einbezogenen Daten genauer zu definieren.

Jun.-Prof. Dr. Sebastian Golla