



Stellungnahme

des Deutschen Anwaltvereins durch
den Ausschuss Gefahrenabwehrrecht

**Stellungnahme des Deutschen Anwaltvereins zu
den geplanten Änderungen des Hamburgischen
Polizeirechts (Entwurf für ein Drittes Gesetz zur
Änderung polizeirechtlicher Vorschriften,
Bürgerschaft der Freien und Hansestadt Hamburg,
Drucksache 21/17906 vom 30.07.2019)**

Stellungnahme Nr.: 40/2019

Berlin, im Oktober 2019

Mitglieder des Ausschusses Gefahrenabwehrrecht

- Rechtsanwältin Lea Voigt, Bremen (Vorsitzende und
Berichterstatlerin)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwalt Dr. David Albrecht, Berlin (Berichterstatter)
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt / Main
- Rechtsanwältin Kerstin Oetjen, Freiburg

Deutscher Anwaltverein

Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel

Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Max Gröning
- Rechtsanwältin Uta Katharina Schmidt

Verteiler

Bundesministerium des Innern
Bundesministerium der Justiz und für Verbraucherschutz

Deutscher Bundestag – Ausschuss für Recht und Verbraucherschutz
Deutscher Bundestag - Innenausschuss

Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien
Arbeitskreise Recht der Landtagsfraktionen Hamburg
Arbeitskreise Innen der Landtagsfraktionen Hamburg

Justizministerien und -senatsverwaltungen der Länder
Landesministerien und Senatsverwaltungen des Innern
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Innenausschüsse der Landtage
Rechtsausschüsse der Landtage

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Deutscher Richterbund
Bundesverband der Freien Berufe
Gewerkschaft der Polizei (Bundesvorstand)
Deutsche Polizeigewerkschaft im DBB
Verd.di, Recht und Politik
stiftung neue verantwortung e.V.
Institut für Deutsches und Europäisches Strafprozessrecht und Polizeirecht (ISP)
der Universität Trier
Rechtsanwaltskammer des Landes Hamburg
Deutscher Richterbund Hamburg
Verband der freien Berufe Hamburg
Gewerkschaft der Polizei Hamburg

Vorstand und Landesverbände des DAV
Vorsitzende der Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
Vorsitzende des FORUM Junge Anwaltschaft des DAV

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung
Hamburger Abendblatt
Juris Newsletter
JurPC

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit seinen über 63.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

A. Einleitung/Zusammenfassung

Der Senat der Freien und Hansestadt Hamburg hat am 30. Juli 2019 den Entwurf eines Dritten Gesetzes zur Änderung polizeirechtlicher Vorschriften vorgelegt. In der Hauptsache sieht der Entwurf Änderungen des Gesetzes über die Datenverarbeitung der Polizei (PoIDVG) vor. Hierbei werden in erheblichem Umfang neue Ermächtigungsgrundlagen zur polizeilichen Erhebung und Verarbeitung von Daten geschaffen. Diese stellen zum Teil übermäßige Verkürzungen grundrechtlich geschützter Positionen dar und sind deshalb abzulehnen. Dies betrifft u. A. die Vorschriften zur elektronischen Aufenthaltsüberwachung (§ 30 PoIDVG-E, „elektronische Fußfessel“), zur Einführung einer automatisierten Datenanalyse (§ 49 PoIDVG-E) sowie die geplante Einschränkung der Rechte des Landesdatenschutzbeauftragten (§ 72 PoIDVG-E).

Darüber hinaus wird der Gesetzesentwurf den Anforderungen an einen hinreichenden Schutz des Vertrauensverhältnisses zwischen Betroffenen und den von ihnen konsultierten Berufsgeheimnisträgern, insbesondere Rechtsanwälten, nicht gerecht. Der DAV fordert auch hier eine Regelung, die entsprechend dem Vorbild des § 62 BKAG den notwendigen Schutz zeugnisverweigerungsberechtigter Personen gewährleistet.

Die vorliegende Stellungnahme beschränkt sich auf die vorgenannten Punkte.

B. Elektronische Aufenthaltsüberwachung, § 30 PoIDVG-E

Der mit der elektronischen Aufenthaltsüberwachung (Fußfessel) verbundene Grundrechtseingriff ist ebenfalls erheblich. Es handelt sich um eine Maßnahme, die in erster Linie in Straf- und Maßregelvollzug/-vollstreckung zum Einsatz kommt. Dass der

damit verbundene schwere Grundrechtseingriff bereits zur Abwehr einer nur drohenden Gefahr angemessen wäre, ist schlicht nicht denkbar. In dem frühen und damit zwangsläufig ungewissen Stadium einer drohenden Gefahr muss sich die Gefahrenabwehr darauf beschränken, den Sachverhalt weiter zu erforschen. Erst wenn sich die Gefahr weiter konkretisiert, können unter Beachtung des Verhältnismäßigkeitsgrundsatzes weitere Maßnahmen zur Anwendung kommen.

Darüber hinaus soll nach dem Gesetzesentwurf gem. § 30 Abs. 1 Nr. 3 die Fußfessel zur Verhütung jeglicher Gefahr für Leib, Leben oder Freiheit zulässig sein. Anders als bei der Führungsaufsicht geht es also nicht um die Abwehr schwerer Straftaten. Der Anwendungsbereich wird damit bedenklich ausgeweitet.

Hinzukommt, dass die in § 30 PoIDVG-E geregelte elektronische Aufenthaltsüberwachung als Mittel der Gefahrenabwehr ungeeignet ist. Die Evaluation der im Bereich der Führungsaufsicht in § 68 b Abs. 1 S. 1 Nr. 12 StGB geregelten elektronischen Fußfessel hat ergeben, dass diese nicht dazu beiträgt, die Betroffenen von Straftaten abzuhalten. Gleiches gilt für die Gefahrenwehr. Kein Terrorist wird sich aufgrund einer elektronischen Fußfessel davon abhalten lassen, Straftaten zu begehen.

C. Fehlender Schutz von Berufsgeheimnisträgern

Der Gesetzesentwurf sieht einen Schutz des Berufsgeheimnisses bei der Verarbeitung personenbezogener Daten durch die Polizeibehörden nur bereichsspezifisch vor. Auswirkungen hat dies insbesondere auf das Verhältnis von Betroffenen polizeilicher Maßnahmen zu ihren anwaltlichen Beiständen. So statuiert der Entwurf Erhebungs- und/ oder Verwendungsverbote in Bezug auf personenbezogene Daten, die einem Berufsgeheimnis unterliegen, nicht umfassend, lediglich für bestimmte Maßnahmen. Hierzu zählen beispielsweise Bild- und Tonaufzeichnungen von Personen in amtlichem Gewahrsam (§ 18 Abs. 4 PoIDVG-E), die verdeckte Wohnraumüberwachung (§ 22 Abs. 2 u. 6 PoIDVG-E) und die Quellen-Telekommunikationsüberwachung (§ 26 Abs. 3 PoIDVG-E). Jenseits dieser bereichsspezifischen Sonderregelungen ist eine Verarbeitung von Daten, die einem Berufsgeheimnis unterliegen, für polizeiliche Zwecke uneingeschränkt erlaubt.

Der Gesetzesentwurf folgt damit nicht dem bundesgesetzlichen Vorbild des § 62 BKAG, mit dem die Vorgaben des Bundesverfassungsgerichts aus seiner Entscheidung zum BKA-Gesetz (BVerfG, Urteil v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09) umgesetzt wurden. Der Bundesgesetzgeber hat mit § 62 BKAG eine Generalklausel zum Schutz von Berufsgeheimnisträgern geschaffen, die u. a. Eingriffe in das Vertrauensverhältnis von Rechtsanwälten zu ihren Mandanten absolut untersagt und bereits die Erhebung von Daten, die von einem Berufsgeheimnis umfasst sind, untersagt. Eine vergleichbare Regelung enthält im Übrigen auch der Gesetzesentwurf der Landesregierung von Mecklenburg-Vorpommern zur Neufassung des dortigen Sicherheits- und Ordnungsgesetzes aus dem Juni dieses Jahres.

Dass nach dem vorliegenden Hamburger Gesetzesentwurf überhaupt nur bei einigen wenigen Maßnahmen ein Berufsgeheimnisschutz zu beachten ist und zudem nur zum Teil die Datenerhebung, im Übrigen lediglich die Verwendung bereits erlangter Daten untersagt wird, ist sachlich nicht gerechtfertigt. Die Vertrauensbeziehung zu Berufsgeheimnisträgern wie Rechtsanwälten und Strafverteidigern ist unabhängig davon zu schützen, ob es sich bei der konkreten Maßnahme etwa um die akustische Überwachung oder eine Durchsuchung von Wohnräumen handelt. Auch muss dort, wo Berufsgeheimnisse in Rede stehen, schon die Datenerhebung ausgeschlossen werden, um einen effektiven Schutz zu gewährleisten. Bereits die Speicherung personenbezogener Daten stellt einen Eingriff in Freiheitsrechte dar, der zwecklos und damit ungerechtfertigt ist, wenn die Daten zwingend wieder zu löschen sind, weil sie beispielsweise die Kommunikation des Betroffenen mit seiner Strafverteidigerin betreffen. Auch würde die Statuierung von Erhebungsverboten der Gefahr entgegenwirken, dass zu schützende Inhalte – bewusst oder unbewusst – doch für Zwecke der Gefahrenabwehr verwendet werden.

Bleibt der Schutz, wie im vorliegenden Hamburger Entwurf beabsichtigt, lückenhaft, ist angesichts immer weiterreichender staatlicher Eingriffsbefugnisse eine Erosion des Vertrauens des rechtssuchenden Bürgers und der Allgemeinheit in die Vertraulichkeit anwaltlicher Kommunikation zu befürchten, die rechtsstaatlich nicht hinnehmbar ist.

D. Automatisierte Anwendung zur Datenanalyse, § 49 PoIDVG-E

Der Gesetzesentwurf enthält in § 49 eine neue Rechtsgrundlage für die Verarbeitung personenbezogener Daten in einem automatisierten Analysesystem. Die Regelung ist erkennbar darauf gerichtet, den Einsatz von Analyseprogrammen wie das seit dem Jahr 2017 in Hessen eingesetzte „hessenDATA“ zu legitimieren. § 49 PoIDVG-E ist nahezu inhaltsgleich mit § 25a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung.

„hessenDATA“ basiert auf dem Programm „Gotham“ des US-amerikanischen Softwareanbieters Palantir Technologies und ermöglicht die automatisierte Zusammenführung, Verknüpfung und Auswertung gespeicherter Daten. So können etwa vom Algorithmus erkannte Verbindungen zwischen Personen und Objekten automatisch identifiziert und visualisiert werden und so Anlass für weitergehende polizeiliche Maßnahmen bieten.

Die automatisierte Datenanalyse, die § 49 PoIDVG-E vorsieht, birgt erhebliche Gefahren für die Rechte der Betroffenen und übersteigt den Rahmen des verfassungsrechtlich Zulässigen.

Zum einen besteht das Risiko, dass das Zusammenführen und Verknüpfen bislang über verschiedene Datenbanken verteilter Informationen in einem einheitlichen System es ermöglicht, umfassende Verhaltens- und Persönlichkeitsprofile einzelner Personen zu generieren. Dies wäre mit Verfassungsrecht nicht mehr vereinbar, worauf das Bundesverfassungsgericht ausdrücklich in seinem Beschluss zur Rasterfahndung in Nordrhein-Westfalen (BVerfG, Beschl. v. 4.4.2006 – 1 BvR 518/02) hingewiesen hat. § 49 PoIDVG-E erlaubt die Nutzung aller bei der Polizei Hamburg gespeicherten Daten, zu denen auch die aufgrund bestehender Ermächtigungsgrundlagen bei externen öffentlichen und privaten Stellen generierten Daten gehören. Hierzu zählen beispielsweise Daten aus strafrechtlichen Ermittlungsverfahren, aus der Telekommunikations- und Wohnraumüberwachung sowie von Telekommunikationsanbietern übermittelte Daten. Zudem können auch Daten aus externen Quellen, wie z. B. sozialen Netzwerken, einfließen.

Automatisierte Analysensysteme bergen auch wegen ihrer hohen „Streubreite“ ein besonderes Gefahrenpotenzial. So können Personen allein deshalb in den Fokus der Behörden geraten, weil sie in (irgend)einer vom System erkannten Verbindung zu einer bereits erfassten Person oder einem Gegenstand stehen. Das Programm differenziert selbst nicht hinreichend nach der Qualität der erkannten Verknüpfung. Die damit verbundene Gefahr kann zwar durch Zwischenschaltung einer menschlichen Kontrollinstanz verringert werden, ist aber in automatisierten Analysensystemen angelegt.

Als Eingriffsschwelle benennt § 49 PolDVG-E die vorbeugende Bekämpfung von in § 100a Abs. 2 StPO 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.

Der Begriff der „vorbeugenden Bekämpfung“ ermöglicht den Einsatz der Datenanalyse weit im Vorfeld einer konkreten Gefahr und gewährleistet damit nicht, dass die automatisierte Datenverarbeitung an eine konkrete Gefahr im verfassungsrechtlichen Sinne gebunden wird, wie dies geboten ist (vgl. BVerfG, Beschl. v. 4.4.2006 – 1 BvR 518/02). Darüber hinaus enthält § 100a Abs. 2 StPO strafrechtliche Vorfelddelikte, wie z.B. die Gründung oder Beteiligung an einer terroristischen Vereinigung (§ 129a StGB). Deren „vorbeugenden Bekämpfung“ bedeutet eine nochmalige ganz erhebliche Vorverlagerung der Eingriffsschwelle.

Die Einbeziehung von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, begegnet zudem verfassungsrechtlichen Bedenken in Bezug auf das Bestimmtheitsgebot.

§ 49 PolDVG-E steht auch in Konflikt mit den verfassungsrechtlichen Anforderungen an eine hinreichende Transparenz und Kontrolle staatlicher Eingriffsmaßnahmen. Eine von der Datenanalyse betroffene Person muss weder nachträglich über die Verarbeitung ihrer Daten benachrichtigt werden, noch wird ihr insoweit ein Auskunftsrecht zugestanden. Nach der Konzeption des Gesetzesentwurfs ist zudem jeder Polizeibeamte befugt, eine automatisierte Datenanalyse durchzuführen.

Innerbehördliche Kontrollmechanismen sieht der Entwurf nicht vor; der Datenschutzbeauftragte soll lediglich vor der (erstmaligen) Einrichtung oder wesentlichen Änderung des Systems beteiligt werden und auch diese vorherige Anhörungspflicht soll bei Gefahr im Verzug entfallen.

Die vom Hamburger Senat vorgelegte Regelung wird – ebenso wie ihr hessisches Pendant – den verfassungsrechtlichen Herausforderungen, die mit einer bestandsübergreifenden automatisierten Datenauswertung einhergehen, nicht im Ansatz gerecht. Es ist nicht erkennbar, dass sich die Verfasser des Entwurfs überhaupt das Ausmaß des mit diesem Instrument potentiell einhergehenden Grundrechtseingriffs vergegenwärtigt haben. So heißt es in der Begründung (Drs. 21/17906, S. 70) verharmlosend, die Regelung sei keine Befugnisnorm zur Erhebung neuer personenbezogener Daten, sondern regele lediglich die automatisierte Analyse bereits rechtmäßig erlangter personenbezogener Daten. Diese Sichtweise geht am Kern des Problems der (automatisierten) Zusammenführung verschiedenster riesiger Datenbestände weit vorbei und verstellt den Blick auf den erforderlichen Schutz der Grundrechte betroffener Bürger.

E. Abbau der Befugnisse des Landesdatenschutzbeauftragten (§ 72 PoIDVG-E)

Vor dem Hintergrund der weitreichenden geplanten neuen Eingriffsermächtigungen (s. oben) alarmiert es umso mehr, dass der Hamburger Entwurf zugleich vorsieht, dem Landesdatenschutzbeauftragten lediglich ein Beanstandungsrecht einzuräumen. Dies bedeutet im Umkehrschluss, dass er im Anwendungsbereich des PoIDVG nicht das Recht haben soll, gegenüber der Polizei verbindliche Anordnungen zu treffen. Dieses dem Landesdatenschutzbeauftragten nach der DSGVO zustehende Recht ist schon für sich genommen kein besonders machvolles Instrument, denn diese Anordnungen sind nicht sofort vollziehbar. Dass der Senat es nun dennoch für den Bereich der Polizei abschaffen will, ist höchst bedenklich und stellt zudem einen evidenten Verstoß gegen die für die Datenverarbeitung durch Polizeibehörden geltende EU-Datenschutz-Richtlinie im Bereich von Justiz und Inneres (JI-Richtlinie) dar. Art. 47 Abs. 2 der Richtlinie verpflichtet die Mitgliedstaaten, jeder Datenschutzaufsichtsbehörde wirksame Abhilfebefugnisse zu gewähren. Die Aufsichtsbehörden müssen insbesondere die

Kompetenz haben, Anweisungen und Verarbeitungsverbote gegenüber Verantwortlichen auszusprechen. Es liegt der Verdacht nahe, dass Anlass eine seitens des Hamburger Datenschutzbeauftragten im Zusammenhang mit der automatisierten Auswertung biometrischer Daten aus Videoüberwachungsanlagen durch die Hamburger Polizei kürzlich ausgesprochene Anordnung ist, gegen welche die Polizei derzeit verwaltungsgerichtlich vorgeht.

Der Deutsche Anwaltverein spricht sich dafür aus, die rechtliche Stellung und die Ausstattung der Landes- und des Bundesdatenschutzbeauftragten auszubauen. Nur dies würde der stetigen Ausweitung von Datenerhebungs- und -verwendungsbefugnissen staatlicher Stellen angemessen Rechnung tragen. Dabei ist auch zu berücksichtigen, dass insbesondere bei verdeckten Maßnahmen die Betroffenen selbst nicht in der Lage sind, das staatliche Handeln zeitnah rechtlich überprüfen zu lassen. Gerade hier ist aber eine engmaschige, an Grundrechtspositionen orientierte Kontrolle erforderlich.