Innenausschuss
A-Drs. 18(4)601 F

# Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6 (Block C), D – 20095 Hamburg

An
Herrn Ministerialrat Dr. Heynckes
Platz der Republik 1
11011 Berlin

- per E-Mail -

Klosterwall 6, Block C
D – 20095 Hamburg
Telefon: 040 - 428 54 - 40 40 (Vorzimmer)
Telefax: 040 - 428 54 - 40 00
Ansprechpartner: Prof. Dr. Caspar
E-Mail*: mailbox@datenschutz.hamburg.de

Az.: D /

Hamburg, den 23. Juni 2016

**Ergänzende Stellungnahme zum Entwurf eines Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus (Bundestags-Drucksache 18/8702)**

Sehr geehrter Herr Dr. Heynckes,

ergänzend zu meinen mündlichen Ausführungen anlässlich der Anhörung im Innenausschuss des Bundestages am 20.8.2016, die sich aus Zeitgründen auf den Fragenbereich der Errichtung von Verbunddateien im Zuge der vorgeschlagenen Änderungen des BVerfSchG (§ 22 b, 22c) beschränkten, darf ich Ihnen vorliegend noch einige weitere Anmerkungen zum Gesetzentwurf zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus (BT-Drs.18/8702) übersenden.

## I. Art. 3: Änderung des Bundespolizeigesetzes

1. Die verdeckte Datenerhebung ist zwar im BPolG grundsätzlich nach § 21 Abs. 3 S. 3 zulässig. Allerdings war der Einsatz von Polizeibeamten unter einer Legende - also von Verdeckten Ermittlern - mangels bisheriger ausdrücklicher gesetzlicher Ermächtigung nach BPolG zur Gefahrenabwehr ausgeschlossen (vgl. BR Drs 418/94, S. 52ff), allerdings zur Strafverfolgung gem. § 110 ff. StPO zulässig.

Mit dem vorliegenden Gesetzentwurf soll künftig der Einsatz von Verdecken Ermittlern nunmehr auch zu Gefahrenabwehrzwecken zulässig sein. Unter Verweis auf die gesetzliche Begründung (vgl. BR Drs 418/94, S. 52 ff) hatte der Gesetzgeber seinerzeit diesen „Mangel"



*Vertrauliche Informationen sollten auf elektronischem Weg nur verschlüsselt an uns übermittelt werden.
Unser öffentlicher PGP-Schlüssel ist im Internet verfügbar (Fingerprint: 0932 579B 33C1 8C21 6C9D E77D 08DD BAE4 3377 5707)

gesehen und bisher bewusst darauf verzichtet, den Einsatz von verdeckten Ermittlern im Bundespolizeigesetz zur Gefahrenabwehr zu regeln. Zu Recht, denn bei einem Einsatz von verdeckten Ermittlern im Bereich der Gefahrenabwehr tritt gerade die Längerfristigkeit der Maßnahme, die zur Erlangung einer Vertrauensstellung des verdeckten Ermittlers in den jeweiligen sozialen Milieus erforderlich ist (vgl. Begründung, Drucks. 18/8702, S. 25), mit der tatbestandlich geforderten Gefahrensituation häufig in einen tiefen rechtsstaatlichen Widerspruch.

Die Aufgabenwahrnehmung der Polizei ist nach Maßgabe des Trennungsgebots zwischen Polizei und Nachrichtendienst grundsätzlich durch Offenheit geprägt (vgl. BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 –, BVerfGE 133, 277-377, Rn. 122). Eine Geheimpolizei ist im Gefüge des GG nicht vorgesehen. Der Einsatz von Verdeckten Ermittlern der Polizei muss daher stets auf die zeitliche Dauer einer Gefahrenabwehrsituation beschränkt bleiben. In der Praxis erweist sich jedoch häufig, dass polizeilich tätige Verdeckte Ermittler bereits im Bereich des Gefahrenvorfelds eingesetzt werden und daher ein klarer Bezug zur Gefahrenabwehr nicht hergestellt werden kann.

2. Der Entwurf sieht lediglich bei dem Einsatz technischer Mittel zur Eigensicherung von verdeckten Ermittlern, § 28 a BPoLG-E, einen Kernbereichsschutz vor. Eine Regelung zum Schutz des Kernbereichs privater Lebensgestaltung beim standardmäßigen Einsatz von Verdeckten Ermittlern fehlt. Verdeckte Ermittler können gleichwohl unter Ausnutzung des Vertrauens der Betroffenen in höchstpersönliche Bereiche eindringen. Weil sich die private Lebensgestaltung – besonders in ihren kommunikativen Bezügen – auch außerhalb von Wohnungen vollziehen kann, bedarf es grundsätzlich auch in diesem Bereich kernbereichsschützender Regelungen.

Davon, dass die private Lebensgestaltung auch außerhalb von Wohnungen in den Kernbereich fallen kann, geht das BVerfG aus, wenn es den Kernbereichsschutz für Online-Durchsuchungen und Telekommunikationsüberwachungen fordert. Das privat gesprochene Wort auch außerhalb von Wohnungen ist sowohl faktisch als auch rechtlich vor Überwachungsmaßnahmen geschützt. Rechtlich ist dies beispielsweise in § 201 StGB (Verletzung der Vertraulichkeit des Wortes) manifestiert. Zudem lässt sich bereits aus der Garantie der Menschenwürde ableiten, dass der Kernbereichsschutz nicht auf bestimmte physische Räume beschränkt werden kann. Verfahrensrechtliche Sicherungen sind daher jedenfalls immer auch dann vorzunehmen, wenn Eingriffe verdeckt oder geheim und mit besonderen technischen Mitteln vorgenommen werden, die die üblichen sozialen und physischen Schutzmechanismen überwinden, die von den Betroffenen zur Wahrung ihres Kernbereichs eingesetzt werden.

Verletzungsgeneigte Ermittlungsbefugnisse erfordern daher zwingend Regelungen zum Kernbereichsschutz sowohl auf der Ebene der Erhebung als auch auf der Ebene der Verwertung (so BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 –, BVerfGE 133, 277-377, Rn. 123 ff.).

3. Eine nachträgliche Benachrichtigung der von verdeckten Maßnahmen betroffenen Bürgerinnen und Bürgern stellt einen Grundsatz dar, der zur Realisierung des informationellen Selbstbestimmungsrechtes der Betroffenen beitragen soll. Nachvollziehbar ist, dass aus bestimmten, gewichtigen Gründen von einer Benachrichtigung abgesehen werden können muss. § 28 Abs. 8 S. 1 Nr. 5 der vorliegenden Entwurfsfassung intendiert jedoch, dass bereits die Gefährdung der Möglichkeit der „weiteren Verwendung des Verdeckten Ermittlers" Grund genug für ein Absehen von der Benachrichtigung sein kann. Angesichts des Aufwandes, einen Verdeckten Ermittler unter einer Legende in entsprechende Vertrauensstellungen zu bringen und damit einsatzfähig zu halten, besteht die dringende Besorgnis, dass insbesondere diese Ausnahmebegründung regelhaft einer nachträglichen Benachrichtigung der Betroffenen entgegengesetzt wird; hier ist ein (nahezu) gänzlicher Ausschluss der nachträglichen Benachrichtigung und der damit verbundenen Ziele zu befürchten.

**II. Art. 5: Änderung des Art. 10-Gesetzes**

1. Laut Gesetzentwurf soll in § 15 Abs. 6 des Artikel 10-Gesetzes nach Satz 2 eingefügt werden, dass bei Gefahr im Verzug am Tag der Beantragung bereits vor der Anordnung der Beschränkungsmaßnahme mit der Datenerhebung begonnen werden darf, die bereits erhobenen Daten aber erst nach der Anordnung genutzt werden dürfen. Erfolgt die Anordnung nicht binnen 24 Stunden nach Beantragung, sind die erhobenen Daten unverzüglich automatisiert und unwiederbringlich zu löschen.

Laut Gesetzesbegründung (Drucks. 18/8702, S. 30) soll diese Änderung Maßnahmen des BND für den Fall betreffen, dass bereits der Überwachung unterliegende Fernmeldeverkehrsbeziehungen nach zusätzlichen Telekommunikationsmerkmalen gefiltert werden können. Die Einfügung der Regelung nach S. 2 hätte jedoch zur Konsequenz, dass damit alle G-10 Maßnahmen betroffen wären. Der Entwurf bedarf insofern einer Konkretisierung und einer gesetzlichen Klarstellung, um sicherzustellen, dass nicht sämtliche G-10 Maßnahmen betroffen sind.

2. Schließlich trifft aber auch die Annahme in der Gesetzesbegründung, dass „eine rein technische Erfassung ohne jede menschliche Kenntnisnahme“ der Daten noch keinen Eingriff in Artikel 10 GG darstellt (vgl. Drucks. 18/ 8702, S. 30), nicht zu.

Bereits die Selektierung von Kommunikationsdaten zur weiteren Verwendung stellt für sich genommen einen Eingriff in das Telekommunikationsgeheimnis dar (vgl. BVerfGE 100, 313 <366 f.>). Eine Regelung, die einen derartigen Eingriff vorsieht, muss daher an dem qualifizierten Gesetzesvorbehalt des Art. 10 Abs. 2 GG gemessen werden und löst eine Überprüfung entsprechender Maßnahmen durch die von der Volksvertretung bestellten Organe und Hilfsorgane aus. Eine Ausleitung von Kommunikationsinhalten auf Vorrat, auch wenn auf diese zunächst nicht zugegriffen werden darf, stellt einen Eingriff in Art. 10 Abs. 1 GG dar. Der Schutz durch Art. 10 Abs. 1 GG gilt nicht nur dem eigentlichen Zugriff, mit dem die öffentliche Gewalt von Telekommunikationsvorgängen und -inhalten tatsächlich Kenntnis nimmt. Seine Schutzwirkung erstreckt sich auch auf die Informations- und Datenverarbeitungsprozesse, die sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließen, und auf den Gebrauch, der von den erlangten Kenntnissen gemacht wird (vgl. BVerfGE 100, 313 <359>). Hierzu gehört auch die Aufzeichnung durch die öffentliche Gewalt (vgl. BVerfGE 85, 386 <398>; 100, 313 <366>; 110, 33 <52 f.>). In der Erfassung von Telekommunikationsdaten, ihrer Speicherung, ihrem Abgleich mit anderen Daten, ihrer Auswertung, ihrer Selektierung zur weiteren Verwendung oder ihrer Übermittlung an Dritte liegen damit je eigene Eingriffe in das Telekommunikationsgeheimnis (vgl. BVerfGE 100, 313 <366 f.>).

Diese Rechtsprechung wurde in zahlreichen Entscheidungen – u.a. in der jüngeren Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung (BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 –, BVerfGE 125, 260-385) – bestätigt. Eine Sichtweise, die den Schutzbereich des Grundrechts auf eine tatsächliche Kenntnisnahme der Kommunikation durch staatliche Stellen beschränkte, ist damit nicht zu vereinbaren.

**III. Art. 9: Änderung des Telekommunikationsgesetzes**

1. Bereits gegenwärtig verpflichtet § 111 TKG die Anbieter von Telekommunikationsdiensten, die von ihnen vergebenen Anschlusskennungen bzw. Rufnummern, Mobilfunkendgerätenummern, Kennungen von elektronischen Postfächern sowie auch die persönlichen Daten der Anschlussinhaber, wie Namen, Anschriften, Geburtsdaten, zur Freischaltung zu erheben und zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind. Diese Vorschrift wird nunmehr durch Artikel 9 Nummer 2 des Gesetzentwurfs um die Pflicht der geschäftsmäßigen Erbringer von

Telekommunikationsdiensten, die bereits zu erhebenden Bestandsdaten insbesondere durch die Vorlage eines Ausweises bzw. Passes zu überprüfen, erweitert. Dies führt zu einer gesteigerten Kontrollpflicht der Telekommunikationsanbieter gegenüber ihren Kunden und soll die Abgabe fehlerhafter Namensangaben in den Kundendatenbanken von Telekommunikationsdiensten verhindern.

Das Bundesverfassungsgericht hatte bereits mit Beschluss vom 24. Januar 2012 – 1 BvR 12990/05 – festgestellt, dass die Zuordnung von Telekommunikationsnummern zu individuellen Anschlussinhabern einen Eingriff in das Recht auf informationelle Selbstbestimmung verfassungsrechtlich grundsätzlich rechtfertigen kann. Dieser Eingriff diene dazu, eine verlässliche Datenbasis für die Auskunftserteilung an Behörden zu halten, (BVerfG – 1 BVR 1299/05, Rn. 132). Hiermit sei eine Verbesserung staatlicher Aufgabenwahrnehmung insbesondere im Bereich der Strafverfolgung und bei der Gefahrenabwehr und der nachrichtendienstlichen Tätigkeit verbunden. Trotz der Tatsache, dass die erfassten Daten vorsorglich anlasslos verfügbar gehalten werden sollen, ist dies mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar (Bundesverfassungsgericht 1 BVR 1299/05, Rn. 133).

Die mit dem vorliegenden Entwurf verbundene Erstreckung der Erhebungs- und Speicherungspflicht auf eine Kontrollpflicht der Daten von Anschlussinhabern stellt insoweit keine wesentliche Vertiefung der bereits bestehenden Eingriffssituation dar. Letztlich dient die Erweiterung der Regelung nur einer Durchsetzung der bereits durch das Verfassungsgericht akzeptierten legitimen gesetzgeberischen Zwecksetzung.

Gleichwohl befindet sich der Gesetzentwurf zur Änderung des TKG nicht gänzlich auf der rechtlich sicheren Seite: Das Verbot anonymer Prepaid-Mobilfunkverträge wird derzeit auf Beschwerde von Bürgerrechtlern durch den Europäischen Gerichtshof für Menschenrechte überprüft. In diesem Verfahren wurde jüngst die Bundesregierung zu einer schriftlichen Stellungnahme aufgefordert (hierzu http://www.zeit.de/digital/datenschutz/2016-06/prepaid-karten-anonym-menschengerichtshof)

In diesem Verfahren geht es um die grundsätzliche Frage, inwieweit dem Recht auf Privatsphäre nach Artikel 8 der EMRK ein grundsätzliches Verbot der anonymen Telekommunikationsdienstenutzung entgegensteht und die gesetzliche Eingriffsregelung in einer demokratischen Gesellschaft notwendig für die nationale oder öffentliche Sicherheit im Sinne des Artikels 8 Absatz 2 EMRK ist. Die Klage ist nicht aussichtlos, zumal der Europarat in einer Ministerratsempfehlung zum Schutz der persönlichen Daten im Bereich der Telekommunikationsdienste in der Vergangenheit ausdrücklich einen anonymen Zugang zu

Telekommunikationsdiensten gefordert hatte (Council of Europe, On the Protection of Personal Data in the Area of Telecommunication Services, Committee of Ministers, Recommendation No. R. (95) 4, adopted on 7 Februar 1995, unter 2.2)[1].

2. Die im neuen Abs. 1 Satz 5, 2. Halbsatz vorgesehene Speicherung der Angaben zu Art, Nummer und ausstellender Stelle widerspricht zudem den Vorgaben im Personalausweisgesetz, wonach die automatisierte Speicherung der Ausweisdaten unzulässig ist.

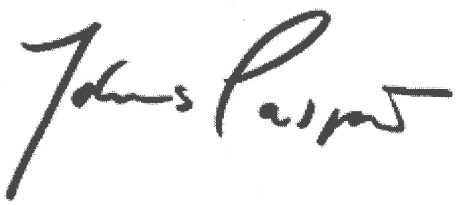
Wenn es dem Gesetzgeber lediglich darum geht, Karteninhaber zu identifizieren, dann sind die Daten, die nicht zur Identifizierung benötigt werden, auch nicht zu speichern. Dies gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer. Aus Nachweisgründen ist die Anfertigung eines entsprechenden Vermerks (z.B.: "Pass-/Personalausweiskopie hat vorgelegen") ausreichend.

Damit fehlt es an der Erforderlichkeit dieser Daten.

3. Im Übrigen stellt sich die Frage nach der Geeignetheit der im Entwurf vorgesehenen Maßnahmen zur Überprüfung der Richtigkeit der nach § 111 Abs. 1 S. 1 erhobenen Daten. Während ein Ausweis und ein Pass gerade der Identifikation dient, kann derzeit nicht nachvollzogen werden, wie z.B. ein alternativ („oder") vorzulegender Handelsregisterauszug geeignet sein kann, die Richtigkeit der zu erhebenden Daten sicherzustellen.

Für weitere Fragen stehe ich Ihnen gern zur Verfügung.

Mit freundlichen Grüßen



Prof. Dr. Johannes Caspar

[1] Abzurufen unter: http://azop.hr/images/dokumenti/168/recommendationr954.pdf sowie https://www.coe.int/t/dghl/standardsetting/dataprotection/EM/EM_R(95)4_EN.pdf.