Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Vorsitzende des Ausschusses für Inneres
und Heimat
des Deutschen Bundestages
Frau Andrea Lindholz
Platz der Republik 1
11011 Berlin

Per E-Mail: innenausschuss@bundestag.de
andrea.lindholz@bundestag.de

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn

FON (0228) 997799-5000
FAX (0228) 997799-5550

E-MAIL referat35@bfdi.bund.de
INTERNET www.bfdi.bund.de

DATUM Bonn, 17.03.2021
GESCHÄFTSZ. 35-643/077#0670

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Entwurf eines Gesetzes zur Modernisierung der Rechtsgrundlagen der Bundespolizei**

HIER Öffentliche Anhörung im Ausschuss für Inneres und Heimat am 22. März 2021
BEZUG Bundestagsdrucksache 19/26541

Sehr geehrte Frau Vorsitzende,

anlässlich der Öffentlichen Anhörung am 22. März 2021 übersende ich Ihnen meine Stellungnahme zu dem Entwurf für ein „Gesetz zur Modernisierung der Rechtsgrundlagen der Bundespolizei“ und wäre Ihnen dankbar, wenn diese den Ausschussmitgliedern zur Verfügung gestellt werden könnte. Da es sich um einen gemeinsamen Gesetzentwurf der Fraktionen von CDU/CSU und SPD handelt, hat im Vorfeld der Ausschussberatung keine Ressortberatung stattgefunden. Daher hatte ich bislang keine Gelegenheit zu einer Stellungnahme in Bezug auf die datenschutzrechtlichen Aspekte des Gesetzentwurfs.

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Entsprechend meiner gesetzlichen Aufgabe, den Deutschen Bundestag in datenschutzrechtlichen Fragestellungen zu beraten, bin ich gerne bereit, meine Bedenken gegen den Gesetzentwurf auch persönlich dem Ausschuss vorzutragen.

Mit freundlichen Grüßen

Ulrich Kelber

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 09.03.2021

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung im Ausschuss für Inneres und Heimat

des Deutschen Bundestages

am 22. März 2021

zum

Gesetzentwurf der Fraktionen von CDU/CSU und SPD

zur Modernisierung der Rechtsgrundlagen der Bundespolizei

(BT-Drucksache 19/26541)

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Mit dem Gesetzesentwurf werden die Befugnisse der Bundespolizei erweitert und den Möglichkeiten des Bundeskriminalamtes (BKA) angeglichen. Dabei wird allerdings verkannt, dass es sich bei der Bundespolizei - auch in Abgrenzung zu den Landespolizeibehörden - um eine Sonderpolizei mit begrenztem Aufgabenspektrum handelt.[1]Zugleich wird die Richtlinie (EU) 2016/680 vom 27. April 2016 (JI-RL) sowie das Urteil des Bundesverfassungsgerichts vom 20. April 2016 zum damaligen Bundeskriminalamtsgesetz umgesetzt. Ich hätte es begrüßt, wenn zunächst eine Evaluierung der Eingriffsbefugnisse der Bundespolizei erfolgt und der Gesetzentwurf vor diesem Hintergrund erarbeitet worden wäre.

Im Folgenden werde ich mich auf die datenschutzrechtlichen Hauptkritikpunkte an dem Gesetzentwurf beschränken.

I. Hervorgehobene Aspekte

1. Zu Art. 1 Nr. 25 (§ 36 BPolG-E: Verzeichnis von Verarbeitungstätigkeiten)

Ausdrücklich kritisiere ich, dass die Errichtungsanordnung (EAO) als Verfahrenssicherung für die Einrichtung automatisierter Dateien, mit denen personenbezogene Daten verarbeitet werden, ersatzlos gestrichen worden ist. Da der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) gemäß § 36 Abs. 2 BPolG vor Erlass einer EAO anzuhören ist, stellt sie ein wirksames Instrument der Datenschutzkontrolle dar. Durch deren Wegfall wird der Datenschutz massiv geschwächt.

Die Begründung zu § 36 BPolG-E verweist auf eine Kompensation des Wegfalls der EAO durch eine Ergänzung des Verarbeitungsverzeichnisses. Dieses Argument geht fehl, denn die in der Regelung zur EAO enthaltene Rechtspflicht zur Anhörung des BfDI vor Beginn einer Verarbeitung ist ersatzlos gestrichen worden. Diese ist jedoch essentiell, denn sie ermöglicht die datenschutzrechtliche Vorab-Prüfung und Beratung. Sie kann auch zu dem Ergebnis führen, dass eine Verarbeitung nicht oder nur auf abgeänderte Weise datenschutzkonform durchführbar ist. Schon aus diesem Grund ist eine frühestmögliche Beteiligung des BfDI unbedingt erforderlich. Dies gilt auch im Hinblick auf die Fälle, in denen Haushaltsmittel für die Errichtung einer neuen Datei ausgegeben werden.

[1] BVerfG, Beschluss des Zweiten Senats vom 28. Januar 1998 - 2 BvF 3/92, Rn. 87 ff.

Gem. § 36 Abs. 3 BPolG-E soll das Verarbeitungsverzeichnis auch dem BfDI zur Verfügung gestellt werden. Ein genauer Zeitpunkt für die Zurverfügungstellung findet sich im Gesetzentwurf jedoch nicht. Außerdem besteht keine Verpflichtung zu einer Anhörung des BfDI.

Darüber hinaus entfällt für die Bundespolizei die Pflicht, in angemessenen Abständen die Notwendigkeit der Weiterführung oder Änderung der geführten Dateien zu überprüfen (zur bisherigen Rechtslage vgl. § 36 Abs. 3 BPolG). Die Verarbeitung von personenbezogenen Daten in automatisierten Dateien stellt einen Grundrechtseingriff dar. Mit dem Wegfall dieser Prüfpflicht besteht die Gefahr, dass die Nutzung und Pflege der Datei ohne weitere Selbstkontrolle fortgeführt wird. Damit wird ein wichtiges Instrument zur Sicherstellung eines angemessenen Datenschutzstandards ohne Not gestrichen. Betroffen hiervon sind in erster Linie die in den Dateien gespeicherten Personen. Die Regelung geht aber auch zulasten eines effektiven Aufgabenvollzuges der Bundespolizei, wenn das Personal der Bundespolizei mit der Pflege von unnötigen oder unzureichenden Dateien gebunden ist.

Ich empfehle dringend, die Regelung zur EAO neben der europarechtlich erforderlichen Einführung eines Verarbeitungsverzeichnisses beizubehalten.

Sollte sich der Gesetzgeber gegen ein Beibehalten der EAO entscheiden, so ist dem BfDI zumindest ein Anhörungsrecht vor Aufnahme einer neuen Verarbeitung in das Verfahrensverzeichnis einzuräumen. In diesem Fall sollte zudem die Pflicht der Behörde aus dem bisherigen § 36 Abs. 3 BPolG übernommen werden, in angemessenen Abständen die Notwendigkeit der Weiterführung oder Änderung der geführten Dateien zu überprüfen.

2. Zu Art. 1 Nr. 25 (§ 37 BPolG-E: Ergänzende Befugnisse der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit)

Mit § 37 Absatz 2 BPolG-E soll Art. 47 Abs. 2 JI-RL umgesetzt werden, der festlegt, dass Aufsichtsbehörden über wirksame Abhilfebefugnisse verfügen müssen.

Die in Abs. 2 aufgestellten Voraussetzungen einer stufenweisen Abfolge von Beanstandung und Anordnung, das Einziehen einer Erheblichkeitsschwelle und die in der Gesetzesbegründung erwähnte Auslassung der Löschanordnung (S. 51) führen zu einer unzureichenden Umsetzung der JI-RL. Die in Art. 47 Abs. 2 lit. a) bis c) JI-RL genannten Beispiele reichen von der Anordnung, die Rechtmäßigkeit wiederherzustellen, über die Anordnung der Datenlöschung bis hin zu einem Verbot der Datenverarbeitung.

Das Erfordernis einer vorherigen Beanstandung gefährdet gerade in den Fällen, in denen eine sofortige Umsetzung von Anordnungen des BfDI zwingend erforderlich ist, die Betroffenenrechte.

Die Einschränkung der Anordnungsbefugnis durch das zusätzliche Kriterium der Erheblichkeit kann allenfalls klarstellenden Charakter haben. Als Aufsichtsbehörde ist der BfDI ohnehin verpflichtet, eine einzelfallbezogene, verhältnismäßige Maßnahme zu treffen. Ist die

Erheblichkeit relativ zur beabsichtigten Maßnahme zu sehen, kommt dem Kriterium also kein Mehrwert zu. Ist es unabhängig von der anzuordnenden Maßnahme zu sehen, schränkt es die Effektivität der Ausübung der Befugnisse ein. Es ist nicht nachvollziehbar, welches Interesse der Bundespolizei bestehen soll, bei einer rechtswidrigen Verarbeitung personenbezogener Daten keiner einzelfallbezogenen, verhältnismäßigen Anordnung der Aufsichtsbehörde Folge leisten zu müssen.

Ich rege an, den Katalog möglicher Maßnahmen des Art. 47 Abs. 2 JI-RL klarstellend in den Gesetzeswortlaut aufzunehmen.

Die in Artikel 47 Absatz 5 JI-Richtlinie vorgesehene Befugnis der Aufsichtsbehörde, Verstöße gegen Datenschutzvorschriften den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben, fehlt in dem Gesetzentwurf ebenfalls. Ich empfehle, dies zu ergänzen.

Ohne die vorgeschlagene Nachbesserung von § 37 BPolG-E besteht mit Blick auf die mangelhafte Umsetzung der Befugnisse des BfDI die Möglichkeit eines Vertragsverletzungsverfahrens der EU-Kommission gegen die Bundesrepublik Deutschland.

3. Zu Art. 1 Nr. 14 (Überschrift von Teil 2 „Weiterverarbeitung und Übermittlung von Daten“)

Den Begriff des „Weiterverarbeitens“ verwendet der Gesetzentwurf überaus zahlreich.

Eine einheitliche Definition für den Begriff der Weiterverarbeitung existiert weder in der JI-Richtlinie noch in der Datenschutz-Grundverordnung (DSGVO). Da der Begriff auch im Gesetzentwurf nicht näher beschrieben wird, fallen hierunter alle denkbaren Datenverarbeitungstatbestände wie die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, der Abgleich oder die Verknüpfung von Daten.

Im gesamten Teil 2 zur „Weiterverarbeitung“ sowie in § 41a BPolG-E wird dieser Begriff pauschal verwendet. Dies betrifft neben der Vorschrift des § 29 BPolG-E auch sämtliche Folgeregelungen. Deshalb wird nicht hinreichend klar, wie mit den personenbezogenen Daten umgegangen wird. Durch die begriffliche Entgrenzung besteht die Möglichkeit einer weitgehenden Verknüpfung und damit einer Anreicherung von Daten zu einer Person. Auf diese Weise werden zusätzliche Eingriffe einer gesonderten Regelung entzogen. Das ist verfassungsrechtlich nicht hinnehmbar. Es muss sichergestellt sein, dass die mit der jeweiligen Regelung beabsichtigten Datenverarbeitungen identifiziert und eindeutig bezeichnet werden.

II. Einzelne Vorschriften

1. Zu Art. 1 Nr. 6 (§ 21 BPolG-E: Erhebung personenbezogener Daten)

§ 21 Abs. 2 BPolG-E sieht als Voraussetzung für die Datenerhebung „Straftaten mit erheblicher Bedeutung“ vor. Die bisher bestehende Bezugnahme auf die konkrete, in § 12 Abs. 1 BPolG genannten Straftatbestände wurde gestrichen. Angesichts des Eingriffsgewichts und der potentiellen Folgen der Datenverarbeitung ist diese Eingriffsnorm nicht ausreichend bestimmt.

2. Zu Art. 1 Nr. 8 (§ 24 BPolG-E: Erkennungsdienstliche Maßnahmen)

Die Erweiterung erkennungsdienstlicher Maßnahmen in Abs. 1 Nr. 2 auf die Strafverfolgungsvorsorge auch als eigener Hauptzweck muss kritisch hinterfragt werden. Nicht dargetan ist, warum die einschlägigen Regelungen der Strafprozessordnung (StPO) hier nicht ausreichend sein sollen. Zudem fehlt die Voraussetzung einer hinreichenden Negativprognose. Denn es ist nicht geklärt, wie konkret der Gefahreneintritt sein muss (z.B. „in naher Zukunft“).[2]

Dies entspricht der Änderung von § 1 Abs. 5 BPolG-E, der als Aufgabe der Bundespolizei innerhalb der Gefahrenabwehr nun auch die „*Vorsorge für die künftige Verfolgung von Straftaten*“ aufführt. Je nach Zugehörigkeit zur Strafverfolgungsvorsorge oder zur Gefahrenabwehr führt dies potentiell zu unterschiedlichen verfassungsrechtlichen Anforderungen.

Die Vorsorge für die spätere Verfolgung von Straftaten betrifft die Verfolgung noch gar nicht begangener, sondern in ungewisser Zukunft bevorstehender Straftaten. Eine Verwertung der erhobenen Daten für diesen Zweck kommt erst in Betracht, wenn tatsächlich eine Straftat begangen wurde und daraus strafprozessuale Konsequenzen gezogen werden. Die der Verfolgungsvorsorge zugeordneten Daten und Informationen sind insofern dazu bestimmt, in ungewisser Zukunft in ein Ermittlungs- und Hauptverfahren einzufließen. Es geht - jenseits eines konkreten Anfangsverdachts - um die Beweisbeschaffung zur Verwendung in künftigen Strafverfahren, nicht um eine präventive Datenerhebung zur Verhütung von Straftaten. Eine solche Verfolgungsvorsorge ist kompetenzmäßig dem „*gerichtlichen Verfahren*” i. S. des Art. 74 Absatz 1 Nr. 1 GG zuzuordnen (BVerfG, Urteil vom 27. 07. 2005 -

[2] BVerfG NJW 2016, 1781, Rn. 165.

1 BvR 668/04). Die Regelung sollte daher nicht im Bundespolizeigesetz, sondern in der StPO erfolgen.

Bei der Vorsorge für die Verfolgung künftiger Straftaten oder bei ihrer Verhütung kann zudem nicht an dieselben Kriterien angeknüpft werden, die für die Gefahrenabwehr oder die Verfolgung begangener Straftaten entwickelt worden sind (BVerfG, Urteil vom 27. 7. 2005 - 1 BvR 668/04).

3. Zu Art. 1 Nr. 10 (§ 27d BPolG-E: Überwachung der Telekommunikation)

Mit den Möglichkeiten zur heimlichen Überwachung der Telekommunikation einer Person bzw. zur sog. Quellen-TKÜ werden der Bundespolizei neue Befugnisse eingeräumt.

In der Gesetzesbegründung heißt es, dass Normzweck vor allem die Abwehr von Gefahren für Leib und Leben sei. Grund soll insbesondere die Schleusungskriminalität, im Falle der präventiven Überwachung nach Abs. 1 auch der Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt, sein. Hierunter sollen „primär" Infrastrukturen im Bahn- und Flugbereich fallen. Die Norm wird an § 51 Bundeskriminalamtgesetz (BKAG) angelehnt, welcher der Terrorabwehr dient.[3] Besonders im Bereich der Eigentumskriminalität im Bahnbereich ist zweifelhaft, ob Delikte in diesem Bereich die mit einer Telekommunikationsüberwachung einhergehende Eingriffstiefe rechtfertigt. Angesichts der Intensität des Eingriffs sollte ein abschließender Straftatenkatalog vorgegeben werden.

a. Präventive TKÜ

Laut Gesetzesbegründung soll sich die Überwachung der Telekommunikation nach § 27d Abs. 1 BPolG-E präventiv gegen Personen richten, gegen die noch kein Tatverdacht begründet ist und daher keine Maßnahme nach § 100a StPO angeordnet werden kann. Die Rechtsgrundlage soll Fälle betreffen, in denen die Voraussetzung der StPO nicht gegeben sind, also keine Umstände vorliegen, die nach der kriminalistischen Erfahrung in erheblichem Maße darauf hindeuten, dass jemand als Täter oder Teilnehmer die Tat begangen hat[4]. Vielmehr soll die Norm schon im Vorfeld einer etwaigen Tatbegehung greifen. Das wirft die Frage auf, ob eine angemessene Differenzierung zwischen präventiven und repressiven Maßnahmen möglich ist. Problematisch ist zudem, dass eine mit der StPO vergleichbare Prüfung, nämlich ob eine Tat auch im Einzelfall besonders schwer wiegt

[3] Schenke/Graulich/Ruthig/Ralf P. Schenke, 2. Aufl. 2018, BKAG § 51 Rn. 1.

[4] Vgl. zu der in Bezug genommenen Vorschrift BeckOK StPO/Graf, 38. Ed. 1.10.2020, StPO § 100a Rn. 100.

(§ 100a Abs. 1 S. 1 Nr. 2 StPO), nach dieser Rechtsgrundlage nicht durchgeführt werden muss.

Sollte die Norm aufrechterhalten werden, sollte dem besseren Verständnis halber in Abs. 1 S. 1 "einer Person" durch "dieser Person" ersetzt werden.

In Nr. 2 ist der Unterschied zu dem Regelungsgehalt von Nr. 1 unklar, insbesondere, wann die Tatbestandsvoraussetzungen vorliegen. Wann ist „bei einer Person“ anzunehmen, dass eine Schädigung etwa am Bestand eines Landes eintritt? Hier wird letztlich keine umsetzbare Eingriffsschwelle formuliert. Aktuell ist kein Regelungsgehalt zusätzlich zur Nr. 1 erkennbar.

In Nr. 3 werden die vom Bundesverfassungsgericht aufgestellten engen Bedingungen in Bezug auf die Behandlung von Kontaktpersonen unterlaufen.

In Nr. 4 werden auch Unbeteiligte erfasst, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass die Person ihren Telekommunikationsanschluss oder ihr Endgerät nutzen wird. Dies kann also nichtsahnende Familienangehörige u. ä. betreffen.

b. Quellen-TKÜ

Mit der sog. Quellen-TKÜ nach § 27d Abs. 2 BPolG-E wird der bei der Telekommunikationsüberwachung ohnehin schon schwere Grundrechtseingriff noch einmal vertieft. Das Bundesverfassungsgericht hat auf die besonderen Risiken hingewiesen, die mit einer Quellen-Telekommunikationsüberwachung verbunden sind.[5] Mit der Infiltration des Systems sei „die entscheidende Hürde genommen, um das System insgesamt auszuspähen.“

Sicherheitslücken

Diese Gefahren allerdings entstehen nicht nur durch das gezielte Auslesen des Systems durch Ermittlungsbehörden, sondern auch durch abstrakte Gefährdungen. Sie können entstehen, wenn eine Behörde Sicherheitslücken des betroffenen Systems gezielt ausnutzt und eine Überwachungssoftware einschleust. Durch das Zurückhalten von Sicherheitslücken wird das allgemeine IT-Sicherheitsniveau gesenkt. Es kann nicht ausgeschlossen werden, dass auch Kriminelle oder ausländische Akteure (Nachrichtendienste etc.) diese Sicherheitslücken nutzen. Dieses Risiko ist in der Gesetzesbegründung nicht angemessen bewertet worden.

[5] BVerfGE 120, 274, 308.

Unbeabsichtigter Beifang

Zudem besteht das Risiko, unbeabsichtigt Informationen ohne Bezug zur laufenden Telekommunikation zu erlangen. Das Bundesverfassungsgericht hat in diesem Zusammenhang auf die Gefahr hingewiesen, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden könnten.

Wenn beispielsweise während einer laufenden Quellen-TKÜ ein Backup des überwachten Gerätes an einen Cloudspeicher übertragen wird - wie es heutzutage häufig automatisch durchgeführt wird - so können damit auch alle auf dem Gerät gespeicherten Daten betroffen sein. Diese dürften im Rahmen der Quellen-TKÜ ausgewertet werden. Damit hat die Quellen-TKÜ effektiv eine vergleichbare Eingriffstiefe wie die Online-Durchsuchung. Um dies einzugrenzen, wäre die Überwachung auf laufende menschliche Chat-, IP-Telefonie oder Videokonferenzen sowie den manuellen Aufruf von Webseiten zu begrenzen.

Zudem sind in dem durch die Quellen-TKÜ erfassten Datenstrom üblicherweise auch Zugangsdaten (wie etwa Passwörter) für Online-Dienste im Klartext enthalten. Dies würde der Bundespolizei einen umfassenden Zugriff auf alle verwendeten Online-Dienste der betroffenen Person ermöglichen, wie etwa E-Mail-Postfächer, Cloudspeicher, etc. Auch die unbemerkte Manipulation dieser Dienste im Namen der überwachten Person ist dadurch möglich (auch Identitätsdiebstahl).

c. Online Durchsuchung

§ 27d Abs. 2 Satz 2 BPolG-E sieht eine verfassungsrechtlich höchst problematische Erweiterung der Quellen-TKÜ auf eine echte Online-Durchsuchung vor.

Die Norm lässt den Datenzugriff bereits für den Fall einer nur hypothetischen Überwachung zu („wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.“).

Sie gestattet rückwirkend den Zugriff auf vergangene Kommunikationsdaten, namentlich solche, die eine Zielperson zwischen Anordnungszeitpunkt und Inbetriebnahme der Überwachungssoftware übertragen oder erhalten hat. Damit überschreitet die Norm die kritische Grenze zur Online-Durchsuchung; der Eingriff muss sich am so genannten IT-Grundrecht messen. Die Vorschrift ist daher verfassungswidrig[6] und sollte gestrichen werden.

[6] Martini/Fröhlingsdorf: Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, NVwZ 2020, 1803, 1804 zu dem gleichlautenden § 100a Abs. 1 S. 3 StPO.

In der Begründung fehlt eine Erläuterung, wie diese Formulierung in Abgrenzung zu der Voraussetzung von § 27d Abs. 2 Satz 1 Nr. 1 BPolG-E zu verstehen ist, wie ein konkreter Anwendungsfall aussehen soll und wie die technische Umsetzung erfolgen soll.

d. Absätze 5, 6

Unklar ist welche Geräte oder Kennungen im Antrag und dem anordnenden Beschluss anzugeben sind. Schon die in Abs. 5 Nr. 2 sowie Absatz 6 Nr. 2 gewählte Formulierung zeigt deutlich die Schwierigkeiten, "Geräte" eindeutig zu identifizieren. Die Zeiten „einer Festnetzrufnummer“ sind vorbei. Als Folge ist bereits die Identifikation von Geräten problematisch. Daher sollte für diejenigen Fällen, in denen keine sichere Feststellung oder Zuordnung möglich ist, bestimmt werden, dass von der Überwachung abzusehen ist.

e. Kernbereichsschutz

Unklar ist, inwieweit aktuell die Möglichkeit besteht, technisch sicherzustellen, dass Daten, die dem Kernbereich der privaten Lebensgestaltung der betroffenen Person zuzurechnen sind, nicht erhoben werden (Abs. 8 S. 1, S. 2 des Entwurfs). In der Vergangenheit bestanden bereits technische Schwierigkeiten bei der Löschung erlangter kernbereichsrelevanter Daten (siehe mein 24. Tätigkeitsbericht, Nr. 7.4.1). Erst recht dürfte es technisch kaum umsetzbar sein, durch eine Unterbrechung, wie sie in Abs. 8 S. 2 angedacht wird, sicherzustellen, dass Daten, die den Kernbereich betreffen, nicht erhoben werden. Bei einer Quellen-TKÜ könnte dies wohl nur unter hohem Aufwand durch ein „Live-Mithören“ organisiert werden. Was die Online Durchsuchung betrifft, erscheint dies unmöglich. Es kann niemand „live“ mehrere Gigabyte Download „mithören“ oder „mitlesen“.

f. Fazit

Die Quellen-TKÜ ist im Vergleich zur herkömmlichen TKÜ sowohl mit zusätzlichem Aufwand als auch mit hohen rechtlichen und technischen Risiken verbunden. Hier gilt für die Quellen-TKÜ aus technischer Sicht nichts anderes als für die Online-Durchsuchung (die hier verfassungswidrig ist und somit gestrichen werden sollte, s. o.). Es ist fraglich, ob die genannten Risiken im Einzelfall tatsächlich erkannt und eingegrenzt werden können.

Auch aus diesen Gründen ist eine stärkere Einschränkung und Konkretisierung des Anwendungsbereichs insbesondere der Quellen-TKÜ dringend notwendig.

Anders, als es der Wortlaut und die Systematik vermuten lassen, wird die Quellen TKÜ-den Regelfall der TKÜ darstellen. Aus der Begründung geht hervor, dass die hierauf bezogenen Kommunikationswege deliktsübergreifend bevorzugt genutzt werden. Die in der Begründung dargestellte Subsidiarität der Quellen-TKÜ gegenüber der herkömmlichen TKÜ tritt damit in den Hintergrund.

4. Zu Art. 1 Nr. 10 (§ 27e BPolG-E: Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten)

Zwar sieht die Begründung in § 27e BPolG-E eine Rechtsgrundlage für die Versendung sog. stiller SMS vor. Eine korrespondierende, ausdrückliche Rechtsgrundlage zur Erhebung der durch den Versand erzeugten, retrograden Standortdaten vergleichbar mit § 100g Abs. 1 Satz 1 Nr. 1 und Satz 3 i. V. m. Abs. 2 StPO ist allerdings nicht vorgesehen. Auf die Telekommunikationsüberwachung nach § 27d BPolG-E kann die Erhebung nicht gestützt werden, da die Daten nicht im Rahmen von Telekommunikation anfallen.[7]

Die Begründung stellt weiterhin darauf ab, der Versand stiller SMS könne infolge des genannten Beschlusses des BGH nicht mehr auf § 100a StPO gestützt werden, sodass für den präventiven Einsatz eine gesonderte Rechtsgrundlage zu schaffen sei. Es wurde allerdings nicht die in § 100a Abs. 1 S. 1 Nr. 2 StPO verankerte Prüfung, ob eine Tat im Einzelfall besonders schwer wiegt, in den Entwurf übernommen.

5. Zu Art. 1 Nr. 11 (§ 28 BPolG-E: Besondere Mittel der Datenerhebung)

Die Befugnis, besondere Mittel der Datenerhebung anzuwenden, wird auf Kontakt- und Begleitpersonen ausgeweitet (Abs. 1 Satz 1 Nr. 3). Dies wird nicht begründet. Die Vorschrift kann daher nicht mitgetragen werden.

Der bisherige Absatz 4 (unverzügliche Vernichtung der Unterlagen, die nicht benötigt werden) sollte fortbestehen, falls keine anderweitige Löschregel getroffen wird.

6. Zu Art. 1 Nr. 13 (§ 28b BPolG-E: Einsatz technischer Mittel gegen fernmanipulierte Geräte)

Die Regelung enthält nicht nur eine neue Befugnis zur Abwehr einer Gefahr. Sie enthält auch die Vorfeld-Befugnis, jedwede technischen Mittel zur Erkennung einer Gefahr ohne weitere Voraussetzungen oder Beschränkungen einzusetzen. Dies ist verfassungsrechtlich bedenklich.

Das Regelungsziel nach Satz 1 ist zwar nachvollziehbar. Allerdings kann der Begriff „Fernmanipulierte Geräte“ sehr weit ausgelegt werden. Im Grunde wäre ein Auto im Summon-Modus (autonomes Einparken) auch ein solches Gerät. Drohnen werden heutzutage oft durch Smartphones (also die Steuerungseinheit) ferngesteuert. Ein technisches Mittel gegen eine solche Steuerungseinheit könnte das Übernehmen des entsprechend Smartphones durch Sicherheitslücken in der Funkschnittstelle sein. Welches technische Mittel zum

[7] vgl. BGH, Beschluss vom 08.02.2018, Rn. 5 zu § 100a StPO.

Einsatz kommt, ist vollkommen offen. Damit ist auch offen, welcher Eingriffscharakter und welche Eingriffstiefe vorliegen.

Zudem ist § 28b BPolG-E im Titel 1 „Datenerhebung“ verortet. Sofern eine Datenerhebung mit der Maßnahme nicht verbunden sein soll, ist die systematische Stellung der Regelung zu überdenken. In diesem Zuge muss dann auch berücksichtigt werden, wie eine Erhebung personenbezogener Daten ausgeschlossen werden kann.

Da eine Gefährdung durch fernmanipulierte Geräte potentiell immer eintreten könnte, wäre die hierauf bezogene Detektionstechnik nicht in ihrer Einsatzdauer beschränkt. Sie könnte also immer zum Einsatz kommen. Auch insoweit ist zu prüfen, welche technischen Mittel zum Einsatz kommen sollen und inwieweit eine Erhebung personenbezogener Daten erfolgt.

Mit Satz 2 erhält die Bundespolizei eine Befugnis nicht nur zur Gefahrenabwehr, sondern auch die Möglichkeit, technische Mittel im Vorfeld zu einer Gefahrenerkennung einzusetzen. Jegliche Eingrenzungen, Einschreitschwellen oder auch Verfahrenssicherungen fehlen.

7. Zu Art. 1 Nr. 15 (§ 29 BPolG-E: Weiterverarbeitung personenbezogener Daten)

Zur Problematik des Begriffs „Weiterverarbeitung“ verweise ich auf meine Ausführungen unter Nr. I. 3.

Auch in § 29 Satz 2 BPolG-E des Entwurfs drängt sich die Frage auf, ob und wie die Befugnis der Bundespolizei zur Erledigung besonderer Ersuchen durch Nachrichtendienste (§ 17 Abs. 2 BVerfSchG) mit Verwendung des Begriffs „Weiterverarbeitung“ erweitert wird. Eine Datenverarbeitung sollte weiterhin nur zur Erfüllung eines Ersuchens im Rahmen der grenzpolizeilichen Aufgaben möglich sein.

Satz 3 erscheint insgesamt zu unbestimmt und wird den verfassungsrechtlichen Voraussetzungen der Normenklarheit nicht gerecht. Der Verweis in Satz 3, dass Satz 1 und 2 auch für personenbezogene Daten gelten, die die Bundespolizei ohne Anforderung von Dritten erhalten hat, ist bezüglich seiner Intention und Zielsetzung insgesamt unverständlich. Es ist schon nicht erkennbar, auf welche Voraussetzungen sich der Verweis genau bezieht und welche Wirkung er in der Praxis entfalten soll. Zudem ist die Gesetzesbegründung hierzu völlig unzureichend, da auch dort der Zweck nicht angegeben wird. Außerdem müsste zumindest in der Gesetzesbegründung konkretisiert werden, ob an die von Dritten bekanntgewordenen Daten besondere Anforderungen zu stellen sind, bevor sie an die Nachrichtendienste übermittelt werden, z. B. ob sie zunächst von der Bundespolizei auf ihren Wahrheitsgehalt geprüft werden sollten. Schließlich fehlt es auch an einer Beschreibung, welche Personengruppen unter den Begriff „Dritte“ zu subsumieren sind. Satz 3 sollte gestrichen werden, sofern keine ausreichende Begründung zu Sinn und Zweck der Regelung erfolgt, die erkenntlich macht, für welche Praxisfälle die Vorschrift gedacht ist.

8. Zu Art. 1 Nr. 15 (§ 29a BPolG-E: Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung)

§ 29a Abs. 1 BPolG-E betrifft eine weitere Datenverarbeitung im Rahmen der Zweckbindung. Nach den insoweit einschlägigen Vorgaben des BVerfG (BVerfG NJW 2016, 1781, Rn. 282) ist neben der Nutzung der Daten im selben Aufgabenkreis und dem Schutz derselben Rechtsgüter auch die Nutzung der fraglichen Daten zur Verfolgung oder Verhütung derselben Straftaten erforderlich. Daher ist das "oder" nach "Rechtsgüter" durch ein "und" zu ersetzen.

Bei Datenerhebungen mit einem außerordentlichen Eingriffsgewicht ist nach der Rechtsprechung des BVerfG die Zweckbindung enger auszugestalten (vgl. BVerfG NJW 2016, 1781, Rn. 283). Hier ist jede weitere Nutzung der Daten nur dann zulässig, wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechenden Einschreitschwelle erforderlich ist (BVerfG NJW 2016, 1781, Rn. 283). Dies trifft zumindest auf Datenerhebungen nach §§ 27d, 27e, 28 Abs. 3 und 28 BPolG-E zu. Zudem ist auszuschließen, dass diese Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz erfolgt genutzt werden (BVerfG NJW 2016, 1781, Rn. 283).

In § 29a Abs. 2 BPolG-E wird die zweckändernde Nutzung von Daten geregelt. Mit Abs. 2 soll generell eine „Weiterverarbeitung“ (welcher Art auch immer) ermöglicht werden. Die für die unterschiedliche Gewichtung der Eingriffstiefe jeweils erforderliche Differenzierung führt jedoch zu einer Häufung von unscharfen Begrifflichkeiten. So wird etwa keine konkrete Tatsache gefordert, sondern lediglich ein „Ermittlungsansatz“. Auch der Begriff „übersehbarer Zeitraum“ ist nicht klar umrissen. Gleiches gilt für den Begriff der „drohenden Gefahr“. Schon aufgrund der Abweichung von den tradierten Begrifflichkeiten bedarf es hier näherer Ausführungen in der Gesetzesbegründung. Auch ist unklar, welcher Maßstab für eine Vergleichbarkeit der Schwere von Straftaten und der Bedeutsamkeit der Rechtsgüter gelten soll. Mit dieser Formulierung sollen laut Gesetzesbegründung die Vorgaben des Bundesverfassungsgerichts umgesetzt werden. Zwar nutzt das BVerfG entsprechende Begriffe, führt aber dazu aus, dass der Gesetzgeber hier konkrete Angaben machen muss. Es muss vermieden werden, dass der Normadressat selbst die ihn verpflichtende Norm konkretisieren darf.

Der Regelungsgehalt von § 29a Abs. 3 BPolG-E ist unklar. Die Identifizierung ist kein Selbstzweck, auch nicht zur Datenerhebung. Sofern ein weiterer Zweck verfolgt wird, ist dieser der eigentliche. Im Übrigen ist fraglich, aus welchem Grund der Regelungsgehalt der Verordnung zu § 20 BKAG in den hier betroffenen Fällen stets zutreffen sollen. Hier fehlt eine entsprechende Begründung.

9. Zu Art. 1 Nr. 15 (§ 29b BPolG-E: Daten zu Verurteilten, Beschuldigten, Tatverdächtigen und sonstigen Anlasspersonen)

In § 29b Abs. 1 Nr. 4 BPolG-E wird der Begriff "Anlasspersonen" verwendet und legaldefiniert. Diese Definition ist nicht hinreichend normenklar und bestimmt (Schenke/Graulich/Ruthig/Graulich, 2. Aufl. 2018, BKAG § 18 Rn. 6). Zudem enthält sie die vom Bundesverfassungsgericht (im Zusammenhang mit § 20g Abs. 1 Nr. 2 BKAG a.F.) bereits für nicht hinreichend normenklar erachtete Formulierung einer Vorfeldkompetenz (BVerfG NJW 2016, 1781, Abs. 162 ff., 165).

§ 29b Abs. 3 BPolG-E berechtigt die Bundespolizei zur Verarbeitung von Daten zu sogenannten Prüffällen, bei denen noch nicht feststeht, ob die betreffende Person zu dem zu speichernden Personenkreis zählt.

Zwar sieht die Vorschrift eine Zweckbegrenzung sowie eine maximale Speicherfrist vor. Dies ändert jedoch nichts an der Tatsache, dass eine automatisierte Sammlung solcher Fälle grundsätzlich abzulehnen ist. Hier werden Daten zu Personen in Vorsorgedateien gespeichert und weiter verarbeitet, gegen die im Zeitpunkt der Speicherung rechtlich keine Negativprognose festgestellt werden kann. Die Speicherung ermöglicht eine „Anreicherung“ der Daten mit dem Ziel, eine Negativprognose in Zukunft begründen zu können. Die Daten werden hier zur Verdachtsgenerierung auf Vorrat gespeichert. Auch eine bloß befristete Speicherung löst das Problem nicht. Die Ausweitung auf Prüffälle ist verfassungsrechtlich nicht hinnehmbar

10. Zu Art. 1 Nr. 15 (§ 29c BPolG-E: Daten zu anderen Personen)

Abs. 2 betrifft ebenfalls Prüffälle. Die Problematik bei Prüffällen habe ich bereits unter Nr. 9 dargestellt. Diese Problematik verschärft sich, weil hier Daten zu Personen gespeichert werden, die Opfer einer zukünftigen Straftat werden könnten oder als Zeugen einer zukünftigen Strafverfolgung fungieren könnten. Das bisherige Erfordernis der Einwilligung durch die betroffene Person (vgl. § 29 Abs. 3 S. 3 BPolG), das im Gesetzentwurf gestrichen worden ist, sollte wieder eingefügt werden.

11. Zu Art. 1 Nr. 15 (§ 29e PolG-E: Kennzeichnung)

Die Kennzeichnung personenbezogener Daten soll der Umsetzung des Grundsatzes der hypothetischen Datenneuerhebung dienen. Der Grundsatz geht von einer Zweckänderung aus. Hierfür ist die Kenntnis über den Zweck unabdingbar. Auch diese Information muss in Bezug auf das konkrete Datum verfügbar sein und sollte daher in dem Gesetzentwurf ergänzt werden.

Bei nachträglichen Kennzeichnungen nach Absatz 4 ist zudem sicherzustellen, dass die Kennzeichnung auch den Stellen mitgeteilt werden, denen die Daten übermittelt wurden.

12. Zu Art. 1 Nr. 17 (§ 31a BPolG-E: Ausschreibungen von Personen und Sachen … im Schengener Informationssystem)

Die vorgesehene Regelung des § 31a BPolG-E sieht eine Erweiterung der Befugnis der Bundespolizei vor, gezielte und verdeckte Kontrollen oder Ermittlungsanfragen im Schengener Informationssystem auszuschreiben, also über die Grenzen Deutschlands hinaus. Hierbei handelt es sich um erhebliche Eingriffe in das Grundrecht auf informationelle Selbstbestimmung.

Zwar könnte der Eindruck entstehen, dass dies auf bestimmte Aufgaben der Bundespolizei beschränkt ist, letztendlich sind aber alle Aufgaben der Bundespolizei von der Norm umfasst. Dabei wird kaum begründet, warum die Bundespolizei solch weitreichende Befugnisse für alle ihre Aufgaben, insbesondere solche ohne grenzüberschreitenden Bezug, benötigt.

Insgesamt könnte die Bundespolizei hiernach in großem Umfang Ausschreibungen durchführen, die die Übermittlung auch von besonders schützenswerten personenbezogenen Daten über die nationale Grenze hinaus ermöglichen. Durch die Ausschreibung im gesamten Schengenraum erhalten weit mehr Personen die Möglichkeit der Kenntnisnahme. Die Eingriffstiefe gerade für verdeckte Kontrollen geht daher weit über die der Ausschreibung nach § 31 BPolG hinaus. Das nationale Schutzniveau wird unterlaufen. Hier fehlt eine Zuständigkeitskonzentration auf die Leitung der zuständigen Bundespolizeibehörde (vgl. § 31 Abs. 3 BPolG). Es fehlt auch eine ausreichend kurze Prüffrist. In der aktuellen Form wäre pauschal ein Jahr anzunehmen; schon § 31 Abs. 4 BPolG sieht hier aber eine mehrstufige Aussonderungsprüffrist vor (zunächst 3 Monate, Verlängerung auf max. 6 Monate, darüber hinaus mit richterlicher Anordnung). Artikel 53 Abs. 5 Verordnung (EU) 2018/1862 ermöglicht ausdrücklich kürzere Prüffristen. Angesichts der Reichweite von Ausschreibungen im SIS ist die Ermöglichung von verdeckten Ausschreibungen ohne mindestens vergleichbare Schutzmechanismen unverhältnismäßig.

Gegen die derzeitige Ausgestaltung der Norm bestehen somit erhebliche datenschutzrechtliche Bedenken.

13. Zu Art. 1 Nr. 19 (§ 32 BPolG-E: Übermittlung personenbezogener Daten im innerstaatlichen Bereich)

§ 32 Absatz 3 PolG-E ergänzt die Übermittlungsbefugnis an andere nicht-öffentliche Stellen um einen zusätzlichen Übermittlungsgrund, nämlich die Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl. Zum Hintergrund wird in der Gesetzesbegründung erläutert, dass Daten der Bundespolizei durch die Zentrale Informationsstelle Sporteinsätze (ZIS) an nicht-öffentliche Stellen (insbesondere an den Deutschen Fußball-Bund) z. B. nach dem Polizeirecht von Nordrhein-Westfalen übermittelt werden. Mit einer entsprechenden Ergänzung von Absatz 3 werde ein Gleichlauf mit nordrheinwestfälischen

Vorschriften hergestellt und damit der Vorwurf einer Umgehung bundespolizeilicher Regelungen entkräftet.

Diese Begründung trägt jedoch nicht. Hier wird eine neue, sehr weitreichende generalklauselartige Übermittlungsbefugnis geschaffen, die lediglich durch eine Erheblichkeitsschwelle beschränkt ist.

Zunächst bedarf es, um eine sehr spezifische Konstellation im Sportbereich zu regeln, eines Regelungsbedarfs. Eine weitergehende Erforderlichkeit, insbesondere umfassende Defizite der bisherigen Regelung jenseits der angesprochenen Konstellation, sind nicht dargelegt. Dementsprechend ist die Erforderlichkeit nicht nachvollziehbar.

Darüber hinaus ist die geschilderte Praxis der Datenübermittlung an die ZIS schon grundsätzlich unzulässig, selbst wenn sie nicht nur zum Zwecke der Durchleitung an eine nichtöffentliche Stelle wie beispielsweise den Deutschen Fußball-Bund erfolgt, sondern in eine umfassende polizeiliche Bewertung einfließt. Die in der ZIS bearbeiteten Sachverhalte greifen über den Bereich NRW hinaus und können daher aus hiesiger Sicht nicht landesrechtlich geregelt werden.

Nach § 32 Absatz 10 PolG-E darf die Bundespolizei zur Erfüllung ihrer Aufgaben auch außerhalb des polizeilichen Informationsverbunds nach § 2 Abs. 3 BKAG an einem polizeilichen Datenverbund mit anderen Landes- und Bundesbehörden teilnehmen, der auch eine automatisierte Datenübermittlung ermöglicht.

Die Regelung impliziert die Zulässigkeit eines polizeilichen Datenverbundes außerhalb des BKA-Verbunds. Dieses Ziel wird auch mit einem Teilprojekt des Gesamtprojekts „Polizei 2020“ verfolgt. Es handelt sich um den Proof of Concept (PoC) Datenkonsolidierung, mit dem ein Datenverbund unterhalb der im BKAG festgelegten Schwellen für die Polizeibehörden der Länder errichtet werden soll. Das BKA soll als Auftragsverarbeiter der Länder fungieren. Gegen diesen PoC habe ich gegenüber BMI von Beginn an meine erheblichen datenschutzrechtlichen Einwände geäußert (vgl. 28. Tätigkeitsbericht des BfDI zum Datenschutz 2019, 6.3 Polizei 2020, S. 50).

Vor diesem Hintergrund mutet es umso erstaunlicher an, dass mit § 32 Absatz 10 BPolG-E nunmehr eine bundesrechtliche Grundlage für die Teilnahme der Bundespolizei an eben diesem Datenverbund geschaffen werden soll, obgleich auf Bundesebene von einer Länderzuständigkeit ausgegangen wird.

Die Errichtung und der Betrieb von Verbunddateien im Polizeibereich richtet sich nach § 29 BKAG und werden vom BKA als eigene Aufgabe betrieben. Diese Regelung ist abschließend und enthält Schwellen, die für die beteiligten Behörden der Länder und des Bundes gleichermaßen gelten. Für die Bundespolizei gelten die Vorgaben für den Informationsverbund nach § 29 Abs. 4 S. 2 i. V. m. Abs. 3 Nr. 2 BKAG. Eine Verbunddatei außerhalb dieser Schwellen – wie sie mit § 32 Abs. 10 BPolG-E beabsichtigt wird – würde die abschließenden Regelungen des BKAG ad absurdum führen. Die gesetzliche Vorgaben der §§ 29 ff. BKAG

würden umgangen werden. § 32 Abs. 10 BPolG-E steht somit im Widerspruch zu den gesetzlichen Vorgaben des BKAG.

Angesichts der ausschließlichen Gesetzgebungskompetenz des Bundes nach Art. 73 Abs. 1 Nr. 10 und Art. 87 Abs. 1 Satz 2 GG entfaltet das BKAG nach Art. 71 GG zudem eine Sperrwirkung für die Landesgesetzgeber.

Die Vorhaltung zweier oder mehrerer bundesweiter „Datenverbünde“ in Deutschland wäre zudem mit dem Verhältnismäßigkeitsgrundsatz nicht zu vereinbaren. Dies gilt insbesondere für die Verarbeitung personenbezogener Daten außerhalb der Verbundrelevanz im Sinne des § 30 BKAG.

Ich bitte dringend, die geplante Regelung des § 32 Abs. 10 BPolG-E ersatzlos zu streichen.

14. Zu Art. 1 Nr. 20 (§ 32a BPolG-E: Übermittlung personenbezogener Daten an Mitgliedstaaten der Europäischen Union und Schengen assoziierte Staaten)

Neben der Übermittlung an EU-Mitgliedstaaten sollen auch Übermittlungen an Schengen assoziierte Staaten möglich sein. Es ist gesondert zu begründen, dass die Schweiz über Schengen-Sachverhalte hinaus wie ein EU-Mitgliedsstaat behandelt werden kann. Dies müsste aus dem Assoziierungsabkommen hervorgehen und sollte in der Gesetzesbegründung nachgewiesen werden.

15. Zu Art. 1 Nr. 28 (§ 41a BPolG-E: Bild- und Tonüberwachung von Gewahrsamsräumen)

Die Vorschrift soll dem Schutz sowohl der in Gewahrsam genommenen Personen als auch der Polizeibeamtinnen und -beamten dienen. Für einen effektiven Schutz der in Gewahrsam genommenen Person sollte dieser Person ebenfalls die Möglichkeit eingeräumt werden, die Aufnahme selbst durch eine technische Einrichtung zu initiieren.

Zur Verhinderung des Gefühls einer ständigen Beobachtung und zur Berücksichtigung der Barrierefreiheit sollte ein kumulativ optisches und akustisches Signal vorgesehen werden.

III. Erfüllungsaufwand beim BfDI

Da zu dem vorliegenden Gesetzentwurf keine Ressortbesprechung durchgeführt worden ist, konnte der Erfüllungsaufwand des BfDI noch nicht in die Diskussion eingebracht werden. Durch die neuen Kompetenzen der Bundespolizei und die den BfDI betreffenden neuen Pflichtkontrollen nach § 37 Abs. 1 BPolG-E entsteht ein erheblicher Mehraufwand für den BfDI. Aufgrund vergleichbarer Erfahrungen in anderen Bereichen gehe ich davon aus, dass insoweit mindestens eine Personalverstärkung von 2 Stellen im höheren Dienst und 2 Stellen im gehobenen Dienst in Ansatz zu bringen ist.