VON BOETTICHER
RECHTSANWÄLTE

VERMERK

Akte: 0443/13
Von: Matthias Bergt,
VON BOETTICHER Rechtsanwälte Partnerschaftsgesellschaft mbB
Datum: 24. Februar 2014
Betr.: Zulässigkeit der Veröffentlichung eines Transparenzberichts

---

A. Aufgabenstellung

Posteo e.K. beabsichtigt, einen Transparenzbericht zu Überwachungsmaßnahmen von Sicherheitsbehörden – konkret Bestandsdatenabfragen, Verkehrsdatenabfragen, Überwachung und Aufzeichnung der Telekommunikation und Herausgabeverlangen für E-Mail-Postfächer – zu veröffentlichen. Wir sind mit der Prüfung beauftragt, ob und wenn ja unter welchen Bedingungen die Veröffentlichung eines solchen Transparenzberichts zulässig ist.

Nicht Gegenstand der Prüfung sind Überwachungsmaßnahmen/Auskunftsersuchen nach Landesrecht.

B. Kurzzusammenfassung

Bitte beachten Sie, dass die Lektüre dieser Kurzzusammenfassung nicht die Lektüre des vollständigen Gutachtens ersetzen kann. Schlussfolgerungen mit rechtlichen Konsequenzen sollten ausschließlich aus dem vollständigen Gutachten gezogen werden.

Zusammenfassend ist festzuhalten, dass die Veröffentlichung eines Transparenzberichts zulässig ist, soweit dadurch keine Gefährdung von Ermittlungserfolgen oder eine Offenbarung von laufenden Ermittlungen zu befürchten ist. Die Gefährdung von Ermittlungen der Sicherheitsbehörden ist ausgeschlossen, wenn sich die veröffentlichten Angaben im Rahmen des Umfangs der Berichte des Bundesamts für Justiz nach §§ 100b Abs. 5, 6, 100g Abs. 4 StPO bzw. der Berichte der G10-Kommission und des Gremiums nach § 23c Abs. 8 des Zollfahndungsdienstgesetzes halten.

Dies bedeutet, dass die folgenden Angaben zulässig sind:

I. bei strafprozessualer Telekommunikationsüberwachung nach § 100a StPO bzw. § 20l Abs. 1 BKAG:
   (1) Anzahl der TK-Überwachungsanordnungen nach § 100a StPO, unterschieden nach Erst- und Folgeanordnungen,
   (2) zugrunde liegende Anlassstraftaten;

II. bei strafprozessualer Beschlagnahme von Postfächern:
   (1) Anzahl der Beschlagnahmen auf Basis von § 94 StPO,
   (2) Anzahl der Beschlagnahmen auf Basis von § 99 StPO,
   (3) Anzahl der Beschlagnahmen auf Basis von § 100a StPO,
   (4) zugrunde liegende Anlassstraftaten,
   (5) Angabe, auf welchen Zeitraum sich die Beschlagnahme bezog;

III. bei strafprozessualer Bestandsdatenabfrage nach § 100j StPO:
   (1) Anzahl der Bestandsdatenabfragen auf Basis von § 100j StPO,
   (2) zugrunde liegende Anlassstraftaten.

IV. bei strafprozessualer Verkehrsdatenabfrage nach § 100g StPO bzw. § 20m Abs. 1 BKAG:
   (1) Anzahl der Verkehrsdatenabfragen, unterschieden nach Erst- und Folgeanordnungen,
   (2) zugrunde liegende Anlassstraftaten,
   (3) Angabe, auf welchen Zeitraum sich die Verkehrsdatenabfrage bezog,
   (4) Erfolgsquote.

V. bei Telekommunikationsüberwachung, Verkehrsdatenabfrage und E-Mail-Herausgabeverlangen durch Geheimdienste:
   (1) Anzahl der TK-Überwachungsanordnungen der Geheimdienste, unterschieden nach Erst- und Folgeanordnungen,
   (2) Anzahl der E-Mail-Postfach-Herausgabeverlangen der Geheimdienste,
   (3) Anzahl der Verkehrsdatenabfragen der Geheimdienste, unterschieden nach Erst- und Folgeanordnungen,

   aufgeteilt nach dem jeweiligen Geheimdienst und der jeweils angewendeten Rechtsgrundlage;

VI. bei Bestandsdatenabfrage von Geheimdiensten:
   (1) Anzahl der Bestandsdatenabfragen der Geheimdienste,
   (2) aufgeteilt nach den verschiedenen Geheimdiensten;

VII. bei TK-Überwachung nach § 23a Abs. 1 ZFdG und Verkehrsdatenabfrage nach § 23g Abs. 1 ZfdG
   (1) Anzahl der TK-Überwachungsanordnungen nach § 23a Abs. 1 ZFdG, unterschieden nach Erst- und Folgeanordnungen,
   (2) Anzahl der Verkehrsdatenabfragen nach § 23g Abs. 1 ZFdG, unterschieden nach Erst- und Folgeanordnungen,
   (3) zugrunde liegende Anlassstraftaten.

Ein Weniger an Informationen ist natürlich jederzeit zulässig.

Der Transparenzbericht sollte sich mindestens auf ein Quartal beziehen, besser auf ein Halbjahr oder Jahr.

Inhaltsverzeichnis

C. Im Einzelnen

Nach allgemeinen Grundsätzen ist die Veröffentlichung der Daten über Anfragen von Sicherheitsbehörden rechtmäßig, sofern dies nicht gesetzlich untersagt ist. Da der Transparenzbericht keine dem Fernmeldegeheimnis oder dem Datenschutzrecht unterliegenden Angaben enthalten würde, können die diesbezüglichen Vorschriften bei der Prüfung außer Betracht bleiben. Da erst im Nachhinein statistische Angaben veröffentlicht werden sollen, besteht auch kein Risiko, eine Strafvereitelung (§ 258 StGB) zu begehen.

Folgend wird für die verschiedenen Arten von Überwachungsmaßnahmen geprüft, ob und ggf. welche gesetzlichen Regelungen einer Veröffentlichung entgegenstehen.

I. Telekommunikationsüberwachung nach § 100a StPO bzw. § 20l Abs. 1 BKAG

Die laufende Überwachung der Telekommunikation ist den Strafverfolgungsbehörden nach §§ 100a, 100b StPO gestattet. § 110 TKG regelt die Umsetzung von Überwachungsmaßnahmen und enthält insbesondere die Ermächtigung an die Bundesregierung, eine Rechtsverordnung über die technischen Anforderungen und die organisatorischen Eckpunkte zu erlassen; auf dieser Basis wurde die Verordnung über die technische und organisatorische Umsetzung von Maßnahmen der Überwachung der Telekommunikation (TKÜV) erlassen.

Das Bundeskriminalamt hat zudem nach § 20l Abs. 1 BKAG die Möglichkeit zur Telekommunikationsüberwachung. Die Mitwirkungspflicht des Providers ergibt sich aus § 20l Abs. 5 BKAG. Eine gesonderte Verschwiegenheitspflicht enthält das BKAG nicht, so dass es hier nicht weiter zu beachten ist.

1. Gesetzliche Grundlagen einer Verschwiegenheitspflicht

a) Verschwiegenheitspflicht nach § 15 TKÜV

§ 15 TKÜV enthält in Abs. 1 das Verbot, Informationen über die Art und Weise der Umsetzung der Telekommunikationsüberwachung Unbefugten zugänglich zu machen. In Abs. 2 stellt § 15 TKÜV Schutzpflichten auf, die zur Geheimhaltung der Informationen aus der Telekommunikationsüberwachung vom Telekommunikationsdienstleister zu erfüllen sind.

Die TKÜV regelt unter anderem die Anforderungen für technische Einrichtungen zum Zweck der Umsetzung der in §§ 100a, 100b StPO geregelten Überwachung und Aufzeichnung der Telekommunikation und der Erteilung von Auskünften. Die TKÜV erfasst somit richtigerweise weder die Sicherstellung und Beschlagnahme von E-Mail-Postfächern (vgl. hierzu Meyer-Goßner, StPO, 56. Auflage 2013, § 100a Rn. 6b f.; § 94 Rn. 16a, 19a) noch die Überwachung und Aufzeichnung von Verkehrsdaten nach § 100g StPO. Folglich betrifft die Verschwiegenheitspflicht des § 15

TKÜV lediglich die Mitteilung von Informationen über die Telekommunikationsüberwachung im Sinne des § 100a StPO.

b) Verschwiegenheitspflicht nach § 17 Abs. 1 G10-Gesetz

§ 17 Abs. 1 des G10-Gesetzes lautet:

> *„Wird die Telekommunikation (...) nach den §§ 100a, 100b der Strafprozessordnung überwacht, darf diese Tatsache von Personen, die Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, anderen nicht mitgeteilt werden."*

Das Mitteilungsverbot ist nach § 18 G10-Gesetz strafbewehrt.

2. Umfang der Verschwiegenheitspflicht

a) § 15 Abs. 1 TKÜV

§ 15 TKÜV enthält in Abs. 1 das Verbot, Informationen über die Art und Weise der unternehmensinternen technischen Umsetzung der Telekommunikationsüberwachung Unbefugten zugänglich zu machen. Die Begründung zum Verordnungsentwurf (http://www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/20011025UllrichBegruendungTKUeV.html, S. 12) führt dazu aus:

> *„Wenngleich die der technischen Umsetzung von Überwachungsmaßnahmen zugrunde liegenden technischen Vorgänge durch die entsprechenden internationalen technischen Standards als allgemein bekannt anzusehen sind, soll der Verpflichtete unternehmensinterne Informationen, wie derartige Maßnahmen in seiner Telekommunikationsanlage umgesetzt werden, Unbefugten nicht zugänglich machen."*

Die Veröffentlichung einer Statistik über die Anfragen der Sicherheitsbehörden berührt diese Verschwiegenheitspflicht nicht, so dass sich die Frage nicht stellt, ob die Vorschrift überhaupt den Rahmen ihrer gesetzlichen Ermächtigungsnorm einhält.

b) § 15 Abs. 2 TKÜV

§ 15 Abs. 2 Satz 1 TKÜV regelt die Schutzpflicht des Telekommunikationsunternehmens, die mit der Überwachung im Zusammenhang stehenden Informationen vor unbefugtem Zugriff Dritter zu bewahren.

Somit muss bereits bezweifelt werden, dass sich aus § 15 Abs. 2 TKÜV überhaupt eine Verschwiegenheitspflicht ergibt, auch wenn die Begründung zum TKÜV-Entwurf dies so sehen will:

> *„Über durchgeführte Überwachungsmaßnahmen hat der Verpflichtete Stillschweigen zu wahren."*

Dies ergibt sich nicht hinreichend aus dem Wortlaut; vielmehr geht es um den „Schutz", „insbesondere hinsichtlich unbefugter Kenntnisnahme", d.h. technische Anforderungen, wie sie auch der zu Grunde liegende § 110 Abs. 2 Nr. 1 lit. a) TKG als zulässigen Regelungsinhalt benennt.

Nach der neueren Rechtsprechung ist es jedoch der Wortlaut einer Vorschrift, der letztlich über ihren Bedeutungsgehalt entscheidet, nicht die Ansichten der Entwurfsverfasser, was sie mit der Vorschrift ausdrücken wollten, wenn sich diese Ansichten nicht im Gesetzeswortlaut niedergeschlagen haben (BGH, Urt. v. 19.4.2012 – I ZB 80/11, NJW 2012, 2958, 2961, Rn. 30 – Alles kann besser werden). Möglicherweise ist aber auch der Satz in der Entwurfsbegründung nur als Hinweis auf eine ohnehin bestehende Rechtslage zu verstehen.

Würde man entgegen der hier vertretenen Ansicht eine echte Verschwiegenheitspflicht annehmen, hätte die TKÜV (als untergesetzliches Recht) jedenfalls unzulässig den Rahmen verlassen, den § 110 Abs. 2 Nr. 1 lit. a) TKG vorgibt. § 15 Abs. 2 TKÜV würde dann gegen den Vorbehalt des Gesetzes und das Bestimmtheitsgebot verstoßen (Art. 80 Abs. 1 Satz 2 GG).

Denn eine Ermächtigung zum Verbot der Weitergabe von Informationen über Überwachungsmaßnahmen lässt sich § 110 TKG – auch unter Berücksichtigung der Rechtsprechung des Bundeverfassungsgerichts, dass Inhalt, Zweck und Ausmaß der Verordnungsermächtigung auch durch Auslegung ermittelt werden können und nicht ausdrücklich im Gesetz genannt werden müssen (BVerfG, Beschl. v. 12.11.1958 – 2 BvL 4/56, NJW 1959, 475, 475 f.) – nicht mit der erforderlichen Klarheit entnehmen.

Auch in der Geschichte des § 110 Abs. 2 TKG gibt es keine Hinweise darauf, dass die Vorschrift etwas anderes regeln wollte als die rein technische Umsetzung der Überwachungsmaßnahmen:

Die Verordnungsermächtigung zur Regelung der technischen Umsetzung von Überwachungsmaßnahmen wurde erstmalig im Rahmen der Postreform II als § 10b Satz 2 des Gesetzes über Fernmeldeanlagen (FAG) eingeführt. Die Regelung geht auf die Stellungnahme des Innenausschusses vom 23.6.1994 zurück (vgl. BT-Drs. 12/8060, S. 172), die vom Ausschuss für Post und Telekommunikation und letztlich vom Bundestag übernommen wurde. Eine Begründung für die Gesetzesänderung findet sich in den Materialien nicht (vgl. BT-Drs. 12/8060, S. 197). Die Vorschrift stellte jedoch bereits damals ausschließlich auf technische Aspekte ab:

> *„Die Bundesregierung wird ermächtigt, durch Rechtsverordnung die technische Umsetzung von Überwachungsmaßnahmen in den Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, zu regeln."*

Die Vorschrift wurde sodann im Wesentlichen in § 88 TKG 1996 = § 85 TKG-E 1996 übernommen. § 85 Abs. 2 Satz 2 TKG-E 1996 lautete:

> *„Die Bundesregierung wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf,*
> *1. die technische und organisatorische Umsetzung von Überwachungsmaßnahmen in diesen Telekommunikationsanlagen und*
> *2. das Genehmigungsverfahren*
> *zu regeln.“*

Die Gesetzesbegründung spricht ausschließlich davon, dass „die *technische* Umsetzung der gesetzlichen Überwachungsmaßnahmen“ durchzusetzen sei, dass durch eine entsprechende „*technische* Gestaltung der zu treffenden Vorkehrungen“ eine Genehmigung zu erhalten sei und dass bei den „*technischen* Vorgaben“ auf Standards zu setzen sei (BT-Drs. 13/3609, S. 54). Die Begründung hält zudem fest:

> *„Nach Satz 2 können den Betreibern von Telekommunikationsanlagen – wie bisher nach § 10b Satz 2 FAG – durch Rechtsverordnung Vorgaben gemacht werden, wie diese ihre Verpflichtung, die Überwachung und Aufzeichnung des Fernmeldeverkehrs zu ermöglichen, zu erfüllen haben.“*

Es ging dem Gesetzgeber demnach ausschließlich um eine Ermächtigung, das „Wie“ der technischen Umsetzung von Überwachungsmaßnahmen durch Rechtsverordnung genauer zu regeln.

Bis zum Inkrafttreten des TKG 2004 war im Gesetz ausschließlich von „technischen“ Aspekten die Rede. § 108 Abs. 2 TKG-E 2004 (BR-Drs. 755/03, S. 55), der im Wesentlichen unverändert als § 110 Abs. 2 TKG 2004 Gesetz geworden ist, bringt erstmalig auch die „organisatorischen Eckpunkte“ ins Spiel:

> *„Die Bundesregierung wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf*
> *1. Regelungen zu treffen*
> *a) über die grundlegenden technischen Anforderungen und die organisatorischen Eckpunkte für die Umsetzung von Überwachungsmaßnahmen einschließlich der Umsetzung von Überwachungsmaßnahmen durch einen von dem Verpflichteten beauftragten Erfüllungsgehilfen,*
> *b) über den Regelungsrahmen für die Technische Richtlinie nach Absatz 3,*
> *c) für den Nachweis nach Absatz 1 Satz 1 Nr. 4 und*
> *d) für die nähere Ausgestaltung der Duldungsverpflichtung nach Absatz 1 Satz 1 Nummer 5 sowie*
> *2. zu bestimmen,*

a) in welchen Fällen und unter welchen Bedingungen vorübergehend auf die Einhaltung bestimmter technischer Vorgaben verzichtet werden kann,
b) dass die Regulierungsbehörde aus technischen Gründen Ausnahmen von der Erfüllung einzelner technischer Anforderungen zulassen kann und
c) bei welchen Telekommunikationsanlagen und damit erbrachten Diensteangeboten aus grundlegenden technischen Erwägungen oder aus Gründen der Verhältnismäßigkeit abweichend von Absatz 1 Satz 1 Nr. 1 keine technischen Einrichtungen vorgehalten und keine organisatorischen Vorkehrungen getroffen werden müssen."

Hierzu hält die Gesetzesbegründung (BR-Drs. 755/03, S. 126) fest:

> *„Die Wortwahl „grundlegenden technischen Anforderungen" soll verdeutlichen, dass die für die technische Entwicklung unabdingbar erforderlichen detaillierten Festlegungen nicht in der Rechtsverordnung erfolgen können, sondern in der technischen Rechtlinie nach Absatz 3; durch die Wörter „organisatorische Eckpunkte" wird klargestellt, dass die Rechtsverordnung nicht grundlegend in die Organisationsfreiheit der Unternehmen eingreift, sondern lediglich Vorgaben für unabweisbare Forderungen der Strafverfolgungs- und Sicherheitsbehörden macht, z.B. Vorgaben zur Erreichbarkeit der Unternehmen, der Zulässigkeit der organisatorischen Ausgliederung der mit der Umsetzung von Überwachungsmaßnahmen verbundenen Aufgaben oder zu Übermittlungsmöglichkeiten von Anordnungen."*

Wie auch die Überschrift des § 108 TKG-E 2004 = § 110 TKG 2004:

> *„Technische Umsetzung von Überwachungsmaßnahmen"*

zeigt, ging es dem Gesetzgeber somit weiterhin ausschließlich darum, in der TKÜV technische Fragen zur Durchführung der Überwachung zu regeln, nicht aber materielle Verbotstatbestände zu ermöglichen. Die Entscheidung, ob Überwachungsmaßnahmen geheim zu halten sind, ist aber grundsätzlicher Natur und daher vom parlamentarischen Gesetzgeber selbst zu treffen.

In der Folge in § 110 TKG hinzugekommen ist nur die „Erteilung von Auskünften", die hinsichtlich der hier entscheidenden Frage jedoch keine Auswirkungen hat.

Somit bleibt festzuhalten, dass § 15 Abs. 2 TKÜV den zulässigen Rahmen der Ermächtigungsgrundlage verlassen würde, wollte man die Norm dahingehend auslegen, dass sie eine Verschwiegenheitspflicht regelt.

Schließlich enthalten die Berichte nach §§ 100b Abs. 5, 6, 100g Abs. 4 StPO ausführliche Angaben hinsichtlich der Anzahl und Grundlagen der Überwachungsanordnungen, so dass der Schutz dieser Informationen durch § 15 Abs. 2 Satz 2 TKÜV offensichtlich nicht beabsichtigt sein kann.

c) § 17 Abs. 1 G10-Gesetz

§ 17 Abs. 1 G10-Gesetz greift zunächst nur ein, wenn die Telekommunikation tatsächlich überwacht wird. Eine Negativ-Aussage hinsichtlich Überwachungsmaßnahmen ist somit zulässig.

Im Fall einer TK-Überwachung darf nach § 17 Abs. 1 G10-Gesetz „diese Tatsache" nicht mitgeteilt werden. Legt man diese Vorschrift streng nach ihrem Wortlaut weit aus, könnte man zu dem Ergebnis kommen, dass jede bejahende Aussage zum Vorliegen einer TKÜ unzulässig wäre. Andererseits ist diese Auslegung nicht zwingend; der Wortlaut lässt auch das Verständnis zu, dass es nur um konkrete Überwachungsmaßnahmen geht, was insbesondere auch unter Berücksichtigung des Wortlauts der Abs. 2 und 3 naheliegend ist, die auf „die Aushändigung von Sendungen" und „ein Auskunftsersuchen oder eine Auskunftserteilung" – und damit Einzelfälle – abstellen und nicht wie Abs. 1 dies – wohl aus sprachlichen Gründen – tut allgemein auf „die Telekommunikation".

Ein allgemeines Verbot jeglicher Aussagen zu Überwachungsmaßnahmen ist offensichtlich auch nicht die Intention des Gesetzgebers gewesen. Vielmehr ging es darum, eine Gefährdung der Ermittlungen durch einzelfallbezogene Angaben zu vermeiden; es geht um die Frage, ob eine Kennung (z.B. E-Mail-Postfach) Gegenstand einer Überwachungsmaßnahme ist. Die Gesetzesbegründung (BT-Drs. 13/5753, S. 7) hält dazu fest:

> *„Die Überwachung nach dem G10 ist nur dann effektiv durchführbar, wenn die davon Betroffenen nicht vorzeitig über die Maßnahme informiert werden."*

Ansonsten wäre die zunächst vorhandene Regelung, dass die anbieterbezogene Überwachungsstatistik Dritten nicht bekannt gemacht werden darf (§ 85 Abs. 5 Satz 3 TKG-E 1996 [BT-Drs. 13/3609, S. 27] bzw. § 88 Abs. 5 Satz 3 TKG 1996 bzw. § 110 Abs. 8 Satz 3 TKG 2004) überflüssig gewesen. Es ist nicht davon auszugehen, dass der Gesetzgeber ein Gesetz ohne Anwendungsbereich erlässt. Auch wären bei einer solchen weiten Auslegung die Berichte nach §§ 100b Abs. 5, 6, 100g Abs. 4 StPO nur deswegen zulässig, weil das Gesetz sie explizit anordnet. Die gesetzlichen Regelungen wären damit in sich unschlüssig, weil eine einzige Handlung einerseits verboten und andererseits erlaubt wäre, ohne dass es für die Unterscheidung einen sinnvollen Grund gäbe.

Das Verbot der Bekanntgabe der betreiberinternen Statistik im TKG wurde zum 1.1.2008 gestrichen. Die Nachfolgeregelung in § 100b Abs. 5 und 6 StPO sieht kein Verbot mehr vor, sondern im Gegenteil die Veröffentlichung von Statistiken über Überwachungsmaßnahmen. Zwar ist die Statistik-Pflicht mittlerweile von den Providern auf die Strafverfolgungsbehörden übergegangen. Hätte der Gesetzgeber aber die bisherigen betreiberinternen Statistiken verbieten wollen, wäre eine entsprechende ausdrückliche Regelung oder jedenfalls ein Hinweis in der Gesetzesbegründung, dass sich trotz der Aufhebung von § 110 Abs. 8 TKG nichts am – wenn es denn be-

standen hätte – Verbot der Bekanntgabe einer Überwachungsstatistik ändert, zu erwarten gewesen. An beidem fehlt es aber (vgl. nur BT-Drs. 16/5846, S. 48 und 68).

d) § 15 Abs. 2 TKÜV und § 17 Abs. 1 G10-Gesetz

Außerdem belegt die im Jahr 2005 eingeführte Regelung des § 15 Abs. 2 Satz 3 TKÜV, dass nach der zentralen gesetzgeberischen Motivation nur die Mitteilung einzelfallbezogener Informationen über Überwachungsmaßnahmen verhindert werden soll. Denn nach der Verordnungsbegründung (BR-Drs. 631/05, S. 32) „verdeutlicht" § 15 Abs. 2 Satz 3 TKÜV, dass eine nicht einzelfallbezogene Weitergabe statistischer Daten über Überwachungsmaßnahmen zulässig ist. Wäre § 17 Abs. 1 G10-Gesetz weit auszulegen, würde es sich einerseits nicht um eine „Verdeutlichung" handeln. Andererseits wäre § 15 Abs. 2 Satz 3 TKÜV nichtig wegen Verstoßes gegen den Vorrang des Gesetzes (hier § 17 Abs. 1 G10-Gesetz), weil § 15 Abs. 2 Satz 3 TKÜV als reine Rechtsverordnung etwas erlauben würde, was das Gesetz verbietet.

3. Ergebnis

Angaben zu einzelnen TK-Überwachungsmaßnahmen dürfen nicht gemacht werden und sind strafbar, §§ 17 Abs. 1, 18 G10-Gesetz, weil diese Ermittlungsmaßnahmen konkret gefährden würden. Durch die Veröffentlichung statistischer Angaben ist eine Gefährdung konkreter Ermittlungen grundsätzlich nicht zu befürchten. Zulässig sind daher statistische Zusammenfassungen nach dem Muster des § 100b Abs. 5 und 6 StPO.

Im Transparenzbericht zulässig ist also die Angabe
(1) der Anzahl der TK-Überwachungsanordnungen nach § 100a StPO, unterschieden nach Erst- und Verlängerungsanordnungen und
(2) der jeweils zugrunde liegenden Anlassstraftat nach Maßgabe der Unterteilung in § 100a Abs. 2 StPO.

II. Strafprozessuale Beschlagnahme von Postfächern

1. Offene Beschlagnahme

Die Beschlagnahme nach § 94 StPO ist auch auf die Beschlagnahme von E-Mails beim Provider anwendbar (BVerfG, Beschl. v. 16.6.2009 – 2 BvR 902/06, MMR 2009, 673, 675, Rn. 55). Es handelt sich dabei um eine grundsätzlich offene Ermittlungsmaßnahme.

Es besteht daher kein Grund, Angaben über erfolgte Postfach-Beschlagnahmen auf der Grundlage von § 94 StPO zurückzuhalten. Diese können also im Transparenzbericht erwähnt werden.

2. Heimliche Beschlagnahme

Soll die Beschlagnahme von E-Mail-Postfächern dagegen heimlich erfolgen, hält eine Mindermeinung die Regelungen über die Postbeschlagnahme (§§ 99, 100 StPO) für einschlägig (darunter auch eine ältere Entscheidung des BGH, Beschl. v. 31.3.2009 – 1 StR 76/09, NJW 2009, 1828, die allerdings durch BVerfG, Beschl. v. 16.6.2009 – 2 BvR 902/06, NJW 2009, 2431, überholt ist).

Jedoch bezieht sich die Regelung nur auf verkörperte Postsendungen (Briefe) und Telegramme. Sie hält zudem die vom BVerfG aufgestellten Anforderungen insbesondere an heimliche Ermittlungsmaßnahmen nicht ein (vgl. dazu BVerfG, Beschl. v. 16.6.2009 – 2 BvR 902/06, NJW 2009, 2431, 2434 f., Rn. 68 ff.). Auch der Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BT-Drs. 16/5846, S. 38 f.) widerspricht einer in der rechtswissenschaftlichen Literatur erhobenen Forderung, eine einheitliche Vorschrift für die Überwachung von „Fernkommunikation“ zu schaffen, mit dem Argument, dass zwischen der Überwachung des Postverkehrs einerseits (§§ 99, 100 StPO) und der Telekommunikation andererseits (§§ 100a, 100b StPO) grundlegende strukturelle Unterschiede bestünden, die eine unterschiedliche gesetzliche Regelung geboten erscheinen ließen. Insbesondere wird die einfache Duplizierbarkeit von Daten als Argument für eine abweichende Regelung in §§ 100a, 100b StPO angeführt. Auch daraus wird deutlich, dass §§ 99, 100 StPO nur für Postsendungen in der herkömmlichen Begriffsbedeutung, d.h. körperliche Schriftstücke, anwendbar ist.

Die herrschende Meinung hält eine heimliche E-Mail-Postfach-Beschlagnahme deshalb nur auf Basis von § 100a StPO als Maßnahme der Telekommunikationsüberwachung für zulässig.

Eine weitere Ansicht hält eine heimliche E-Mail-Postfach-Beschlagnahme für überhaupt nicht zulässig, solange es keine ausdrückliche gesetzliche Regelung gibt. (Dafür sprechen immerhin auch Art. 10 und 19 Abs. 1 GG: Das Telekommunikationsgeheimnis kann nur eingeschränkt werden, wenn das entsprechende Gesetz – dies kann auch das Gesetz sein, mit dem die StPO geändert wird – das so genannte Zitiergebot einhält, also ausdrücklich schreibt, dass das Grundrecht des Art. 10 GG eingeschränkt wird. Deswegen muss eine analoge Anwendung einer Beschlagnahmeregelung für „Postsendungen“ auf „elektronische Sendungen“ m.E. ausscheiden. Selbst wenn das Zitiergebot hier ausnahmsweise nicht gelten sollte – nämlich dann, wenn § 99 StPO so genanntes vorkonstitutionelles Recht sein sollte, also älter sein sollte als das Grundgesetz, was ich mangels Entscheidungserheblichkeit nicht geprüft habe, – würde ich davon ausgehen, dass eine nach Inkrafttreten des Grundgesetzes erstmals angewandte analoge Anwendung von § 99 StPO das Zitiergebot auslösen würde und deswegen nicht möglich ist.)

Die Postbeschlagnahme nach § 99 StPO bleibt zwar typischerweise zunächst geheim (§ 33 Abs. 4 StPO), doch gilt dies nicht unbeschränkt. Denn wenn ein Brief zwar zunächst zurückgehalten wird, allerdings bestimmte Teile trotz des laufenden Ermittlungsverfahrens nicht unbe-

dingt weiterhin zurückgehalten werden müssen, muss der Empfänger eine Kopie davon bekommen (§ 100 Abs. 5 StPO). Damit wird dem Empfänger klar, dass es eine Überwachung gegen ihn gibt (ähnlich § 100 Abs. 4 StPO: Weiterleitung nach Öffnung). Hier hat also schon der Gesetzgeber den Schutz der Ermittlungen vor Bekanntwerden der Überwachung nur als beschränkt entscheidend angesehen.

Dementsprechend gilt nur für Maßnahmen nach § 100a StPO eine Stillschweigenspflicht (§ 17 Abs. 1 G10-Gesetz):

> *„Wird die Telekommunikation (...) nach den §§ 100a, 100b der Strafprozessordnung überwacht, darf diese Tatsache von Personen, die Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, anderen nicht mitgeteilt werden.“*

Diese Stillschweigenspflicht ist nach § 18 G10-Gesetz strafbewehrt. Zum genauen Umfang dieser Pflicht siehe bereits oben unter I.

3. Ergebnis

a) Beschlagnahme auf der Grundlage von §§ 94, 99 StPO

Für ein Verbot der Offenlegung von Beschlagnahmen auf der Basis von §§ 94 und 99 StPO fehlt es an einer Verbotsnorm. Jedenfalls wenn kein Bezug zu einem einzelnen Postfach bzw. einer Person herstellbar ist, spricht daher nichts gegen eine Offenlegung im Transparenzbericht.

Im konkreten Fall zulässig wären also beispielsweise die Angabe
(1) der Anzahl der Beschlagnahmen auf der Basis von § 94 StPO und von
(2) § 99 StPO und
(3) der jeweils zugrunde liegenden Anlassstraftat.

Möglich wäre auch
(4) die Angabe, auf welchen Zeitraum sich die Beschlagnahme bezog.

b) Beschlagnahme auf der Grundlage von § 100a StPO

Sofern eine heimliche E-Mail-Postfach-Beschlagnahme auf Basis von § 100a StPO erfolgt (zu § 100a StPO bereits oben unter I.), müsste man wohl zumindest auch angeben dürfen, dass es sich nicht um eine laufende TKÜ handelte (was man bei Maßnahmen nach § 100a StPO eigentlich erwarten müsste), sondern um eine heimliche Postfach-Beschlagnahme, und wohl auch entsprechend § 100g Abs. 4 Nr. 4 StPO, auf welchen zurückliegenden Zeitraum sich diese bezog (Wortlaut: *„Anzahl der zurückliegenden Monate, für die Verkehrsdaten nach Absatz 1 abgefragt wurden, bemessen ab dem Zeitpunkt der Anordnung“*).

Im konkreten Fall zulässig ist somit die Angabe
(1) der Anzahl der Beschlagnahmen auf Basis von § 100a StPO und
(2) der jeweils zugrunde liegenden Anlassstraftat nach Maßgabe der Unterteilung in § 100a Abs. 2 StPO.

Möglich wäre wohl auch
(3) die Angabe, auf welchen Zeitraum (in Monaten zurückgerechnet) sich die Beschlagnahme bezog.

III. Bestandsdatenauskunft nach § 100j StPO

1. Verschwiegenheitspflicht

Die Bestandsdatenauskunft zu Strafverfolgungszwecken ist in § 100j StPO geregelt. § 113 Abs. 4 Satz 2 TKG regelt eine diesbezügliche Verschwiegenheitspflicht:

> *„Über das Auskunftsersuchen und die Auskunftserteilung haben die Verpflichteten gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren."*

Diese Verschwiegenheitspflicht betrifft ausweislich ihrer systematischen Stellung ausschließlich Bestandsdaten im Sinne des § 95 TKG i.V.m. § 3 Nr. 3 TKG sowie im Sinne des § 111 TKG. Ein Verstoß stellt nach § 149 Abs. 1 Nr. 35 TKG eine Ordnungswidrigkeit dar.

2. Umfang der Verschwiegenheitspflicht

Die Verschwiegenheitspflicht erstreckt sich ausweislich des Wortlauts des § 113 Abs. 4 Satz 2 TKG auf Auskunftsersuchen durch und Auskunftserteilung an die in § 113 Abs. 3 TKG genannten Sicherheitsbehörden. Dass die Verschwiegenheitspflicht auch die Veröffentlichung statistischer Angaben über Art und Anzahl der erfolgten Anfragen hinsichtlich der Übermittlung von Bestandsdaten nach §§ 95, 111 TKG untersagt, erscheint angesichts des Wortlauts des § 113 Abs. 4 Satz 2 TKG („das Auskunftsersuchen und die Auskunftserteilung") zwar nicht von vornherein ausgeschlossen.

a) Bestimmtheitsgebot und Wortlautgrenze

Es ist jedoch zu beachten, dass jedenfalls für eine ordnungswidrigkeitenrechtliche Verfolgung das Bestimmtheitsgebot des Art. 103 Abs. 2 GG gilt: Eine Bestrafung (dazu gehört auch ein Bußgeld) ist nur dann möglich, wenn das Gesetz eindeutig ist. Hier verwendet das Gesetz den bestimmten Artikel im Singular („das" Auskunftsersuchen, „die" Auskunftserteilung). Das Verbot bezieht sich demnach bereits nach seinem Wortlaut (nur) auf einzelne Ersuchen und Auskünfte.

Es bezieht sich nicht auf den Umstand, dass in einem bestimmten Zeitraum keine Auskunftsersuchen eingegangen sind, und nicht auf statistische Angaben ohne Bezug zu einem einzelnen Auskunftsersuchen.

b) Sinn und Zweck der Norm

Der erkennbare gesetzgeberische Wille sowie Sinn und Zweck der Regelung sprechen zudem dafür, dass die Verschwiegenheitspflicht nur im Falle der Gefährdung von Ermittlungen der Sicherheitsbehörden Anwendung findet:

Die Verschwiegenheitspflicht des heutigen § 113 Abs. 4 Satz 2 TKG beruht maßgeblich auf der erstmals in § 87 Abs. 5 Satz 3 TKG-RegE 1996 enthaltenen Regelung. Nach der gesetzgeberischen Intention sollte die Verschwiegenheitspflicht sicherstellen, dass die Ermittlungen der Behörden nicht gefährdet werden (vgl. BT-Drs. 13/3609, S. 29, 56). Die Verschwiegenheitspflicht wurde in der ursprünglichen Fassung des TKG vom 25.7.1996 (vgl. Bundesgesetzblatt I, S. 1120) in §§ 89 Abs. 6 Satz 2, 90 Abs. 5 Satz 3 TKG 1996 übernommen. Seitdem wurde die Verschwiegenheitspflicht ohne Änderung der gesetzgeberischen Regelungsintention beibehalten (vgl. BT-Drs. 15/2316, S. 97 mit Verweis auf § 111 Abs. 1 Satz 3 TKG-RegE 2004; später geregelt in § 113 Abs. 1 Satz 4 TKG 2004).

Die Gesetzgebungsmaterialien belegen auch bezüglich der heute gültigen Regelung des § 113 Abs. 4 Satz 2 TKG, dass an der ursprünglichen Regelungsintention der Verschwiegenheitspflicht festgehalten werden sollte (vgl. BT-Drs. 17/12879, S. 10; BR-Drs. 664/12, S. 18). Folglich dient die Verschwiegenheitspflicht nach der gesetzgeberischen Intention ausschließlich der Vorbeugung der Gefährdung von Ermittlungserfolgen bzw. der Offenbarung der laufenden Ermittlungen (so auch Eckhardt, in: Beck'scher TKG-Kommentar, 4. Auflage 2013, § 113 Rn. 50 m.w.N.; Bär, TK-Überwachung, § 100g Rn. 45).

c) Verbot daher nur bei Behinderung von Ermittlungen

Nach alledem liegt ein Verstoß gegen die Verschwiegenheitspflicht durch die Veröffentlichung der Anzahl der erfolgten Anfragen der Sicherheitsbehörden allenfalls vor, sofern hierdurch Ermittlungen der Sicherheitsbehörden behindert werden könnten.

Diese Behinderung könnte sich auf konkrete Ermittlungsmaßnahmen einerseits und die generelle Ermittlungstaktik der Sicherheitsbehörden andererseits beziehen. Die Behinderung konkreter Ermittlungstätigkeiten durch die Veröffentlichung statistischer Angaben ist jedoch ausgeschlossen, da die Zahlen keine Rückschlüsse auf konkrete Ermittlungen zulassen. Allenfalls ist denkbar, dass infolge der Statistik generelle Rückschlüsse auf die Ermittlungstaktik der deutschen Sicherheitsbehörden möglich sind. Die Verhinderung von Rückschlüssen auf das Ermittlungsverhalten der Sicherheitsbehörden ist aber vom Schutzzweck der Verschwiegenheitspflicht

nicht erfasst: So belegt bereits die Gesetzeshistorie die Tendenz zum besonderen Schutz konkreter Ermittlungsmaßnahmen.

Darüber hinaus wäre der Schutz von Informationen über das Ermittlungsverhalten durch die Verschwiegenheitspflicht nach § 113 Abs. 4 Satz 2 TKG ohnehin nicht zu gewährleisten: Denn eine ausdrückliche Verschwiegenheitspflicht für Maßnahmen der Beschlagnahme nach § 94 StPO bzw. § 99 StPO oder der Verkehrsdatenüberwachung nach § 100g StPO existiert nicht (zu Maßnahmen der Telekommunikationsüberwachung nach § 100a StPO siehe oben unter I.).

Außerdem schreibt der Gesetzgeber im Hinblick auf die Überwachung der Telekommunikation in § 100b Abs. 5, 6 StPO und im Hinblick auf die Überwachung von Verkehrsdaten in § 100g Abs. 4 StPO ausdrücklich vor, dass das Bundesamt für Justiz zur Erstellung und Veröffentlichung einer Statistik der jährlich bundesweit angeordneten Maßnahmen verpflichtet ist (siehe hierzu die Berichte unter https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html). Die Berichte des Bundesamtes für Justiz beinhalten unter anderem Informationen über Anzahl der Verfahren, in denen Überwachungsmaßnahmen durchgeführt wurden, die Anzahl der angeordneten Überwachungsmaßnahmen untergliedert nach Art der zu überwachenden Telekommunikation sowie Informationen über die Anlassstraftaten und eine zahlenmäßige Aufgliederung nach Bundesländern. Hieraus folgt, dass diese statistischen Angaben nach Ansicht des Gesetzgebers keinen (messbaren) Einfluss auf Ermittlungserfolge haben können.

Folglich ist davon auszugehen, dass ein Verstoß gegen die Verschwiegenheitspflicht des § 113 Abs. 4 Satz 2 TKG allenfalls bei Gefährdung konkreter Ermittlungen gegeben ist, wobei jedoch bereits die Wortlautgrenze eine Beschränkung auf Angaben zu einzelnen Auskunftsverlangen zieht.

d) Relevant Detailgrad

Bedenken gegen die Veröffentlichung von Informationen über die Anzahl von Anfragen zur Bestandsdatenübermittlung könnten daher allenfalls hinsichtlich des Detaillierungsgrades des Zeitraumes bestehen, für den die jeweiligen Anfragezahlen veröffentlicht werden sollen.

Die Berichte nach §§ 100b Abs. 5, 6, 100g Abs. 4 StPO enthalten Zahlen über Anfragen innerhalb eines Jahres. Angesichts der gesetzgeberischen Intention sowie Sinn und Zweck der Verschwiegenheitspflicht dürften aber auch gegen die Veröffentlichung von Informationen für Intervalle von einem Halbjahr oder sogar einem Quartal keine durchgreifenden Bedenken bestehen. Denn es kommt abermals maßgeblich darauf an, ob die Gefährdung konkreter Ermittlungen zu befürchten ist. Aufgrund des erheblichen Abstrahierungsgrades der statistischen Angaben dürfte ein Rückschluss auf konkrete Ermittlungsmaßnahmen auch bei Intervallen von einem

Halbjahr oder einem Quartal gänzlich ausgeschlossen sein. Dementsprechend beziehen sich auch die Berichte über die Überwachungstätigkeit der Geheimdienste nach § 14 Abs. 1 Satz 2 G10-Gesetz auf Halbjahreszeiträume.

Zwar sieht § 100g Abs. 4 Nr. 5 StPO bezüglich Verkehrsdatenabfragen eine Veröffentlichung der *„Anzahl der Maßnahmen, die ergebnislos geblieben sind, weil die abgefragten Daten ganz oder teilweise nicht verfügbar waren“* vor. Man könnte deshalb überlegen, ob auch Angaben zum (Miss-) Erfolg der Bestandsdatenanfragen zulässig sind.

Dagegen spricht im konkreten Fall bei Posteo das Problem, dass beim Fehlen von Bestandsdaten alle Bestandsdatenauskünfte notwendig erfolglos sein müssen und somit selbst eine rein zahlenmäßige Zusammenfassung zwangsweise auch das Ergebnis jeder einzelnen Anfrage umfasst. Diese Schwierigkeit ergibt sich allerdings immer, wenn es 100- oder 0-Prozent-Ergebnisse gibt, ohne dass diese gesetzlich verboten wären. Jedoch kommt so etwas bei einer bundesweiten Jahres-Statistik rein praktisch nicht vor.

Zudem besteht bei einer providerbezogenen Statistik die Gefahr, dass künftige Ermittlungen dadurch erschwert werden, dass Interessierte klar erkennen können, dass Bestandsdatenabfragen bei Posteo bisher stets erfolglos waren, weil die entsprechenden Daten fehlten. Sie könnten daher motiviert sein, von bestandsdatenspeichernden Anbietern zu Posteo zu wechseln. Andererseits lässt sich diese Erkenntnis zwangsweise auch daraus gewinnen, dass bekanntermaßen keine Bestandsdaten erhoben werden, so dass auch eine Auskunft zwangsweise erfolglos bleiben muss.

Dagegen spricht weiter, dass eine Erfolglosigkeitsstatistik nur in § 100g StPO vorgesehen ist, nicht in § 100b StPO. Dies könnte auf den ersten Blick dafür sprechen, dass die Erfolglosigkeitsstatistik nur in dem einen konkret geregelten Fall zulässig sein soll. Jedoch ist zu berücksichtigen, dass sich das Problem der Erfolgslosigkeit wegen fehlender Daten bei einer laufenden Telekommunikationsüberwachung nach § 100a StPO überhaupt nicht stellt, weil diese stets zukunftsgerichtet ist (weswegen § 100a StPO m.E. auch keine Rechtsgrundlage für die Beschlagnahme eines E-Mail-Postfachs darstellt). Das Problem fehlender Daten kann sich nur bei der (auch) rückwärtsgewandten Verkehrsdatenabfrage nach § 100g StPO stellen und muss daher auch nur dort geregelt werden. Aus dem Fehlen einer entsprechenden Regelung in § 100b StPO lässt sich somit nichts ableiten.

Im Ergebnis spricht gerade unter Berücksichtigung des Bestimmtheitsgebots („das“ Auskunftsersuchen, „die“ Auskunftserteilung) vieles dafür, dass auch eine Offenlegung der Anzahl der erfolglosen Bestandsdatenanfragen zulässig ist, selbst wenn damit indirekt über die Angabe „100 Prozent“ das Ergebnis jeder einzelnen Anfrage mitgeteilt wird; ganz sicher lässt sich dies allerdings nicht sagen.

e) Ergebnis

Die Verschwiegenheitspflicht des § 113 Abs. 4 Satz 2 TKG untersagt die Mitteilung von Informationen somit nur, sofern hierdurch konkrete Ermittlungen gefährdet werden könnten. Die Gefährdung von Ermittlungen ist ausgeschlossen und die Veröffentlichung der Informationen im Rahmen eines Transparenzberichts ist somit zulässig, wenn der Transparenzbericht nur statistische Angaben nach dem Vorbild der §§ 100b Abs. 5, 6, 100g Abs. 4 StPO enthält.

Im konkreten Fall zulässig ist somit die Angabe
(1) der Anzahl der Bestandsdatenabfragen auf Basis von § 100j StPO und
(2) der jeweils zugrunde liegenden Anlassstraftat nach Maßgabe der Unterteilung in § 100a Abs. 2 StPO.

Zur Frage, ob die Anzahl der erfolglosen Bestandsdatenabfragen genannt werden darf, siehe soeben unter d).

IV. Verkehrsdatenauskünfte nach § 100g StPO bzw. § 20m Abs. 1 BKAG

§ 100g StPO gestattet den Strafverfolgungsbehörden, bei Providern Verkehrsdaten im Sinne von § 96 Abs. 1 TKG abzufragen. Die Auskunftspflicht folgt aus §§ 100g Abs. 2 Satz 1, 100b Abs. 3 StPO.

Das Bundeskriminalamt kann zudem nach § 20m Abs. 1 BKAG Verkehrsdaten (Abs. 2 für Telemedien-Nutzungsdaten) herausverlangen. Die Auskunftspflicht ergibt sich aus § 20m Abs. 3 Satz 1 i.V.m. § 20l Abs. 5 BKAG. Eine gesonderte Verschwiegenheitspflicht enthält das BKAG nicht, so dass es hier nicht weiter behandelt wird.

§ 100g Abs. 2 Satz 1 StPO verweist auf §§ 100a Abs. 3, 100b Abs. 1 bis 4 Satz 1 StPO. Dies ist für die Gutachtenfrage insoweit von Bedeutung, als dass § 17 Abs. 1 des G10-Gesetzes lautet:

> *„Wird die Telekommunikation (...) nach den §§ 100a, 100b der Strafprozessordnung überwacht, darf diese Tatsache von Personen, die Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, anderen nicht mitgeteilt werden.“*

Durch den reinen Verweis auf Teile der §§ 100a, 100b StPO wird allerdings eine Verkehrsdatenauskunft nach § 100g StPO nicht zu einer Telekommunikationsüberwachung im Sinne der §§ 100a, 100b StPO. Das Verbot des § 17 Abs. 1 G10-Gesetz gilt daher nicht für Verkehrsdatenauskünfte nach § 100g StPO, obwohl § 100g StPO seiner Konzeption nach zu den heimlichen Ermittlungsmethoden gehört (BT-Drs. 14/7008, S. 8; BT-Drs. 15/3349, S. 6).

Soweit kein Bezug zu einzelnen Postfächern erkennbar wird – hier könnte die Gefahr einer Strafvereitelung nach § 258 StGB entstehen – besteht somit keine Verpflichtung, über Verkehrsdatenauskünfte nach § 100g StPO Stillschweigen zu bewahren.

Im konkreten Fall zulässig wären also beispielsweise die Angabe
(1) der Anzahl der Verkehrsdatenanfragen, unterschieden nach Erst- und Folgeanfragen,
(2) der Anlassstraftat,
(3) der Anzahl der zurückliegenden Monate, für die Verkehrsdaten abgefragt wurden,
(4) der Erfolgsquote.

V. TKÜ, Verkehrsdatenabfragen und E-Mail-Herausgabeverlangen durch Geheimdienste

Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst können nach §§ 2 Abs. 1 Satz 3, 1 Abs. 1 G10-Gesetz von Providern
(1) Auskunft über die näheren Umstände der nach Wirksamwerden der Anordnung durchgeführten Telekommunikation (Verkehrsdaten) verlangen,
(2) Sendungen zur Übermittlung auf dem Telekommunikationsweg (bei Posteo: E-Mails) herausverlangen und
(3) verlangen, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen.

Weitere Ermächtigungsgrundlage für den Verfassungsschutz ist § 8a Abs. 2 Nr. 4 BVerfSchG für Telekommunikations-Verkehrsdaten (Nr. 5 für Telemedien-Nutzungsdaten); die Auskunftspflicht ergibt sich aus § 8b Abs. 6 BVerfSchG. Diese Regelung ist nach § 4a MAD-Gesetz auch auf den Militärischen Abschirmdienst und nach § 2a BND-Gesetz auch auf den Bundesnachrichtendienst anwendbar.

1. Gesetzliche Grundlagen einer Verschwiegenheitspflicht

a) § 17 Abs. 1 G10-Gesetz für Telekommunikationsüberwachung

§ 17 Abs. 1 G10-Gesetz regelt eine Geheimhaltungspflicht bei Telekommunikationsüberwachung:

> *„Wird die Telekommunikation nach diesem Gesetz (...) überwacht, darf diese Tatsache von Personen, die Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, anderen nicht mitgeteilt werden.“*

b) § 17 Abs. 2 G10-Gesetz für Herausgabe von E-Mails

§ 17 Abs. 2 G10-Gesetz regelt eine Geheimhaltungspflicht, wenn die Geheimdienste E-Mails herausverlangen:

> *„Wird die Aushändigung von Sendungen nach § 2 Abs. 1 Satz 1 oder 3 angeordnet, darf diese Tatsache von Personen, die zur Aushändigung verpflichtet oder mit der Sendungsübermittlung betraut sind oder hieran mitwirken, anderen nicht mitgeteilt werden.“*

c) § 17 Abs. 3 G10-Gesetz für Verkehrsdatenauskünfte

§ 17 Abs. 3 G10-Gesetz regelt eine Geheimhaltungspflicht hinsichtlich sämtlicher Auskunftsverlangen von Geheimdiensten nach § 2 Abs. 1 G10-Gesetz, d.h. bei Posteo bezüglich Verkehrsdaten:

> *„Erfolgt ein Auskunftsersuchen oder eine Auskunftserteilung nach § 2 Abs. 1, darf diese Tatsache oder der Inhalt des Ersuchens oder der erteilten Auskunft von Personen, die zur Beantwortung verpflichtet oder mit der Beantwortung betraut sind oder hieran mitwirken, anderen nicht mitgeteilt werden.“*

d) § 8b Abs. 4 Satz 2 BVerfSchG für Verkehrsdatenauskünfte

§ 8b Abs. 4 Satz 2 BVerfSchG enthält ein Mitteilungsverbot für Anordnungen nach § 8a BVerfSchG (für Posteo relevant nur hinsichtlich Verkehrsdaten):

> *„Anordnungen und übermittelte Daten dürfen dem Betroffenen oder Dritten vom Verpflichteten nicht mitgeteilt werden.“*

2. Umfang der Verschwiegenheitspflicht

Hinsichtlich des Umfangs der Verschwiegenheitspflicht nach § 17 Abs. 1 G10-Gesetz (Telekommunikationsüberwachung) darf zunächst auf die umfassende Darstellung unter I. verwiesen werden: Die Regelung steht einer Statistik des Detailgrades der Berichte nach §§ 100b Abs. 5, 6, 100g Abs. 4 StPO nicht entgegen. Es geht (nur) darum, die geheimdienstliche Aufgabenwahrnehmung vor Beeinträchtigungen durch vorzeitiges Bekanntwerden von Überwachungsmaßnahmen zu schützen (Roggan, G10-Gesetz, 1. Auflage 2012, § 18 Rn. 3).

Das unter I. hinsichtlich Überwachungsmaßnahmen nach §§ 100a, 100b StPO gefundene Ergebnis wird bestätigt durch die sich rein auf geheimdienstliche Überwachung beziehenden Vorschriften:

Nach § 14 Abs. 1 Satz 2 G10-Gesetz (und § 8b Abs. 3 Satz 2 BVerfSchG) berichtet das Parlamentarische Kontrollgremium dem Bundestag jährlich über die Überwachungstätigkeit der Geheimdienste. Die Norm verweist ausdrücklich auf die Geheimhaltungsvorschrift des § 10 Abs. 1 des Kontrollgremiumgesetzes (Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes, PKGrG). Die dortigen Vorschriften sind mit ihrer umfassenden Einstufung aller Informationen als „geheim“ noch strenger, wenn auch hinsichtlich des Bekanntgabeverbotes an Dritte vergleichbar.

Selbst dieser strengen Geheimhaltung unterfallen allerdings nicht Angaben über die Anzahl der durchgeführten Überwachungsmaßnahmen, aufgeteilt nach dem jeweiligen Geheimdienst, der jeweils angewendeten Rechtsgrundlage, neu begonnener oder fortgesetzter Überwachung und Anzahl der Haupt- und Nebenbetroffenen, jeweils bezogen auf Halbjahre. Denn diese werden durch das Parlamentarische Kontrollgremium selbst in seinem Bericht an den Bundestag veröffentlicht (zuletzt BT-Drs. 17/12773).

Dies bestätigt das bereits unter I. gefundene Ergebnis, dass derartige statistische Informationen, die keinen Bezug zu einer konkreten Überwachungsmaßnahme aufweisen, nicht unter das Verbot des § 17 G10-Gesetz fallen, weil sie Ermittlungsmaßnahmen nicht gefährden können. Da im Bereich der geheimdienstlichen Maßnahmen nicht die Anlasstat für die politische Bewertung von Entscheidung ist, sondern der überwachende Geheimdienst, und diese Unterteilung keine Gefährdung der Maßnahmen bedeutet (vgl. auch die entsprechende Unterteilung in den Berichten der G10-Kommission), ist auch eine Unterteilung nach den ermittelnden Diensten zulässig.

Dies gilt entsprechend für die Verschwiegenheitspflichten nach § 17 Abs. 2 G10-Gesetz (Herausgabe von E-Mails) und nach § 17 Abs. 3 G10-Gesetz (Verkehrsdatenauskünfte): Auch diese Verbote greifen zunächst nur ein, wenn tatsächlich die Aushändigung von Nachrichten bzw. eine Auskunft angeordnet wird. Eine Negativ-Information hinsichtlich dieser Überwachungsmaßnahmen ist hiernach ebenso wie hinsichtlich TK-Überwachungsmaßnahmen nicht verboten.

Im Fall eines Herausgabeverlangens für Nachrichten verbietet das Gesetz, „diese Tatsache“ mitzuteilen. Der Wortlaut des § 17 Abs. 2 G10-Gesetz entspricht insoweit dem Wortlaut des § 17 Abs. 1 G10-Gesetz. Alle vorstehend dargelegten Argumente gelten entsprechend, so dass auch insoweit statistische Angaben nicht vom Verbot umfasst sind.

§ 17 Abs. 3 G10-Gesetz erweitert für Auskunftsersuchen und -erteilungen hinsichtlich Verkehrsdaten das Verbot zudem auf den Inhalt des Ersuchens oder der erteilten Auskunft. Verkehrsdaten unterliegen ohnehin dem Fernmeldegeheimnis und dürfen und sollen in einem Transparenzbericht nicht erscheinen. Wie der Inhalt des Auskunftsersuchens sinnvoll weitergegeben werden kann, ohne zugleich die Tatsache des Vorliegens des Auskunftsersuchens mitzuteilen, erschließt sich nicht. In jedem Fall soll der Transparenzbericht keine Angaben zum Inhalt von

Auskunftsersuchen enthalten, sondern nur statistische Angaben. Insoweit gelten die Ausführungen zu § 17 Abs. 1 und Abs. 2 G10-Gesetz vollumfänglich entsprechend.

Das Mitteilungsverbot aus § 8b Abs. 4 Satz 2 BVerfSchG für Verkehrsdatenauskünfte bezieht sich bereits nach seinem Wortlaut nur auf „Anordnungen und übermittelte Daten", also den Inhalt und nicht die bloße Tatsache ihres Vorliegens. Es bleibt somit hinter den Verboten des § 17 G10-Gesetz zurück. Soweit eine Verkehrsdatenabfrage ausschließlich auf § 8a Abs. 2 Nr. 4 BVerfSchG, ggf. i.V.m. § 4a MAD-Gesetz oder § 2a BND-Gesetz, gestützt wird, gibt es deshalb keine Verschwiegenheitsverpflichtung hinsichtlich der bloßen Tatsache ihres Vorliegens (Huber, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, Stand 196. EL 2013, § 17 Rn. 2).

3. Ergebnis

Im Transparenzbericht zulässig ist also die Angabe
(1) der Anzahl der TK-Überwachungsanordnungen der Geheimdienste,
(2) der Anzahl der E-Mail-Postfach-Herausgabeverlangen der Geheimdienste und
(3) der Anzahl der Verkehrsdatenabfragen der Geheimdienste,
aufgeteilt nach dem jeweiligen Geheimdienst, der jeweils angewendeten Rechtsgrundlage, neu begonnener oder fortgesetzter Überwachung.

VI. Bestandsdatenanfragen von Geheimdiensten

§ 8d Abs. 1 und Abs. 2 BVerfSchG gestatten den Verfassungsschutzbehörden unter Verweis auf § 113 Abs. 1 TKG Anfragen nach Bestandsdaten. § 8d Abs. 4 BVerfSchG verpflichtet den Provider zur Auskunft. Diese Regelung ist nach § 4b MAD-Gesetz auch auf den Militärischen Abschirmdienst und nach § 2b BND-Gesetz auch auf den Bundesnachrichtendienst anwendbar.

Eine gesonderte Verschwiegenheitspflicht enthält das Gesetz insoweit nicht, so dass die allgemeine Verschwiegenheitspflicht nach § 113 Abs. 4 Satz 2 TKG gilt. Hierzu sei auf III. verwiesen.

Wie unter V.2. dargelegt, ist eine Unterteilung nach dem jeweils anfragenden Geheimdienst unproblematisch.

Im konkreten Fall zulässig ist somit die Angabe
(1) der Anzahl der Bestandsdatenabfragen der Geheimdienste,
(2) aufgeteilt nach den verschiedenen Geheimdiensten.
Zur Frage, ob die Anzahl der erfolglosen Bestandsdatenabfragen genannt werden darf, siehe oben unter III.2.d).

VII. TK-Überwachung nach § 23a Abs. 1 ZFdG und Verkehrsdatenabfrage nach § 23g Abs. 1 ZfdG

Das Zollkriminalamt ist nach § 23a Abs. 1 ZFdG zur Überwachung der Telekommunikation befugt. Nach § 23a Abs. 8 ZFdG gilt § 2 des G10-Gesetzes entsprechend, woraus sich die Mitwirkungspflichten des Providers ergeben (§ 2 Abs. 1 Satz 3 G10-Gesetz).

Der Wortlaut des § 23e ZFdG entspricht § 17 Abs. 1 G10-Gesetz:

> *„Werden Maßnahmen nach § 23a vorgenommen, so darf diese Tatsache von Personen, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, anderen nicht mitgeteilt werden.“*

Das Verbot ist nach § 45 ZFdG strafbewehrt (entsprechend § 18 G10-Gesetz).

§ 23c Abs. 8 Satz 2 ZFdG sieht eine (wenn auch einmalige) Berichtspflicht ähnlich dem Bericht des Parlamentarischen Kontrollgremium nach § 14 Abs. 1 Satz 2 G10-Gesetz (vgl. dazu III.2.). Auch dieser Bericht (BT-Drs. 16/9682) enthält detaillierte statistische Angaben über Rechtsgrundlagen nebst Anzahl ihrer Anwendung, Anzahl der Anordnungen getrennt nach Erst- und Folgeanordnungen, Zahl der Betroffenen, bis hin zur Anzahl der betroffenen Kommunikationsverbindungen nebst Anzahl der Verbindungen, an denen Berufsgeheimnisträger beteiligt waren und der Zahl strafrechtlicher Ergebnisse der Überwachungsmaßnahmen. Dies belegt, dass der Wortlaut des § 23e ZFdG nicht anders zu verstehen ist als der Wortlaut des § 17 Abs. 1 G10-Gesetz, so dass auf die diesbezüglichen Ausführungen unter I. und III.2. zu verweisen ist.

§ 23g Abs. 1 ZFdG gestattet dem Zollkriminalamt zudem die Erhebung von Verkehrsdaten; die Mitwirkungspflicht des Providers ergibt sich aus § 23g Abs. 5 ZFdG. Nach § 23g Abs. 6 gelten insbesondere § 23c Abs. 8 sowie § 23e entsprechend, so dass vollumfänglich auf die vorstehenden Ausführungen zur TK-Überwachung, für die diese Vorschriften gelten, zu verweisen ist.

Im Transparenzbericht zulässig ist also die Angabe
(1) der Anzahl der TK-Überwachungsanordnungen nach § 23a Abs. 1 ZFdG, unterschieden nach Erst- und Verlängerungsanordnungen,
(2) der Anzahl der Verkehrsdatenabfragen nach § 23g Abs. 1 ZFdG, unterschieden nach Erst- und Verlängerungsanordnungen,
(3) der jeweils zugrunde liegenden Anlassstraftat.

D. Gesamtergebnis

Nach alledem kommen wir zu dem Ergebnis, dass der geplanten Veröffentlichung statistischer Angaben im Rahmen eines Transparenzberichts keine gesetzlichen Regelungen entgegenste-

hen. Für den zulässigen Detailgrad sei auf die Ausführungen zu den einzelnen Überwachungsmaßnahmen verwiesen.

Berlin, 24. Februar 2014

Matthias Bergt
Rechtsanwalt