Rekonstruktion eines Staatsgeheimnisses

Jan-Hendrik Dietrich*

Die Identifizierung von Staatsgeheimnissen i.S. von § 93 StGB bereitet seit vielen Jahren Schwierigkeiten. Dies gilt insbesondere, soweit sie Gegenstand von Presseveröffentlichungen sind. In der Literatur wird der Problematik gleichwohl vergleichsweise wenig Aufmerksamkeit geschenkt. Der Beitrag nimmt dies zum Anlass, den Staatsgeheimnisbegriff des StGB anhand eines aktuellen Sachverhalts zur Anwendung zu bringen und dadurch gleichzeitig kritisch zu hinterfragen.

A. Einleitung

Der Staat des Grundgesetzes ist ein Staat in Öffentlichkeit; im besten Sinne ist er *res publica*.[1] Die demokratische Legitimation erfordert Transparenz. Allein eine informierte Öffentlichkeit ist in der Lage, Partizipationsrechte wahrzunehmen und die Beachtung rechtsstaatlicher Schutzpflichten einzufordern. Gleichwohl verbleiben ausnahmsweise Bereiche, in denen gerade eine Nicht-Öffentlichkeit eine notwendige staatliche Funktionsbedingung darstellt.[2] In diesen Zusammenhang ist

* Prof. Dr. Jan-Hendrik Dietrich ist Professor an der Hochschule des Bundes in München/Brühl. .

1 Vgl. *Jestaedt*, Das Geheimnis im Staat der Öffentlichkeit, AöR 126 (2001), S. 205 (206). Näher dazu *Wegener*, Der geheime Staat, Göttingen 2006, S. 390 ff., 458 ff.

2 Siehe ausführlich *Jestaedt*, Geheimnis (Fn. 1), S. 205 (225 ff.).

RW 4/2016, DOI: 10.5771/1868-8098-2016-4-566

auch das Staatsgeheimnis i.S.v. § 93 Abs. 1 StGB einzuordnen. Um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden, können bestimmte Sachverhalte allein einem begrenzten Personenkreis zugänglich gemacht werden. Verrat steht unter Strafandrohung der §§ 94 ff. StGB. So berechtigt Exklusion und Vertraulichkeit im Ausnahmefall sein mögen, so schwierig erweist sich in der Rechtspraxis die Beurteilung, wann tatsächlich die tatbestandlichen Voraussetzungen für die Annahme eines Staatsgeheimnisses vorliegen.[3]

Eine gewisse Aufmerksamkeit hat dieses Problem zuletzt im Zusammenhang eines Ermittlungsverfahrens des Generalbundesanwalts beim Bundesgerichtshof gegen zwei Blogger der Internetplattform „Netzpolitik.org" erlangt.[4] Die Blogger hatten vertrauliche Dokumente des Bundesamtes für Verfassungsschutz (BfV) zumindest auszugsweise im Originalwortlaut veröffentlicht und kritisch kommentiert.[5] Bei den Dokumenten handelte es sich um einen Auszug aus dem BfV-Wirtschaftsplan für das Jahr 2013 sowie um ein Konzept zur Einrichtung einer Referatsgruppe „Erweiterte Fachunterstützung Internet im BfV" („EFI-Konzept"). Beide Dokumente waren durch das BfV als Verschlusssachen i.S.d. sog. VS-Anweisung (VSA) eingestuft. Die Aufnahme der staatsanwaltlichen Ermittlungen rief z.T. heftige Kritik hervor. Insbesondere die Geheimhaltungsbedürftigkeit der veröffentlichten Dokumente wurde bezweifelt. Von einer „absurden Konstruktion eines Staatsgeheimnisses"[6] war die Rede; es wurde gefragt, seit wann eigentlich Staatsgeheimnisse nur als „VS-Vertraulich" klassifiziert würden? Schließlich sei doch „VS-V die niedrigste Geheimhaltungsstufe".[7] Das Vorgehen des Generalbundesanwalts sei vor diesem Hintergrund „martialisches äffisches Machtgehabe",[8] „nur noch peinlich".[9] „Mit

3 So bereits *Posser*, in: *Ruge* (Hrsg.), Landesverrat und Pressefreiheit, Köln/Berlin 1963, Wortbeitrag S. 22.

4 Siehe dazu die Zusammenfassungen von *Müller-Neuhof*, Saison der Verräter, Berliner Tagesspiegel vom 7.10.2015, abrufbar unter: http://www.tagesspiegel.de/politik/landesverrat-saison-der-verraeter/12404144.html (Stand: 12.2.2016); *Rath*, Intrigen, Konflikte und Gefühle, lto vom 22.9.2015, abrufbar unter: http://www.lto.de/recht/hintergruende/h/landesverrat-ermittlungen-netzpolitik-hypothesen-wie-es-gewesen-sein-koennte/ (Stand: 12.2.2016).

5 Siehe *Meister*, Geheimer Geldregen: Verfassungsschutz arbeitet an „Massendatenauswertung von Internetinhalten" (Updates), abrufbar unter: https://netzpolitik.org/2015/geheimer-geldregen-verfassungsschutz-arbeitet-an-massendatenauswertung-von-internetinhalten/ (Stand: 12.2.2016); *Meister*, Wir enthüllen die neue Verfassungsschutz-Einheit zum Ausbau der Internet-Überwachung (Updates), abrufbar unter: https://netzpolitik.org/2015/geheime-referatsgruppe-wir-praesentieren-die-neue-verfassungsschutz-einheit-zum-ausbau-der-internet-ueberwachung/ (Stand: 12.2.2016).

6 *von Notz*, zitiert nach http://www.zeit.de/politik/deutschland/2015-08/netzpolitik-affaere-harald-range-heiko-maas-streit-um-verantwortung (Stand: 12.2.2016).

7 *Schaar*, zitiert nach http://www.zeit.de/digital/2015-07/pressefreiheit-ralf-stegner-netzpolitik (Stand: 12.2.2016).

8 *Prantl*, Martialisches äffisches Machtgehabe, SZ vom 1.8.2015, abrufbar unter: http://www.sueddeutsche.de/politik/ermittlungen-gegen-netzpolitikorg-martialisches-aeffisches-machtgehabe-1.2590152 (Stand: 12.2.2016).

Kanonen auf Blogspatzen zu schießen“ entspreche nicht seinen Pflichten.[10] In einem offenen Brief machten zudem „Journalisten, Wissenschaftler und Aktivisten aus mehreren Ländern“ einen „Angriff auf die Pressefreiheit“ aus.[11] Die Kritik blieb bekanntlich nicht ohne Wirkung. Am 04. August 2015 beantragte der Bundesminister der Justiz beim Bundespräsidenten, den Generalbundesanwalt in den einstweiligen Ruhestand zu versetzen. Wenige Tage später wurde das Verfahren gegen die beiden Blogger nach § 170 Abs. 2 StPO eingestellt. In ihrer Pressemitteilung ließ die Behörde wissen, sie gehe nunmehr mit dem Bundesministerium der Justiz und für Verbraucherschutz davon aus, dass es sich bei den veröffentlichten Inhalten nicht um ein Staatsgeheimnis im Sinne des § 93 StGB handelte.[12]

Manchen Rechtskundigen mögen manche Facetten der beschriebenen Entwicklungen in Erstaunen versetzt haben. Als besonders erstaunlich darf die divergierende, z.T. wechselvolle Beurteilung der Staatsgeheimnisqualität der unter „Netzpolitik.org“ veröffentlichten Dokumente angesehen werden. Nachdem ein Gutachten des Verfassungsschutzes zunächst den Generalbundesanwalt von der Staatsgeheimnisqualität zumindest insoweit überzeugt hatte, ein Ermittlungsverfahren einzuleiten, stellte wenige Wochen später eine gutachterliche Stellungnahme des Justizministeriums das Gegenteil fest.[13] Im letzterem Falle hatte der Justizminister zuvor damit überrascht, innerhalb weniger Tage ein eigenes Gutachten seines Hauses – und zugleich dessen Ergebnis – anzukündigen.[14] Begründungen für die eine oder die andere Position suchte man vergeblich.

Vor diesem Hintergrund soll nachfolgend die Staatsgeheimnisqualität der veröffentlichten Dokumente noch einmal eingehend in den Blick genommen werden. So dringlich die Abkehr von der Arkantradition der Stempelsucht und Geheimniskrämerei in der Vergangenheit war,[15] so wichtig bleibt im Staat der Öffentlichkeit der verantwortungsvolle Umgang mit sensiblen Informationen, soweit Nicht-Öffentlichkeit ausnahmsweise eine notwendige staatliche Funktionsbedingung darstellt. Es gilt, im Einzelfall die rechte Mischung zwischen Öffentlichkeit und begründeter

9 *Flisek*, zitiert nach http://www.rp-online.de/politik/deutschland/nur-noch-die-union-unterstuetzt-generalbundesanwalt-range-aid-1.5280412, (Stand: 12.2.2016).

10 *Stegner*, zitiert nach http://www.zeit.de/news/2015-08/01/internet-demonstration-fuer-netzpolitikorg-01053404, (Stand: 12.2.2016).

11 Siehe Abdruck im Berliner Tagesspiegel, abrufbar unter: http://www.tagesspiegel.de/politik/streit-um-netzpolitik-org-offener-brief-an-die-bundesregierung/12149160.html, (Stand: 12.2.2016).

12 Abrufbar unter http://www.generalbundesanwalt.de/de/showpress.php?newsid=561. (Stand: 12.2.2016).

13 Siehe *Rossmann*, Krieg der Gutachter, DIE ZEIT vom 7.8.2015, abrufbar unter: http://www.suddeutsche.de/politik/landesverrat-affaere-krieg-der-gutachter-1.2599727, (zuletzt besucht am 12.2.2016).

14 Vgl. *Jungholt/Müller*, Sachverstand in der Netzpolitik-Affäre? Nein, danke!, DIE WELT vom 16.8.2015, abrufbar unter: http://www.welt.de/politik/deutschland/article145278613/Sachverstand-in-der-Netzpolitik-Affaere-Nein-danke.html, (zuletzt besucht am 12.2.2016).

15 Näher dazu *Wegener*, Geheimer Staat (Fn. 1), S. 390 ff.

Vertraulichkeit zu finden.[16] Der Beitrag widmet sich daher zunächst der Frage, ob es sich bei den unter „Netzpolitik.org“ veröffentlichten Dokumenten um Staatsgeheimnisse i.S.d. § 93 StGB gehandelt hat (dazu unter B. und C.), um anschließend das Problem ihrer Identifizierung zu erörtern (dazu unter D.). Keine Antwort gibt der Beitrag dagegen darauf, ob die bundesanwaltschaftlichen Ermittlungen gegen die Blogger gerechtfertigt waren. Auch sollen die nachfolgenden Ausführungen keine sachverständige Begutachtung in einem Strafverfahren nachahmen, was Einblicke in verwaltungsinterne Sachverhalte erfordern würde. Grundlage der Untersuchung sind allein offen verfügbare Dokumente.

B. Der Staatsgeheimnisbegriff gem. § 93 StGB

Nach der Legaldefinition von § 93 Abs. 1 StGB sind Staatsgeheimnisse Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheim gehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden. Keine Staatsgeheimnisse sind dagegen Tatsachen, die gegen die freiheitliche demokratische Grundordnung oder unter Geheimhaltung gegenüber den Vertragspartnern der Bundesrepublik Deutschland gegen zwischenstaatlich vereinbarte Rüstungsbeschränkungen verstoßen, § 93 Abs. 2 StGB.

Diese Gestalt hat der Staatsgeheimnisbegriff im Wesentlichen durch das 8. Strafrechtsänderungsgesetz vom 25.6.1968[17] gefunden. Neu war seinerzeit insbesondere die Tatbestandseinschränkung im zweiten Absatz, die nicht zuletzt der Pressefreiheit zur Durchsetzung verhelfen sollte.[18] Vorangegangen waren viel beachtete, bis heute fortwirkende Entscheidungen des Bundesverfassungsgerichts und des BGH. In der berühmten „*Spiegel*-Entscheidung“[19] hatte das Bundesverfassungsgericht im Zusammenhang des sog. publizistischen Landesverrats nicht nur auf die Bedeutung der Presse „als Wesenselement des freiheitlichen Staates“ hingewiesen, sondern gleichsam das sich aus dem „demokratischen Prinzip ergebende Anrecht der Öffentlichkeit an der Information und Diskussion der betreffenden Fakten“ betont. Der BGH hatte dies in seinem „*Pätsch*-Urteil“ bereits vorgezeichnet:[20] Bei einer Verletzung des „Kernbereichs des Verfassungsrechts“, müsse jeder das Recht haben, sofort und ohne Umwege die Öffentlichkeit anzurufen, auch wenn dies

16 *Jestaedt*, Geheimnis (Fn. 1), S. 205 (243).

17 BGBl. I S. 741. Zum Reformprozess siehe ausführlich *Scholz*, Der Begriff des Staatsgeheimnisses im freiheitlichen Rechtsstaat, Freiburg 1970, S. 180 ff.

18 *Krauth/Kurfess/Wulf*, Die Reform des Staatsschutz-Strafrechts durch das Achte Strafrechtsänderungsgesetz, JZ 1968, S. 609 (610 f.).

19 Siehe dazu ausführlich den Rückblick von *Hoffmann-Riem*, Die Spiegel-Affäre 1962 – ein Versagen der Justiz, ZRP 2012, S. 225 (225) sowie die politische Aufarbeitung von *Schoenbaum*, Die Spiegel-Affäre, Berlin 1968.

20 Näher dazu *Deiseroth*, Illegale Dienst- und Staatsgeheimnisse und ihre Enthüllung – Lessons learnt? Betrifft JUSTIZ, Nr. 117, März 2014, S. 5.

zwingend zur Preisgabe von Staatsgeheimnissen führe.[21] Diese dem Widerstandsrecht i.S. von Art. 20 Abs. 4 GG folgende Ratio war die Hintergrundfolie für die Formulierung von § 93 Abs. 2 StGB.

Seit der Gesetzesnovelle von 1968 ist der Staatsgeheimnisbegriff trotz einiger Kritik[22] unverändert geblieben. Durch Rechtsprechung und Literatur hat er eine gewisse Kontur erhalten, wenngleich Judikate rar sind und die meisten Beiträge im Schrifttum aus den 1960er sowie 1970er Jahren stammen.[23] Aus heutiger Sicht erhebt sich gelegentlich die Frage, wie mit der gegenwärtigen Fassung von § 93 StGB gleichzeitig aktuellen sicherheitspolitischen Herausforderungen und rechtsstaatlichen Anforderungen genügt werden soll.[24] Die dekadenspezifische Patina, die über Rechtsbegriffen wie „fremde Macht" oder „äußere Sicherheit" liegt, erschwert z.T. die Anwendung in der Rechtspraxis. Solange indes der Staatsgeheimnisbegriff i.S.v. § 93 StGB geltendes Recht darstellt, müssen sich Verdachtsfälle wie der oben erwähnte Sachverhalt an ihm messen lassen.

C. Staatsgeheimnisqualität unter „Netzpolitik.org" veröffentlichter Unterlagen

I. Staatsgeheimnisobjekt

Gegenstände eines Staatsgeheimnisses sind Tatsachen, Gegenstände und Erkenntnisse. Die veröffentlichten Textpassagen lassen sich überwiegend als Erkenntnisse qualifizieren. Sie beinhalten wertende Einsichten in gedankliche Zusammenhänge und verfügen demgemäß über einen eigenständigen Aussagegehalt.[25] So wird beispielsweise im Auszug aus dem Wirtschaftsplan des BfV der Finanzbedarf unter Bezugnahme auf sicherheitspolitische Entwicklungen oder die nachrichtendienstliche Praxis konkretisiert:

> *„Eine zentrale Rolle nehmen dabei so genannte „Soziale Netzwerke" (...) ein, die auch von verfassungsschutzrelevanten Personen rege genutzt werden. Erfahrungen aus der täg-*

21 BGHSt 20, 342 (365).

22 Vgl. z.B. *Woesner*, Das neue Staatsschutzstrafrecht, NJW 1968, 2129 (2129 ff.); *Scholz*, Begriff des Staatsgeheimnisses (Fn. 17), S. 256 ff. Zu Reformbemühungen vor 1968 siehe bereits kritisch *Arndt*, Landesverrat, Berlin 1966, S. 17 f.

23 Die Kommentarliteratur rekurriert bis heute im Wesentlichen etwa auf: *Baumann*, Die Reform des politischen Strafrechts, JZ 1966, S. 331 ff.; *Roeder*, Der Landesverrat nach dem deutschen und österreichischen Staatsgesetzentwurf, ZStW 76 (1964), S. 359 ff.; *Laufhütte*, Staatsgeheimnis und Regierungsgeheimnis, GA 1974, S. 52 ff.; *Lüttger*, Das Staatsschutzstrafrecht gestern und heute, GA 1970, S. 121 ff.; *Wagner*, Aus der Rechtsprechung in Staatsschutzverfahren, GA 1968, S. 291 ff.; *Krauth/Kurfess/Wulf*, Reform des Staatsschutz-Strafrechts (Fn. 18), S. 609 ff.; *Woesner*, Neues Staatsschutzstrafrecht (o. Fn. 22), S. 2129 ff.; *Kohlmann*, Der Begriff des Staatsgeheimnisses und das verfassungsrechtliche Gebot der Bestimmtheit von Strafvorschriften, Köln 1969; *Jescheck*, Pressefreiheit und militärisches Staatsgeheimnis, Berlin 1964.

24 Siehe ausführlich dazu *Lampe/Hegmann*, in: Münchener Kommentar StGB, Bd. 3, 2. Aufl. 2012, Vor § 93 ff. Rn. 21 ff. sowie auch *Paeffgen*, in: Nomos-Kommentar StGB, Bd. 2, 4. Aufl. 2013, § 93 Rn. 20.

25 Vgl. *Schmidt*, Leipziger Kommentar StGB, Bd. 4, 12. Aufl. 2007, § 93 Rn. 2; *Lampe/Hegmann*, in: MüKo (Fn. 24), § 93 Rn. 6; *Laufhütte*, Staatsgeheimnis (Fn. 22), S. 52; *Roeder*, Landesverrat (Fn. 22), S. 364.

lichen Internetarbeit des BfV zeigen, (...)"; „Um große Datenmengen automatisiert und systematisch analysieren zu können, soll (...). Damit soll das BfV in die Lage versetzt werden (...)."

Im Übrigen liegen Tatsachen vor, d.h. Geschehnisse, Zustände und Verhältnisse aus der Vergangenheit und der Gegenwart, die sinnlich wahrgenommen werden können.[26]

II. Geheimhaltungsfähigkeit

Die Tatsachen und Erkenntnisse dürfen gem. § 93 Abs. 1 StGB nur einem begrenzten Personenkreis zugänglich sein (Geheimhaltungsfähigkeit). Der Gesetzgeber folgt damit dem sog. materiellen Geheimnisbegriff, d.h. das Vorliegen eines Staatsgeheimnisses wird nicht von einer formellen Sekretur oder einem staatlichen Geheimhaltungswillen abhängig gemacht.[27] Es kommt stattdessen auf das tatsächliche Geheimsein an.[28]

1. Zugänglichkeit

Zugänglich ist eine Tatsache oder eine Erkenntnis, wenn und soweit sie mit Sinnesorganen wahrnehmbar ist und in ihrem sachlichen Aussagegehalt erkennbar ist.[29] Entscheidend ist allein die Möglichkeit der Kenntnisnahme.[30] In Schriftform waren beide Dokumente sinnlich wahrnehmbar, ihr sachlicher Aussagehalt erkennbar. Insofern lag grundsätzlich eine wirkliche, sichere und zuverlässige Zugangsmöglichkeit vor.

2. Begrenzter Personenkreis

Die Möglichkeit der Kenntnisnahme darf nur einem begrenzten Personenkreis eingeräumt werden. Dahinter verbringt sich, dass der tatsächliche Zugang in einer Weise kontrolliert, überwacht und begrenzt wird, die geeignet erscheint, ein allgemeines Bekanntwerden des geheim zu haltenden Inhalts zu verhindern.[31]

In Bezug auf beide Dokumente ergibt sich die notwendige personelle Begrenzung aus den (Rechts-) Folgen ihrer Einstufung als Verschlusssachen.[32] Wirtschaftspläne des BfV werden üblicherweise mit dem Geheimhaltungsgrad „GEHEIM" gem. § 4

26 Vgl. *Kohlmann*, Begriff des Staatsgeheimnisses (Fn. 23), S. 66 f.; *Roeder*, Landesverrat (Fn. 22), S. 364; *Lampe/Hegmann*, in: MüKo (Fn. 24), § 93 Rn. 4; *Schmidt*, in: LK (Fn. 25), § 93 Rn. 2.

27 *Rudolphi/Pasedach/Wolter*, Systematischer Kommentar StGB, Bd. 3, 145. Lieferung (September 2014), § 93 Rn. 7.

28 *Lampe/Hegmann*, in: MüKo (Fn. 24), § 93 Rn. 7. Eine gewisse Wechselwirkung zwischen der Geheimhaltungsfähigkeit und der VS-Einstufung kann gleichwohl nicht übersehen werden. Siehe hierzu unter II. 2.

29 Vgl. *Schmidt*, in: LK (Fn. 25), § 93 Rn. 4; *Paeffgen*, in: NK (Fn. 24), § 93 Rn. 14.

30 *Lampe/Hegmann*, in: MüKo (Fn. 24), § 93 Rn. 8.

31 *Lampe/Hegmann*, in: MüKo (Fn. 24), § 93 Rn. 7. Siehe als Beispiel der Rechtspraxis BGH NJW 1971, S. 715 (716).

32 Siehe dazu *Laufhütte*, Staatsgeheimnis (Fn. 22), S. 54; *Lampe/Hegmann*, in: MüKo (Fn. 24), § 93 Rn. 7.

Abs. 2 Nr. 2 SÜG[33] i.V.m. § 3 Nr. 2 VSA versehen. Das „EFI-Konzept“ wurde als „VS-VERTRAULICH“ nach § 4 Abs. 2 Nr. 3 SÜG i.V.m. § 3 Nr. 3 VSA eingestuft. Für solche Verschlusssachen sieht die VSA eine Fülle an Vorkehrungen zur Sicherung der Geheimhaltung vor. § 10 VSA legt beispielsweise hohe Anforderungen an Personen fest, die Zugang zu Verschlusssachen haben, die mindestens als „VS-VERTRAULICH“ eingestuft sind, oder sich diesen Zugang verschaffen können. Insbesondere müssen solche Personen eine Sicherheitsüberprüfung i.S.d. §§ 8 ff. SÜG durchlaufen. Für Mitarbeiter/-innen von Nachrichtendiensten ist nach § 10 Nr. 3 SÜG regelmäßig eine „erweiterte Sicherheitsüberprüfung mit Sicherheitsmitteilungen“ (sog. „Ü-3“) vorgesehen. Näheres ergibt sich aus der AVV SÜG.[34] Diese aufwendige und zeitintensive Maßnahme personeller Sicherheit gewährleistet bereits faktisch eine begrenzte Zahl von „Mitwissern“.[35] Schließlich wird der Personenkreis durch Vorkehrungen materiellen Geheimschutzes weiter eingeschränkt. Nach § 14 Abs. 2 VSA erhält jede Ausfertigung einer als „GEHEIM“ eingestuften Verschlusssache eine laufende Nummer.[36] Der jeweilige Empfänger und die Anzahl der Vervielfältigungen sind gem. § 15 VSA zu dokumentieren. Vervielfältigungen sind nach Maßgabe von § 15 Abs. 1 S. 2 VSA nur unter Einhaltung des „Need-to-know-Prinzips“ zulässig. Als „VS-VERTRAULICH“ oder „GEHEIM“ eingestufte Verschlusssachen dürfen nach § 17 Abs. 1 VSA grundsätzlich nur in VS-Registraturen aufbewahrt werden. Auch auf diese Weise bleibt der Personenkreis zumindest nach allgemeinen Merkmalen beschreibbar und überschaubar.[37]

Es ist davon auszugehen, dass die Dokumente über den Herrschaftsbereich des BfV hinaus gelangt sind. Beide waren an das Vertrauensgremium des Deutschen Bundestages adressiert, das auf der Grundlage von § 10a Abs. 2 BHO für die parlamentarische Kontrolle der Wirtschaftspläne der Nachrichtendienste des Bundes zuständig ist. Bevor ein Wirtschaftsplan dem Vertrauensgremium übermittelt wird, ist er regelmäßig Gegenstand verwaltungsinterner Erörterungen und Abstimmungen. Einbezogen werden neben dem BfV die zuständige Aufsichtsbehörde – hier das Bundesinnenministerium – sowie das federführende Bundesfinanzministerium

33 Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (SÜG) vom 20.4.1994, BGBl. I S. 867, zuletzt geändert durch Art. 2 des Gesetzes vom 3.10.2015, BGBl. I S. 2161.

34 Allgemeine Verwaltungsvorschrift zur Ausführung des Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (AVV SÜG) vom 29. April 1994 (GMBl. S. 550) i.d.F. der mit Rundschreiben des Bundesministeriums des Innern vom 31. Januar 2006 – IS 4 – 606 411-1/1 – bekanntgegebenen Änderungen.

35 Zu Begrenzungsmaßnahmen bei größeren Personenzahlen vgl. *Paeffgen*, in: NK (Fn. 24), § 93 Rn. 13.

36 Für elektronisch vorliegende Verschlusssachen gelten besondere Bestimmungen, vgl. § 14 Abs. 3 VSA.

37 Vgl. dazu *Schmidt*, in: LK (Fn. 25), § 93 Rn. 3; *Laufhütte*, Staatsgeheimnis (Fn. 22), S. 53 f.

und der Bundesrechnungshof.[38] In Bezug auf das „EFI-Konzept“ wird wenigstens das Innenministerium befasst worden sein. Der Personenkreis wird auf diese Weise zahlenmäßig größer. Auf seine Begrenztheit ist dies gleichwohl ohne Auswirkung. In den Behörden gilt die VSA nach Maßgabe von § 1 VSA unterschiedslos. Auch im parlamentarischen Raum kommen ihre wichtigsten Bestimmungen zur Anwendung, da die „Geheimschutzordnung des Deutschen Bundestages“ in weiten Teilen der VSA entspricht. Insofern bestand für beide Dokumente grundsätzlich eine begrenzte Zugänglichkeit i.S.v. § 93 StGB.

3. Problematik der Vorveröffentlichungen

Die Limitierung des Personenkreises entfällt jedoch, soweit das Geheimnis über den begrenzten Personenkreis derart hinausdringt, dass seine substanzielle Aussage im Wege der Erkundigung allgemein zugänglich oder allgemein bekannt ist.[39] Dies könnte im vorliegenden Fall infolge von vorangegangenen Presseveröffentlichungen eingetreten sein.

a) Vorveröffentlichungen und BfV-Wirtschaftsplan 2013

Hinsichtlich des BfV-Wirtschaftsplans finden sich zwei Vorveröffentlichungen aus dem Jahr 2014. Die Süddeutsche Zeitung berichtet am 26.6.2014 zum Thema „Geheimdienste rüsten auf“.[40] Einen Tag zuvor war auf der Internetseite „tagesschau.de“ ein Artikel unter dem Titel „Verfassungsschutz will soziale Medien überwachen“ zu lesen.[41] Beide Publikationen stammen aus dem sog. Rechercheverbund von Süddeutscher Zeitung, WDR sowie NDR und gehen überwiegend auf dasselbe Autorenteam zurück. In Wortlaut und Inhalt unterscheiden sie sich kaum voneinander. Insofern genügt es, die (frühere) Veröffentlichung auf der Internetseite „tagesschau.de“ in den Blick zu nehmen. Ihre substanzielle Aussage bezieht sich auf die Überwachung sozialer Medien durch den Verfassungsschutz. In Bezug auf den BfV-Wirtschaftsplan 2013 finden sich folgende relevante Passagen:

> *„Das Bundesamt für Verfassungsschutz plant den Aufbau einer neuen Referatsgruppe zur Überwachung einzelner Personen in sozialen Netzwerken wie Twitter, Facebook und YouTube. (...) Zudem solle ein ‚System zur Gewinnung, Verarbeitung und Auswertung von großen Datenmengen aus dem Internet’ entwickelt werden. Dies geht aus einem internen Dokument (...) hervor, das NDR, WDR und Süddeutscher Zeitung vorliegt. (...) Bereits 2012 hatte das BfV in einer Vorlage zum eigenen Etat argumentiert, inzwischen fielen so viele Daten an, dass eine manuelle Auswertung schlichtweg ‚nicht mehr möglich’ sei. Daher sollen nach den Plänen der Verfassungsschützer nun die Standorte Berlin und*

38 Vgl. *Bartodziej*, in: *Dietrich/Eiffler* (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 7. Teil, § 2 Parlamentarische Kontrolle, Rn. 101, Stuttgart i.E.

39 Vgl. BGH NJW 1965, S. 1190; *Rudolphi/Pasedach/Wolter*, in: SK StGB (Fn. 27), § 93 Rn. 13.

40 *Goetz/Pinkert/Obermaier*, Geheimdienste rüsten auf, SZ vom 26.6.2014, S. 6.

41 Siehe *Goetz/Pinkert/Tieg*, Verfassungsschutz will soziale Medien überwachen, abrufbar unter: https://www.tagesschau.de/inland/verfassungsschutz-soziale-netzwerke-100.html (Stand: 12.2.2016).

Köln mit neuer Technik und Personal aufgerüstet werden. Es sollen spezielle Analysetools angeschafft und neue Mitarbeiter eingestellt werden.“

Die wörtlichen Zitate beziehen sich damit lediglich auf wenige Textstellen aus dem Wirtschaftsplan. Inhaltlich kaprizieren sich die Ausführungen auf die Überwachung sozialer Medien. Unerwähnt bleibt das im Wirtschaftsplan skizzierte Bedrohungsszenario:

„Erfahrungen aus der täglichen Internetarbeit des BfV zeigen, dass Extremisten und Terroristen jeglicher Prägung immer größere Datenmengen im Internet veröffentlichen. (...) Weiterhin nimmt die Komplexität elektronischer Angriffe durch fremde Nachrichtendienste immer mehr zu. (...).“

Gleiches gilt für Folgerungen aus der Bedrohungsanalyse:

„Bei der Massendatenauswertung von Internetinhalten handelt es sich um eine für das BfV neuartige Herausforderung. (...) Die für die Internetarbeit notwendige flächendeckende Verfügbarkeit von Internetarbeitsplätzen setzt den Aufbau einer modernen Netzinfrastruktur im BfV voraus.“

Bei eingehender Betrachtung lässt sich hieraus indes kein über die Presseberichterstattung hinausgehender Informationsgehalt ziehen. Das im Wirtschaftsplan angesprochene Bedrohungsszenario findet sich weitaus präziser im Verfassungsschutzbericht wieder. Den „Bedrohungen durch elektronische Angriffe“ gilt ein eigener Abschnitt.[42] Soziale Netzwerke werden als wichtigster Multiplikator zur Verbreitung von extremistischen Ideologien gekennzeichnet.[43] Das Bedrohungsszenario darf insofern als allgemein bekannt gelten. Den in den Vorveröffentlichungen unerwähnten Folgerungen aus der Bedrohungsanalyse kommt gleichfalls kein neuer, eigenständiger Aussagewert mehr zu. Durch das wörtliche Zitat, wonach beim BfV so viele Daten anfielen, dass eine „manuelle Auswertung schlichtweg nicht mehr möglich“ sei und deshalb bestimmte finanzielle Mittel erforderlich wären, wird die entscheidende substanzielle Aussage des Wirtschaftsplans bereits ausgedrückt. Dass die Massendatenauswertung von Internetinhalten eine neuartige Herausforderung darstelle und den Aufbau einer modernen Netzinfrastruktur verlange, ist vor diesem Hintergrund nur eine logische Konsequenz ohne eigenen Informationswert.

Diese Erwägungen sprechen dafür, dass die wesentliche Aussage aus dem BfV-Wirtschaftsplan 2013 bereits vor der Veröffentlichung der Auszüge unter „netzpolitik.org“ allgemein zugänglich war. Daran ändert auch nicht, dass die Blogger den Wirtschaftsplan auszugsweise im Originalwortlaut ins Netz gestellt haben. Soweit eine Beurteilung der Authentizität allgemeiner Meldungen oder Berichte nicht sicher möglich ist, soll nach überwiegender Auffassung im Schrifttum eine unver-

42 Vgl. BMI (Hrsg.), Verfassungsschutzbericht 2014, S. 142 ff.
43 Vgl. BMI (Hrsg.), Verfassungsschutzbericht 2014, S. 89 und 96.

bindliche Vorveröffentlichung vorliegen, mit der Folge, dass die geschützte Information noch geheim und Gegenstand eines Verrats bleiben könne.[44] Die (spätere) kompetente Bestätigung der Information – etwa durch amtliche Quellen und seriöse Beweismittel – bliebe insoweit weiterhin strafbar.[45] Im Falle des Wirtschaftsplans bleiben die Vorveröffentlichungen recht allgemein. Die als GEHEIM eingestufte Verschlusssache wird durch Bezeichnungen wie „internes Dokument" bzw. „Vorlage zum eigenen Etat" verfremdet. Die Publikation des Original-*Wortlauts* unter netzpolitik.org kann trotz dieser Unverbindlichkeit kaum als offizielle Bestätigung gelten. Dafür erschiene eher das Original-*Dokument* mit seinen behördlichen Kennzeichnungen als Verschlusssache geeignet, das in Augenschein genommen werden könnte. Erst dadurch wäre eine sichere Beurteilung der Authentizität möglich.

Nach alledem ist festzustellen, dass zum Zeitpunkt der Veröffentlichung der Auszüge aus dem BfV-Wirtschaftsplan diesbezüglich bereits kein Staatsgeheimnis mehr vorlag.

b) Vorveröffentlichungen und „EFI-Konzept"

Auch in Bezug auf das „EFI-Konzept" sind Vorveröffentlichungen vorfindlich. Die umfangreichste Publikation erscheint am 28.6.2014 in der Zeitung „Neues Deutschland" unter dem Titel „Verfassungsschutz lässt EFI aufs Internet los".[46] Ein Hinweis auf die Herkunft des Konzepts oder seinen Geheimhaltungsgrad findet sich nicht. Insoweit besteht im Vergleich zu den Vorveröffentlichungen über den BfV-Wirtschaftsplan eine etwas stärkere Unverbindlichkeit der Information.

Mehrere Textpassagen aus der Verschlusssache werden entweder wörtlich übernommen oder geringfügig paraphrasiert:

> *Bsp.: „Die Informationssammlung und Auswertung in Bezug auf das Internet soll ‚eine strategische und organisatorische Neuaufstellung' erfahren. (...). Es geht um die strategische, technische und rechtliche Entwicklung neuer Methoden der Informationsauswertung und-analyse und eine zentralisierte Analyse aller im BfV vorhandenen Daten. (...) Das betreffe sowohl die Aufbereitung der klassischen Telefonie (Sprache, Telefax, SMS) wie die Internetkommunikation (E-Mail, Chatprotokolle, Websessions und Datentransfere).*"

Im Vergleich zum Original bleibt es überwiegend bei einer stark verkürzten Darstellung. Zur Funktionsweise der Telekommunikationsüberwachungsanlage PERSEUS hält sich der Artikel beispielsweise bedeckt, obgleich in der Verschlusssache detailliertere Ausführungen gemacht werden, wie z.B.:

44 *Lampe/Hegmann*, in: MüKo (Fn. 24), § 93 Rn. 9; *Rudolphi/Pasedach/Wolter*, in: SK StGB (Fn. 27), § 93 Rn. 11.

45 Vgl. *Paeffgen*, in: NK (Fn. 24), § 93 Rn. 18.

46 *Heilig*, Verfassungsschutz lässt EFI aufs Internet los, abrufbar unter: http://www.neues-deutschland.de/artikel/937366.verfassungsschutz-laesst-efi-aufs-internet-los.html (Stand: 12.2.2016).

> *„Ein Teil der gewonnenen Rohdaten wird den G10-Auswerter/-innen von PERSEUS automatisch aufbereitet und lesbar zur Verfügung gestellt. Jedoch bedarf es zum Auffinden und zur Darstellung bestimmter Informationen aus den Individualüberwachungsmaßnahmen (z.B. eines Facebook-Chats) speziellerer Kenntnisse (...). Ein Teil der Rohdaten kann von der PERSEUS-Anlage nicht automatisiert dekodiert werden."*

Teilweise wirken die journalistischen Verkürzungen sinnentstellend. Ein Beispiel: Im Presseartikel heißt es:

> *„Es geht um die strategische, technische und rechtliche Entwicklung neuer Methoden der Informationsauswertung und -analyse und eine zentralisierte Analyse aller im BfV vorhandenen Daten. Dabei setzt man zum einen auf die Kompetenz des Strategie- und Forschungszentrums Telekommunikation, das im Bereich des Bundesinnenministeriums bereits 2011 gebildet wurde. Zum anderen will der Verfassungsschutz die Möglichkeiten der Telekommunikationsüberwachung (...) ausbauen."*

Der Originalwortlaut gibt diese Erkenntnis kaum her. Das zuletzt genannte Zentrum wird lediglich am Rande erwähnt:

> *„Für die vorgenannten Aufgaben wird das Referat 3 C 1 zentraler Ansprechpartner im BfV. Dies umfasst auch Kontakte zu LfV und anderen Sicherheitsbehörden sowie die Zusammenarbeit mit dem Strategie und Forschungszentrum Telekommunikation (SFZTK)."*

Insgesamt gesehen bleiben die Ausführungen der Vorveröffentlichung insofern überwiegend oberflächlich. Nahezu keine Aufmerksamkeit wird der organisatorischen Struktur der Referatsgruppe geschenkt. Insbesondere der detaillierte Personalplan, der je Referat Aufgaben und konkreten Personalbedarf ausweist, kommt nicht zur Sprache. Das Geheimnis wird daher über die Vorveröffentlichung nur unvollständig, teilweise sogar missverständlich wiedergegeben. Infolgedessen bleibt der Geheimnischarakter jedenfalls insoweit erhalten und geschützt.[47]

4. Zwischenergebnis

Der BfV-Wirtschaftsplan 2013 hat – jedenfalls so weit er auf der Website von „netzpolitik.org" veröffentlicht wurde – infolge der Vorveröffentlichungen seine begrenzte Zugänglichkeit eingebüßt und kann demgemäß nicht (mehr) als Staatsgeheimnis i.S.v. § 93 StGB gelten. Anders verhält es sich bei dem „EFI-Konzept". Hier bleibt trotz der vorangegangenen Presseberichterstattung eine wesentliche substanzielle Aussage vor der Öffentlichkeit verborgen und insofern geheimhaltungsfähig.

III. Geheimhaltungsbedürftigkeit

Über die begrenzte Zugänglichkeit hinaus verlangt § 93 StGB, dass die Tatsache oder die Erkenntnis auch geheimhaltungsbedürftig ist. Die Geheimhaltung des „EFI-Konzepts" vor einer fremden Macht muss erforderlich sein, um die Gefahr

47 Dazu siehe *Jescheck*, Pressefreiheit (Fn. 23), S. 25 f. Der BGH lässt eine glaubwürdige Bestätigung der zuvor verratenen Informationen für einen Geheimnisverrat ausreichen, vgl. BGHSt 20, 342 (377, 383); ausführlich dazu *Kohlmann*, Begriff des Staatsgeheimnisses (Fn. 23), S. 95 ff.

eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden.

1. Erforderliche Sekretur vor fremder Macht

Die Geheimhaltungserforderlichkeit besteht vor einer fremden Macht. Damit sind Einrichtungen gemeint, die sich auf höchster Ebene in öffentlicher „Machtfülle" repräsentieren und außerhalb des Geltungsbereichs des deutschen Grundgesetzes stehen,[48] was regelmäßig auf ausländische Regierungen zutrifft. Mit dem Aufbau der „Erweiterten Fachunterstützung Internet" beabsichtigt das BfV insbesondere die Verbesserung der Überwachung von internetgestützter Individualkommunikation. Vor allem die zunehmend größer werdenden Datenmengen im Internet sollen mit Hilfe der Einrichtung der neuen Referatsgruppe bewältigt werden. Für nicht wenige ausländische Regierungen sind verlässliche Detailinformationen über solche Vorhaben von einigem Interesse, lassen sie doch Rückschlüsse u.a. darüber zu, auf welchem Niveau sich die deutsche Spionageabwehr – qualitativ wie quantitativ – befindet.[49] Sie fällt in den Zuständigkeitsbereich des Verfassungsschutzes.[50] Das Leistungspotential des BfV in dieser Hinsicht wird etwa durch die Offenlegung von organisatorisch-technischen Defiziten oder konkreten Methoden der Informationsgewinnung deutlich:

> *Bsp.: „Die sich ständig verändernden Kommunikationsformen (...) erfordern in Bezug auf die Informationssammlung (...) eine strategische und organisatorische Neuausrichtung des BfV. Ferner soll die Referatsgruppe (...) die Analyse von allen dem BfV aus unterschiedlichen Quellen zugänglichen Daten, die im digitalen Zeitalter aufgrund ihres Umfangs oft nicht mehr manuell ausgewertet werden können, umfassen. (...) Ein Teil der Rohdaten kann von der PERSEUS-Anlage nicht automatisiert dekodiert werden."*

Insbesondere der Personal- und Mittelansatz, der im Detail über den Personalplan des „EFI-Konzepts" ausgedrückt wird, spiegelt das Leistungsvermögen des Verfassungsschutzes wieder. Ausländischen Nachrichtendiensten und ihren Regierungen offenbaren sich auf diese Weise Schwachstellen in der „Counterintelligence". Von Bedeutung ist dieser Umstand insbesondere auch, soweit es der „EFI-Referatsgruppe" obliegt, an der Aufklärung von „Cyber-Angriffen" mitzuwirken.

> *Der BfV-Wirtschaftsplan 2013 umreißt diese Aufgabe der Referatsgruppe näher: „Weiterhin nimmt die Komplexität Elektronischer Angriffe durch fremde Nachrichtendienste zu. Dies betrifft sowohl den Aufbau der eingesetzten Software als auch die Identifizierungsmöglichkeiten der Urheber. Um diesen Angriffen adäquat begegnen zu können, ist eine entsprechend leistungsfähige IT-Infrastruktur erforderlich, mittels derer sich Elektronische Angriffe analysieren und zurückverfolgen und dadurch wirksamer als bisher abwehren lassen."*

48 Vgl. *Schmidt*, in: LK (Fn. 25), § 93 Rn. 10.

49 Zum Potential von „Leaks" siehe näher *Lowenthal*, Intelligence – From Secrets to Policy, 6th edition, Los Angeles 2015, pp. 204 et seqq.

50 Siehe ausführlich *Droste*, Handbuch des Verfassungsschutzrechts, Stuttgart 2007, S. 125 ff.

Dem BfV kommt demgemäß die Aufgabe zu, die Urheber der grundsätzlich anonymen Attacken zu identifizieren.[51] Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) fehlen hierfür die notwendigen operativen Mittel; eine entsprechende Rechtsgrundlage gibt es nicht. Der „Cyber-Angriff" auf informationstechnische Systeme des Deutschen Bundestags[52] im Sommer 2015 hat eindrücklich vor Augen geführt, dass Schwächen in der IT-Sicherheit feindselig ausgenutzt werden können. Das BSI geht in seinem Lagebericht zur IT-Sicherheit 2014 davon aus, dass allein das Regierungsnetz zwischen 15 und 20 Mal pro Tag Ziel von Cyberangriffen war, die mit herkömmlichen Schutzmaßnahmen nicht mehr hätten abgewehrt können; mindestens einer dieser Angriffe sei mit nachrichtendienstlichem Hintergrund erfolgt.[53] Ohne die zuverlässige „Attribution" der Angreifer, ohne die Identifizierung ihrer Motivation lassen sich keine wirksamen Gegenmaßnahmen ergreifen.[54] Die Kenntnis der Cyberabwehrfähigkeit des BfV verschafft daher potentiellen Angreifern erhebliche Vorteile. Insoweit war die Geheimhaltung des Leistungspotentials des BfV vor einer fremden Macht erforderlich.

Es spricht einiges dafür, von der Notwendigkeit der Sekretur auch gegenüber „fremden Mächten" auszugehen, die nicht als ausländische Regierungen angesehen werden können. Weitgehende Einigkeit besteht in der Literatur, dass Exilregierungen oder Aufständische innerhalb eines fremden Staatsgebiets eine fremde Macht darstellen können, sofern sie staatliche Funktionen ausüben wollen und dazu – zumindest teilweise – in der Lage sind.[55] Soweit ausländische terroristische oder kriminelle Vereinigungen ein vergleichbares objektives Bedrohungspotential entfalten, entspricht es dem Schutzzweck der Norm, diese ausnahmsweise gleichfalls als fremde Mächte anzusehen.[56] In Bezug auf das Bedrohungspotential wird von Teilen der Literatur gefordert, dass die jeweilige Gruppierung eine über kleinräumige lokale Bereiche hinausgehende Macht zu regionaler Herrschaftsausübung besitzt.[57] Zumindest im Falle des „Islamischen Staates" (IS) ist ein erhebliches objektives Be-

51 BMI (Hrsg.), Verfassungsschutzbericht 2014, S. 142 ff.

52 Siehe dazu *Busse*, Die wahre Bedrohung, FAZ vom 11.6.2015, abrufbar unter: http://www.faz.net/aktuell/politik/cyberangriff-auf-den-bundestag-die-wahre-bedrohung-13642293.html (Stand: 12.2.2016).

53 BSI, Die Lage der IT-Sicherheit in Deutschland 2014, S. 28.

54 Vgl. *Gaycken*, Cyberwar, München 2011, S. 80 f.

55 *Schmidt*, in: LK (Fn. 25), § 93 Rn. 10.

56 Dazu überzeugend *Lampe/Hegmann*, in: MüKo (Fn. 24), § 93 Rn. 15.

57 So *Paeffgen*, in: NK (Fn. 24), § 93 Rn. 22.

drohungspotential nicht zu übersehen.[58] Die Bedrohung, die vom IS für die Bundesrepublik ausgeht, lässt sich gegenwärtig nicht in den Kategorien einer militärischen Auseinandersetzung erfassen. Die jüngsten Anschläge von Paris haben aber erneut die Strategie des IS vor Augen geführt, den „Dschihad" direkt in das öffentliche Leben westlicher Staaten zu tragen.[59] Seit langem ist bekannt, dass soziale Netzwerke bevorzugte Kommando- und Kontrollzentren des IS darstellen.[60] Auch Online-Spiele wie „World of Warcraft" oder „Second Life" dienen der internen Kommunikation.[61] Hinzu kommt, dass Whatsapp, Twitter oder Facebook durch den IS als Propagandaplattformen genutzt werden.[62] Sie tragen maßgeblich zur Radikalisierung von Muslimen in westlichen Staaten bei.[63] Offen, gelegentlich verklausuliert, wird auf diesem Wege zu Anschlägen aufgefordert.[64] Das objektive Bedrohungspotential des IS darf nach alledem als erheblich gelten. Er ist deshalb als „fremde Macht" i.S.v. § 93 Abs. 1 StGB anzusehen, vor der die Geheimhaltung des Leistungspotentials des BfV erforderlich war.

2. Äußere Sicherheit der Bundesrepublik Deutschland

Das Geheimhaltungserfordernis muss sich auf die Gewährleistung der äußeren Sicherheit der Bundesrepublik beziehen. Angesprochen ist damit die Fähigkeit des Staates, sich gegen äußere Angriffe, Pressionen, Eingriffe, Störungen und ähnliche (evtl. verdeckte) Einflussnahmen zu wehren, um seine Machtstellung auf interna-

58 Das Einflussgebiet des IS umfasste im Dezember 2015 insgesamt ca. 78.000 km^2. Vgl. dazu *Schulte von Drach*, Der Islamische Staat schrumpft, SZ vom 12.2.2016, abrufbar unter: http://www.sueddeutsche.de/politik/rueckschlaege-fuer-terroristen-der-islamische-staat-schrumpft-1.2795410 (Stand: 12.2.2016). Nach Angaben *des Internationalen Komitees vom Roten Kreuz* lebten dort im vergangenen Jahr mehr als 10 Millionen Menschen. Vgl. IKRK-Präsident *Maurer* im Interview in der ZEIT vom 1.4.2015, abrufbar unter: http://www.zeit.de/2015/14/rotes-kreuz-internationales-komitee (Stand: 12.2.2016). Soweit bekannt ist, wird die Machtausübung im Inneren hierarchisch organisiert. Herzstück des Regimes sind insgesamt neun Räte, die direkt der Führungsebene unterstellt sind (z.B. Militärrat, Rechtsrat, Schurarat) und die Funktion von Ministerien übernehmen. Lokal wird die Macht des IS über Regionalregierungen mit Bürgermeistern oder Gouverneuren gesichert. Siehe ausführlich *Cronin*, ISIS is not a terrorist group, Foreign Affairs Vol. 94 No. 2 (4/5 2015), pp. 87-101; *Abu Hanieh/Abu Rumman*, The „Islamic State" Organization, Amman 2015, pp. 265 et seqq.

59 Vgl. *Krüger*, Der IS trägt den Krieg zu seinen Feinden, SZ vom 14.11.2015, abrufbar unter: http://www.sueddeutsche.de/politik/islamischer-staat-wie-der-is-den-krieg-zu-seinen-feinden-traegt-1.2737553 (Stand: 12.2.2016).

60 Siehe *Leyendecker/Mascolo*, Die Macht der Terror-Tweets, SZ vom 24.1.2015, abrufbar unter: http://www.sueddeutsche.de/digital/islamismus-die-macht-der-terror-tweets-1.2318119 (Stand: 12.2.2016).

61 Siehe *Gruber/Tanriverdi*, Hacker drohen IS mit Vergeltung, SZ vom 17.11.2015, abrufbar unter: http://www.sueddeutsche.de/digital/terror-in-paris-hacker-erklaeren-is-den-cyberkrieg-1.2740630 (Stand: 12.2.2016).

62 Näher dazu *Wolf*, Big Data und Innere Sicherheit, Marburg 2015, S. 39 f.

63 Vgl. BMI (Hrsg.), Verfassungsschutzbericht 2014, S. 96.

64 Siehe näher *Leyendecker/Mascolo*, Die Macht der Terror-Tweets, SZ vom 24.1.2015, abrufbar unter: http://www.sueddeutsche.de/digital/islamismus-die-macht-der-terror-tweets-1.2318119 (Stand: 12.2.2016).

tionaler Ebene relativ ungefährdet zu erhalten.[65] In welcher Weise die äußere Machtposition nachteilig berührt wird, ist ohne Belang. Zu einer negativen Veränderung der deutschen Machtposition auf internationaler Ebene kann sowohl der Verrat militärischer Geheimnisse beitragen als auch der Verrat nachrichtendienstlicher oder wirtschaftlicher Geheimnisse.[66] Diese weite Auslegung des Begriffs der „äußeren Sicherheit" legt nicht zuletzt die verfassungsgerichtliche Judikatur nahe: In seiner Entscheidung zur strategischen Fernmeldeüberwachung durch den Bundesnachrichtendienst hat das Bundesverfassungsgericht betont, dass auch der internationale Drogen- und Waffenhandel sowie Proliferation und Geldwäsche in währungsgefährdenden Dimensionen von der staatlichen Gewährleistung äußerer Sicherheit erfasst werden.[67]

Nachrichtendienstliche Nachteile sind nicht notwendigerweise zugleich auch solche für die äußere Sicherheit. Nicht jede Information über Arbeitsweisen der Nachrichtendienste betrifft die Machtstellung der Bundesrepublik in der Welt.[68] Die Bedeutung der Cyber-Kompetenz des BfV für die Gewährleistung der äußeren Sicherheit ist allerdings kaum zu übersehen: Die allermeisten Cyberattacken[69] erfolgen aus dem Ausland. Aus der Distanz sind sie weitgehend risikolos. Die Angriffsmittel sind kostengünstig und weltweit jederzeit verfügbar. Sie können parallel eingesetzt und oft nur unter größtem Aufwand zurückverfolgt[70] werden. Das Schädigungspotential ist so enorm, dass manche Cyberattacken die Qualität von Verletzungen des Interventionsverbots gem. Art. 2 Nr. 7 UN-Charta bzw. sogar von Verletzungen des Gewaltverbots gem. Art. 2 Nr. 4 UN-Charta erreichen können.[71] Es liegt auf der Hand, dass die äußere Sicherheit eines Staates, der hierfür keine sinnvolle Prävention betreibt, nicht gewährleistet sein kann. Die Geheimhaltung der Cyberabwehr-Fähigkeiten des BfV betraf insoweit die äußere Sicherheit. Gleiches gilt für die „Social-Media-Intelligence"- (SOCMINT)[72] Kompetenzen der Behörde. Terroristische Anschläge wie in New York, London, Madrid und Paris

65 Vgl. Schmidt, in: LK (Fn. 25), § 93 Rn. 13; *Sternberg-Lieben*, in: *Schönke/Schröder*, StGB, 29. Aufl. 2014, § 93, Rn. 17.

66 BGHSt 24, 72 (74 f.) = BGH NJW 1971, S. 715 (715 f.); BayObLGSt 1991, S. 127 (129); *Lüttger*, Staatsschutzstrafrecht (Fn. 22), S. 126; *Woesner*, Neues Staatsschutzstrafrecht (Fn. 22), S. 2133; *Laufhütte*, Staatsgeheimnis (Fn. 22), S. 56; *v. Weber*, Der Begriff des Staatsgeheimnisses, JZ 1964, S. 127 ff.; *Sternberg-Lieben*, in: *Schönke/Schröder* (Fn. 65), § 93, Rn. 17.

67 BVerfGE 100, 313 (371).

68 *Lampe/Hegmann*, in: MüKo (Fn. 24), § 93 Rn. 20; *Rudolphi/Pasedach/Wolter*, in: SK StGB (Fn. 27), § 93 Rn. 27; *Schmidt*, in: LK (Fn. 25), § 93 Rn. 13.

69 Näher dazu *Schulze*, Cyber-„War" – Testfall der Staatenverantwortlichkeit, Tübingen 2015, S. 13 ff.; *Gaycken*, Cyberwar (Fn. 54), S. 192 ff.; *Borchert/Rosenkranz/Ebner*, Cybersicherheit in Österreich, in: *Lange/Bötticher* (Hrsg.), Cyber-Sicherheit, Wiesbaden 2015, S. 121, 129.

70 Zur Rückverfolgungsproblematik („Clearing" bzw. Attribution) siehe *Schulze*, Cyber-„War" (Fn. 69), S. 36 ff.

71 Siehe *Schulze*, Cyber-„War" (Fn. 69), S. 123 ff.

72 Siehe ausführlich *Omand/Bartlett/Miller*, Intelligence and National Security Vol. 27, Issue 6 /2012, pp. 1 et seqq.

sollen die jederzeitige Verwundbarkeit westlicher Staaten vor Augen führen und ihre politischen Entscheidungsträger zu bestimmten außenpolitischen Handlungen veranlassen.[73] Auch in diesen Dimensionen ist die äußere Sicherheit tangiert. Die Aufklärungstätigkeit von Nachrichtendiensten in sozialen Medien dient jedenfalls insoweit dem Schutz der Bundesrepublik,[74] wie diese nachweislich eine zentrale Rolle bei der Anschlagsvorbereitung spielen.

3. Abwendung der Gefahr eines schweren Nachteils

Schließlich verlangt § 93 Abs. 1 StGB, dass die Geheimhaltung des „EFI-Konzepts" geboten gewesen sein müsste, um die Gefahr eines schweren Nachteils für die äußere Sicherheit abzuwenden.

a) Tatrichterliche Entscheidung und sachverständige Expertise

Ob der Verrat einer geheimen Information ein solches Potential aufweist, ist eine Frage tatsächlicher Natur, die nur vom Tatrichter zu beantworten ist.[75] Dem Tatrichter wird eine Risikoeinschätzung und -bewertung übertragen, für die im Verwaltungsrecht üblicherweise ein exekutiver Beurteilungsspielraum besteht. Wann beispielsweise „zwingende Gründe der Verteidigung" i.S.v. § 3 Abs. 2 UVPG vorliegen, bedarf einer vorausschauenden militärfachlichen Einschätzung, zu der in erster Linie die Bundeswehr in der Lage ist.[76] Im Fall der von § 93 Abs. 1 StGB geforderten Prognose ist der Richter dagegen oft gezwungen, sachverständigen Rat in Anspruch zu nehmen.[77] Im nachrichtendienstlichen Bereich besteht hierbei die Schwierigkeit, dass der notwendige Sachverstand und das durch praktische Erfahrung geschärfte Urteilsvermögen zunächst in den Nachrichtendiensten selbst zu finden sind. Sie stehen im Lager des Geschädigten. Als Sachverständige einbezogene Mitarbeiter/-innen der Dienste sind im formellen Sinne nicht unabhängig; ihre sachliche Unabhängigkeit ist nicht einfach zu gewährleisten.[78] Mit überzeugenden Argumenten kommt deshalb in Betracht, eine sachverständige Expertise außerhalb der Sicherheitsverwaltung – etwa in Wissenschaft oder Justiz – zu suchen.[79] Zu be-

73 Siehe hierzu etwa Auszug aus dem Bekennerschreiben des IS bezüglich der Anschläge in Paris: „Que la France et ceux qui suivent sa voie sachent qu'ils resteront à la tête des cibles de l'Etat islamique". Volltext abrufbar unter: http://www.leparisien.fr/faits-divers/le-groupe-etat-islamique-revendique-les-attentats-de-paris-14-11-2015-5276369.php#xtref=https%3A%2F%2Fwww.google.de%2F (Stand: 12.2.2016).

74 Zur Bedeutung der Aufklärungstätigkeit der Nachrichtendienste für die Gewährleistung äußerer Sicherheit siehe BGH NJW 1991, S. 2498 (2499); BayObLGSt 1991, S. 127 (133).

75 Vgl. BGHSt 24, 72 (75); näher *Willms*, Der Sachverständige im Landesverratsprozess, NJW 1963, S. 190 (190 f.); *Arndt*, Das Staatsgeheimnis als Rechtsbegriff und als Beweisfrage, NJW 1963, S. 465 (469).

76 Vgl. dazu BVerwG NJW 1994, S. 535; 1995, S. 1690 (1691 f.); OVG Münster NVwZ-RR 1990, S. 177.

77 Kritisch dazu *Paeffgen*, in: NK (Fn. 24), § 93 Rn. 20.

78 Zur Rolle von Behördenangehörigen als Sachverständigen siehe etwa BVerfG NJW 1966, 1603 (1612) sowie *Willms*, Sachverständige (Fn. 75), S. 191; *Jescheck*, Pressefreiheit (Fn. 23), S. 32 f.

79 Vgl. *Willms*, Sachverständige (Fn. 75), S. 191; *Arndt*, Staatsgeheimnis (Fn. 75), S. 469.

achten ist indes dabei, dass selbst eine hohe fachliche Kompetenz externer Sachverständiger praktische Erfahrungswerte nicht ersetzen kann. Deshalb werden auch unabhängige Sachverständige regelmäßig gehalten sein, sich die nachrichtendienstliche Praxis im Dialog mit den Diensten zu erschließen, um das Gewicht des Nachteils i.S.v. § 93 StGB umfassend würdigen zu können. Da die Untersuchung im vorliegenden Fall allein auf offen verfügbaren Informationen basiert, ist die nachrichtendienstliche Praxis insoweit zu berücksichtigen, wie sie sich bisher in ähnlich gelagerten Judikaten niedergeschlagen hat oder in der Fachliteratur Erwähnung findet.

b) Gefahr eines schweren Nachteils durch Offenlegung nachrichtendienstlicher Organisationsstrukturen

Der Gefahrbegriff des § 93 Abs. 1 StGB knüpft an eine abstrakte Gefährlichkeit: Es kommt darauf an, ob allgemein gesehen das Bekanntwerden der Tatsachen oder Erkenntnisse bei einer fremden Macht geeignet ist, einen schweren Nachteil herbeizuführen.[80] Die fremde Macht müsste insofern über verbesserte Möglichkeiten verfügen.[81] In Bezug auf den schwerwiegenden Nachteil für die äußere Sicherheit wird auf die Anfälligkeit des Gesamtstaates Bundesrepublik Deutschland abgestellt, namentlich vor Gefahren, denen nicht mehr mit innerstaatlichen Mitteln – insbesondere mit solchen des Polizeirechts – begegnet werden kann und die Auswirkungen auf Sachverhalte haben, die von Einfluss auf die nationale Sicherheit sind.[82] Im nachrichtendienstlichen Bereich wird ein schwerwiegender Nachteil insbesondere bei Offenlegung von personellen und organisatorischen Strukturen der Behörden angenommen, wenn mit ihrer Kenntnis gleichzeitig der Einblick in Details der Aufgabenverteilung und Zuständigkeiten verbunden ist.[83] Bei einem geringen nachrichtendienstlichen Wert der Information ist ein gewichtiger Nachteil freilich ausgeschlossen.[84]

Das veröffentlichte „EFI-Konzept“ enthält im Anhang einen detaillierten Personalplan, der für jedes Referat Personalansatz, Laufbahngruppenzugehörigkeit, Aufgaben und Arbeitszeitbelastung ausweist.

80 *Schmidt*, in: LK (Fn. 25), § 93 Rn. 14.

81 *Lampe/Hegmann*, in: MüKo (Fn. 24), § 93 Rn. 24.

82 So *Lampe/Hegmann*, in: MüKo (Fn. 24), § 93 Rn. 25.

83 So ausdrücklich BayObLGSt 1991, S. 127 (129 f.); wohl ebenso *Paeffgen*, in: NK (Fn. 24), § 93 Rn. 26. Ausführlich *Schmidt*, in: LK (Fn. 25), § 93 Rn. 14. Beispiele aus früher Rechtsprechung bei *Wagner*, GA 1968, S. 291 (294).

84 Vgl. BGHSt 20, 342 (381); BGH NJW 1965, S. 1191. Der Plan einer Botschafterkonferenz ist etwa von geringem nachrichtendienstlichen Wert. Die damit verbundene Erkenntnis berührt den Gesamtstaat nicht. Vgl. *Träger/Mayer/Krauth*, Das neue Staatsschutzrecht in der Praxis, in: FS BGH, München 1975, S. 227 (244 f.).

Bsp.: „Referat 3C6: Informationstechnische Operativmaßnahmen, IT-forensische Analysemethoden (...)

3C6: Unkonventionelle TKÜ[85]

Tage	Laufbahn	Aufgabe
297	gD	Technische Beratung von Bedarfsträgern in operativen Angelegenheiten des BfV (...)
36	gD	Einsatzdurchführung von Operativmaßnahmen des BfV zur verdeckten Informationserhebung über Computernetze (...)
248	mD	Betrieb von konspirativen technischen Strukturen (...)“

Was Außenstehenden auf den ersten Blick als banale Verwaltungsorganisation erscheinen mag, birgt bei näherer Betrachtung – zusammen mit weiteren Ausführungen im „EFI-Konzept“ – einen nicht unerheblichen nachrichtendienstlichen Informationswert. Es wird im Detail offengelegt, mit welchem Ressourcenansatz das BfV dem erklärten Bedrohungsszenario begegnen will und welche Schwerpunkte dabei gesetzt werden sollen. Ein Beispiel: Das Referat 3C2 (Inhaltliche/technische Auswertung von G10-Informationen) soll insgesamt über neun Mitarbeiter/-innen verfügen. Aus der Angabe der Laufbahngruppenzugehörigkeit lässt sich deren Vorbildung erkennen, etwa inwieweit eine akademische Qualifikation besteht. Zieht man jeweils die Aufgabenbeschreibungen hinzu, lässt sich ein fachliches Kompetenzprofil je Referat konturieren. Auch Priorisierungen der nachrichtendienstlichen Aufklärung sind leicht identifizierbar: Dem oben erwähnten Referat 3C2 in Köln ist die Bearbeitung von Daten aus G-10-Beschränkungsmaßnahmen in den Bereichen Rechtsextremismus/-terrorismus, Geheim- und Sabotageschutz, Spionageabwehr, Ausländerextremismus sowie Linksextremismus/-terrorismus übertragen. Das Referat 3C3 in Berlin – von Größe und Aufgabe identisch – wertet dagegen allein Daten aus dem Bereich Islamismus und islamischer Terrorismus aus. Interessierten Fachkreisen im Ausland wird durch solche Zusammenhänge das Leistungsvermögen des BfV – im Detail – offenbart. Ausländische Nachrichten- und Geheimdienste werden dadurch in die Lage versetzt, die (technische) Auswertungs- und Abwehrkompetenz des BfV besser beurteilen zu können. Mit Blick auf das hohe Aufkommen geheim- und nachrichtendienstlicher Aktivitäten fremder Staaten in der Bundesrepublik ist das nicht unproblematisch. Jährlich dokumentiert der Verfassungsschutzbericht ein geheim- und nachrichtendienstliches „Grundrauschen“ auf deutschem Boden:[86] Im Fokus der Informationsbeschaffung ausländischer Dienste stehen z.B. Erkenntnisse über die deutsche Außen- und Sicherheitspolitik oder über militärische Fähigkeiten der Bundeswehr (insb. Militärtechnik).

85 TKÜ = Telekommunikationsüberwachung.

86 Siehe z.B. BMI (Hrsg.), Verfassungsschutzbericht 2014, S. 140 ff.

Auch technisches Know-How in der zivilen Wirtschaft oder Exiloppositionelle sind Ausforschungsziele. Hinter den Aktivitäten stehen keinesfalls allein große Staaten von bedeutendem internationalen Einfluss (wie z.B. China oder Russland). Auch Dienste kleinerer Staaten sind in Deutschland tätig. Sie können ihre Operationen nur begrenzt auf eigene Auswertungsergebnisse stützen, da ihnen für eine professionelle „Intelligence Analysis" oftmals Kapazitäten und Infrastruktur fehlen. Zuverlässige Erkenntnisse über die Spionageabwehrfähigkeit des BfV sind demgemäß für solche Dienste von besonderem Interesse. Gleiches dürfte für terroristische Gruppierungen wie den IS gelten, die ein hohes Bedrohungspotential aufweisen. Die Kenntnis des Leistungsvermögens des BfV eröffnet den genannten Gegnern die Möglichkeit, den Einsatzwert und die Schlagkraft der Referatsgruppe zu mindern,[87] indem effektivere Operationen angelegt werden können. Die Gefahr eines schweren Nachteils für die äußere Sicherheit sollte somit durch die Geheimhaltung des „EFI-Konzepts" verhindert werden.

Der qualifizierte nachrichtendienstliche Nachteil ist von Bedeutung für die Anfälligkeit des Gesamtstaats. Eine verminderte nachrichtendienstliche Cyberkompetenz kann z.B. unbemerkte Vorbereitungshandlungen für Terroranschläge mit Toten und Verletzten wie zuletzt in Paris erleichtern. Auch ausländischen Cyberattacken mit staatsgefährdendem Ausmaß kann Vorschub geleistet werden. Dies gilt beispielsweise für sog. „Denial-of-Server (DoS) -Angriffe".[88] Mindestens einmal im Monat verzeichnet das BSI einen solchen Angriff auf Webseiten von Bundesbehörden. Bekannt geworden ist v.a. die DoS-Attacke in Estland aus dem Jahr 2007, die Banken, Behörden und Regierung – betroffen war u.a. die Notrufnummer – über mehrere Tage lahmlegte. Die estnische Regierung sollte auf diese Weise zu Zugeständnissen an die russische Minderheit im Land gezwungen werden. Völkerrechtlich sind solche Angriffe regelmäßig als unzulässige Einmischung in innere Angelegenheiten zu qualifizieren. Sie verstoßen gegen das gewohnheitsrechtlich anerkannte Interventionsverbot nach Art. 2 Nr. 7 UN-Charta.[89] Weitaus schwerwiegender können sich elektronische Angriffe auf sog. kritische Infrastrukturen (z.B. Elektrizitäts- oder Wasserversorgung) ausnehmen.[90] Die britische Regierung warnte in

87 Wertungsmäßig besteht kein Unterschied zur Mitteilung waffentechnischer Entwicklungen, vgl. BayObLGSt 1993, S. 39 (40 ff.).

88 Bei DoS-Attacken werden einzelne Adressen in einer gigantischen Menge angefragt, was sie regelmäßig darüber zusammenbrechen lässt. Benutzt werden dafür insbesondere sog. „Botnets", durch versteckte Schadsoftware infiltrierte Rechner in aller Welt, die sich ferngesteuert an den Angriffen beteiligen. Siehe *Schulze*, Cyber-„War" (Fn. 69), S. 26; *Gaycken*, Cyberwar (Fn. 54), S. 169 ff.

89 Vgl. *v. Arnault*, Völkerrecht, 2. Auflage, Heidelberg 2014, Rn. 1013.

90 Das Potential solcher Cyberangriffe führt das 2010 an die Öffentlichkeit gelangte Beispiel des Computerwurms „Stuxnet" vor Augen, mit dessen Hilfe iranische Atomzentrifugen zur Urananreicherung sabotiert wurden. Das US-amerikanisch-israelische Schadprogramm veränderte die Rotationsgeschwindigkeit der Zentrifugen und führte gleichzeitig dem Steuerungsprogramm fehlerhafte Daten zu, was letztlich die physische Zerstörung der Zentrifugen bedeutete. Vgl. *Gaycken*, Cyberwar (Fn. 54); S. 175 ff.; *Schulze*, Cyber- „War" (Fn. 69), S. 16 f. m.w.N.

diesem Zusammenhang kürzlich vor elektronischen Angriffen des IS auf Krankenhäuser oder die Flugverkehrskontrolle mit tödlichen Folgen.[91] Mit Blick auf derart schwerwiegende Konsequenzen eines Cyberangriffs geht die NATO mittlerweile davon aus, dass ein Cyberangriff einer gewissen Größenordnung[92] den Bündnisfall i.S.v. Art. 5 des NATO-Vertrags auszulösen vermag.[93] Vor dem aufgezeigten Hintergrund birgt der qualifizierte nachrichtendienstliche Nachteil die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik.

c) Saldierende Gesamtbetrachtung

Nach überwiegender Auffassung sind bei der Prüfung, ob ein schwerwiegender Nachteil für die äußere Sicherheit droht, die durch die Preisgabe des Geheimnisses erreichbaren Vorteile zu berücksichtigen.[94] Es ist demnach eine Saldierung geboten, um die Erheblichkeit des Schadens beurteilen zu können.[95] Ein erheblicher Schaden kann beispielsweise ausscheiden, wenn zwar infolge des Bekanntwerdens des Geheimnisses die Sicherheitsposition zu *einem* Staat geschwächt, zu einem *anderen* Staat aber gestärkt werden würde. Allerdings müssen in der Saldierung innenpolitische Vorteile außer Acht bleiben.[96] Sie sind vom Schutzgut „äußere Sicherheit" nicht erfasst.[97] Vorteile für die äußere Sicherheit, die sich aus der Offenbarung des „EFI-Konzepts" ergeben, sind nicht ersichtlich.

4. Verfassungskonforme Auslegung

§ 93 StGB enthält keine Rechtsfolge, sondern lediglich eine Legaldefinition des Staatsgeheimnisbegriffs. Es handelt sich insofern um eine Hilfsnorm, die erst im Zusammenhang mit den §§ 94 ff. StGB eine vollständige Regelung ergibt. Durch die Verknüpfung der Legaldefinition mit jeweils dem Tatbestand und der Rechtsfolge von §§ 94 ff. StGB wird die Auslegung des Staatsgeheimnisbegriffs praktisch relevant. Die in der Norm enthaltenden unbestimmten Rechtsbegriffe wie etwa „äußere Sicherheit" oder „schwerer Nachteil" sind verschiedenen Deutungen zu-

91 In der britischen Zeitung „The Guardian" wird der britische Finanzminister *George Osborne* mit den Worten zitiert: „Let's be clear. Isil are already using the internet for hideous propaganda purposes; for radicalisation, for operational planning too. They have not been able to use it to kill people yet by attacking our infrastructure through cyber-attacks. They do not yet have that capability. But we know they want it, and are doing their best to build it". Abrufbar unter: http://www.theguardian.com/uk-news/2015/nov/17/uk-hit-back-terrorists-cyber-attacks-george-osborne-gchq (Stand: 12.2.2016),.

92 Siehe hierzu auch insbesondere das *Schmitt* (Hrsg.), Tallinn Manual on International Law Applicable to Cyber Warfare, Cambridge 2013.

93 SZ-Meldung vom 11.6.2015, abrufbar unter: http://www.sueddeutsche.de/news/wirtschaft/internet-nato-cyberangriff-koennte-gemeinsame-verteidigung-ausloesen-dpa.urn-newsml-dpa-com-20090101-150611-99-05022 (Stand: 12.2.2016).

94 Vgl. *Lampe/Hegmann*, in: MüKo (Fn. 24), § 93 Rn. 26; *Rudolphi/Pasedach/Wolter*, in: SK StGB (Fn. 27), § 93 Rn. 31.

95 *Lampe/Hegmann*, in: MüKo (Fn. 24), § 93 Rn. 26.

96 *Paeffgen*, in: NK (Fn. 24), § 93 Rn. 27; *Sternberg-Lieben*, in: *Schönke/Schröder* (Fn. 65), § 93 Rn. 17.

97 Siehe dazu SA-Bericht zur Strafrechtsreform BT-Drucks. V/2860, S. 17 f.

gänglich. Im Sinne einer verfassungskonformen Auslegung ist diejenige Interpretation vorzuziehen, die den Wertemaßstäben der Verfassung am besten entspricht.[98] Konkret bedeutet dies, dass auf Tatbestandsebene[99] bereits kollidierende Verfassungspositionen im Wege praktischer Konkordanz berücksichtigt werden müssen.

Im hier interessierenden Fall ist insbesondere ein Konflikt der Pressefreiheit mit dem Schutzgut der äußeren Sicherheit vertretbar aufzulösen. Auch das verfassungsrechtlich verbürgte Informationsinteresse der Öffentlichkeit ist in diese Abwägung einzustellen. Auf diese Weise gilt es zu verhindern, dass der Staatsgeheimnisbegriff so weit verstanden wird, dass es allein in den Händen der Exekutiven läge, ob und inwieweit sie sich der demokratischen Öffentlichkeit und ihrer Willensbildung aussetzt. Mit dem 8. Strafrechtsänderungsgesetz von 1968[100] hat der Gesetzgeber die Auflösung des erwähnten Konflikts weitgehend in § 93 Abs. 2 StGB verortet. Danach sollen Verstöße gegen die freiheitlich demokratische Grundordnung nicht unter dem Schutzmantel des Staatsgeheimnisses begangen werden können. Der Gesetzgeber entscheidet insoweit die verfassungsrechtlich gebotene Abwägung zugunsten der Pressefreiheit und des berechtigten Interesses der Öffentlichkeit, von verborgenen Rechtsbrüchen zu erfahren.[101] Außerhalb der Regelung von § 93 Abs. 2 StGB bleibt demgemäß wenig Raum mehr für eine Abwägung.[102] Bei bestehender Gefahr *schwerer* Nachteile für die äußere Sicherheit sind mit Blick auf die Bedeutung des Schutzguts kaum Fallkonstellationen denkbar, in denen das Informationsinteresse der Öffentlichkeit und die Pressefreiheit den Staats-(geheimnis-)schutz verdrängen könnten. Ein Recht auf Bekanntgabe eines Staatsgeheimnisses um jeden Preis gibt es nicht.[103] Das gilt auch für den vorliegenden Sachverhalt. Die Veröffentlichung des „EFI-Konzepts" auf „netzpolitik.org" verfolgte insbesondere den Zweck, Rechtsverstöße des BfV offenzulegen:

> *Bsp.: „Staatstrojaner? Verfassungswidrig. Die ‚Einsatzdurchführung von Operativmaßnahmen (...)' klingt für uns sehr nach der ‚Online-Durchsuchung' (...), also einem Staatstrojaner. Dafür gibt es aber seit dem Urteil des Bundesverfassungsgerichts 2008 keine Rechtsgrundlage für den Verfassungsschutz."*

Dieses investigative Anliegen ist im Rahmen von § 93 Abs. 2 StGB zu berücksichtigen. Darüber hinaus ist jedoch kein Grund erkennbar, warum zugunsten von individuellen Rechtspositionen eine Gefahr schwerer Nachteile für die äußere Sicherheit in Kauf genommen werden sollte. Die *Pätsch*-Entscheidung des BGH hat viel-

98 BVerfGE 8, 210 (221).

99 Zur Tatbestandslösung siehe bereits *Arndt*, Anm. BGH NJW 1967, S. 873 (873); *Klug*, in: *Ruge* (Hrsg.), Landesverrat und Pressefreiheit, Berlin 1963, S. 12 f.

100 s.o. unter Fn. 17.

101 Vgl. Schmidt, in: LK (Fn. 24), § 93 Rn. 20; *Sternberg-Lieben*, in: *Schönke/Schröder* (Fn. 65), § 93 Rn. 25.

102 So übereinstimmend *Paeffgen*, in: NK (Fn. 24), § 93 Rn. 41; *Schmidt*, in: LK (Fn. 25), § 93 Rn. 33.

103 *Schmidt*, in: LK (Fn. 25), § 93 Rn. 33.

mehr klargestellt, dass die Anrufung der Öffentlichkeit jedenfalls nur äußerstes Mittel sein dürfe. Demzufolge sei ein größtmöglicher Schutz des Geheimnisses anzustreben und dafür Sorge zu tragen, dass der Kreis der Eingeweihten auf möglichst wenige und zuverlässige Personen beschränkt bleibe.[104] Vor diesem Hintergrund kann auch das mögliche Ansinnen, eine breit angelegte Diskussion über nachrichtendienstliche Überwachungsmaßnahmen in Gang zu setzen, in diesem Kontext nicht gewürdigt werden. Denn dafür hätte es insbesondere der Veröffentlichung des Personalplans der Referatsgruppe nicht bedurft.

V. Zwischenergebnis

Als Zwischenergebnis ist festzuhalten: Das „EFI-Konzept" des BfV war gem. § 93 Abs. 1 StGB geheimhaltungsfähig und geheimhaltungsbedürftig. Vorbehaltlich eines Tatbestandsausschlusses nach § 93 Abs. 2 StGB lag jedenfalls bis zum Zeitpunkt der Veröffentlichung ein Staatsgeheimnis vor.

VI. Kein illegales Staatsgeheimnis i.S.v. § 93 Abs. 2 StGB

Sog. illegale Staatsgeheimnisse i.S.v. § 93 Abs. 2 StGB sind – wie bereits bemerkt – vom Schutz der §§ 94 ff. StGB ausgenommen. Nur ausnahmsweise ist der Verrat illegaler Staatsgeheimnisse unter den engen Voraussetzungen des § 97a StGB strafbar. § 93 Abs. 2 StGB trägt dem öffentlichen Informationsbedürfnis Rechnung, illegale Vorgänge im staatlichen Bereich aufzudecken. Illegale Staatsgeheimnisse liegen nicht bei einfachen Rechtsverstößen vor;[105] vielmehr werden Verstöße gegen die freiheitlich demokratische Grundordnung oder gegen zwischenstaatlich vereinbarte Rüstungsbeschränkungen verlangt. Der BGH hat diese Anforderungen bereits vorgezeichnet:[106] Es gebe einen Kernbereich des Verfassungsrechts, bei dessen Verletzung jeder das Recht haben müsse, sofort und ohne Umwege die Öffentlichkeit anzurufen, auch wenn dies zwingend zur Preisgabe von Staatsgeheimnissen führe.[107] Zu diesem Kernbereich des Verfassungsrechts – den Prinzipien der freiheitlich demokratischen Grundordnung – zählt nach der Rechtsprechung des Bundesverfassungsgerichts insbesondere die Achtung vor den im GG konkretisierten Menschenrechten.[108] Die Blogger von „netzpolitik.org" rügen in ihrem Beitrag verschiedene Grundrechtsverletzungen, die infolge der Einrichtung der neuen „EFI-Referatsgruppe" beim BfV zu befürchten seien. Fraglich ist, ob sich das „EFI-Konzept" vor dem Hintergrund dieser Kritik in die Kategorie eines illegalen Staatsgeheimnisses i.S.v. § 93 Abs. 2 StGB einordnen lässt.

104 Vgl. BGHSt 20, 342 (364). Siehe hierzu auch *Woesner*, Neues Staatsschutzstrafrecht (Fn. 22), S. 2133.

105 Ausführlich hierzu *Barnert*, Das illegale Staatsgeheimnis, München 1978, S. 135 ff.

106 Näher dazu *Deiseroth*, Illegale Geheimnisse (Fn. 20), S. 5 ff.

107 BGHSt 20, 342 (365).

108 BVerfGE 2, 1, 13. Siehe dazu auch SA-Bericht zur Strafrechtsreform BT-Drucks. V/2860, S. 16 f.

1. „Online-Durchsuchung" ohne gesetzliche Grundlage

Wie oben bereits erwähnt wurde, wird eine verfassungswidrige Ausspähung von Daten mit Hilfe sog. „Staatstrojaner" gerügt. Tatsächlich wäre eine solche Überwachungsmaßnahme mit dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme so lange nicht zu vereinbaren, wie dafür im BVerfSchG keine Rechtsgrundlage geschaffen wird.[109] Durch seine Entscheidung zur Online-Durchsuchung hat das Bundesverfassungsgericht für die Ausgestaltung entsprechender Ermächtigungsvorschriften strenge Maßstäbe aufgestellt.[110] Bislang besteht allein für das bayerische LfV mit Art. 10 BayVSG eine landesrechtliche Befugnisnorm, die zudem einigen verfassungsrechtlichen Bedenken begegnet.[111] Würde das BfV insofern mit Hilfe einer bestimmten Software heimlich auf ein informationstechnisches System zugreifen, wäre dieser Grundrechtseingriff in Ermangelung einer Ermächtigungsgrundlage nicht zu rechtfertigen und mit der freiheitlich demokratischen Grundordnung nicht zu vereinbaren.

Die bloße Behauptung eines verfassungswidrigen Missstands genügt allerdings für die Annahme eines illegalen Staatsgeheimnisses i.S.v. § 93 Abs. 2 StGB nicht. Die gerügte Tatsache muss vielmehr objektiv mit einem Verstoß gegen die freiheitlich demokratische Grundordnung behaftet sein.[112] Hierfür gibt es jedenfalls mit Blick auf Stellungnahmen der Bundesregierung keine Anzeichen. Auf schriftliche Anfrage eines Bundestagsabgeordneten erklärte die Bundesregierung am 23.7.2014, dass in den vergangenen Jahren keine „Trojaner" durch das BfV eingesetzt worden seien.[113] In Bezug auf die „EFI-Referatsgruppe" ließ die Bundesregierung am 4.3.2015 ausdrücklich wissen, deren Arbeit basiere ausschließlich auf Daten, die auf geltender Rechtsgrundlage erhoben würden.[114] Insoweit jedenfalls kann das „EFI-Konzept" nicht als illegales Staatsgeheimnis i.S.v. § 93 Abs. 2 StGB gelten.

2. Verfassungswidrige „Massendatenauswertung"

Weitere Kritik der Netzaktivisten bezieht sich auf die „Massendatenauswertung von Internetinhalten". Besonderes Augenmerk gilt der Erstellung von „Bewegungsprofilen und Beziehungsnetzwerken":

> *Bsp.: „Der Verfassungsschutz wird nicht müde zu betonen, dass er nur konkrete Einzelpersonen überwache. Wir hatten jedoch berichtet, dass das Amt 2,75 Millionen Euro investiert, um massenhaft Internet-Inhalte zu erheben und auszuwerten. (...) Bei der Analyse*

109 Siehe dazu den Bericht des PKGr, BT-Drucks. 16/13968 S. 9.

110 Vgl. BVerfGE 120, 274 ff. Dazu siehe *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, Berlin 2014, S. 99, dort Fußnote 333; 221 ff.

111 Zutreffend *Löffelmann*, in: *Dietrich/Eiffler* (Fn. 38), 6. Teil, § 6 Rn. 34; kritisch auch *Gudermann*, Die Online-Durchsuchung im Lichte des Verfassungsrechts, Hamburg 2010, S. 240.

112 Vgl. *Schmidt*, in: LK (Fn. 25), § 93 Rn. 22.

113 Abrufbar unter: https://netzpolitik.org/2014/bundesregierung-information-wie-oft-der-bnd-trojaner-einsetzt-gefaehrdet-die-sicherheit-der-bundesrepublik/ (Stand: 12.2.2016).

114 Siehe Plenarprotokoll 18/90 vom 4.3.2015, 8555.

der überwachten Internet-Daten nutzt der Geheimdienst genau die Möglichkeiten, über die wir regelmäßig berichten. Zwei neue Referate (...) rastern verschiedene zusammengeführte Daten und erstellen aus Metadaten Bewegungsprofile und Beziehungsnetzwerke (...).“

Der Vorwurf ungerechtfertigter Grundrechtseingriffe wird dabei nicht direkt geäußert. Jedoch werden rechtliche Bewertungen aus dem parlamentarisch-politischen Raum so einbezogen, dass sie der Gesamtaussage des Artikels zugerechnet werden können. Danach bahne das BfV die Überwachung unzähliger Bürger/innen an. Hierin liege ein tiefer und mit den Grundrechten nicht zu vereinbarender Eingriff des Geheimdienstes in die Privatsphäre und die Persönlichkeitsrechte zehntausender Bürger/innen (*Goltz*). An anderer Stelle wird geäußert, eine so weitreichende nachträgliche Auswertung überwachter Telekommunikation, wie das BfV offenbar praktiziere, könne schwerlich durch vorherige Genehmigungen der G10-Kommission gedeckt sein. Zudem seien künftige Massen-Überwachungen solcher Art direkt an Datenservern gesetzlich nicht genehmigungsfähig (*Ströbele*). Dieser z.T. etwas diffusen Kritik sind im Wesentlichen zwei verfassungserhebliche Vorwürfe zu entnehmen: Zum einen wird gerügt, das BfV betreibe ohne gesetzliche Grundlage eine strategische Überwachung des Internets. Zum anderen wird die nachträgliche Auswertungspraxis – das Verknüpfen verschiedener Daten – als ungerechtfertigter Grundrechtseingriff angesehen.

Eine strategische Massendatenerhebung wäre dem BfV tatsächlich versagt. § 3 G10 ermächtigt die Behörde allein zu heimlichen Individualkontrollen. Lediglich der BND ist auf der Grundlage von § 5 G10 zu strategischen Überwachungsmaßnahmen befugt.[115] Die Bundesregierung begegnet der Kritik mit folgender Stellungnahme:

„Das BfV führt Telekommunikationsüberwachungsmaßnahmen ausschließlich bezogen auf Einzelpersonen (...) durch. (...) Dementsprechend führt das Bundesamt für Verfassungsschutz gerade keine massenhaften, anlasslosen, verdachtsunabhängigen oder sonst ungezielten Maßnahmen gegen eine Vielzahl oder beliebige Grundrechtsträger durch.“[116]

Auch sonst finden sich keine Anhaltspunkte für eine bereits praktizierte grundrechtswidrige Massenüberwachung.[117] Für eine verfassungskonforme Praxis sprechen in diesem Zusammenhang statistische Angaben, die das Parlamentarische Kontrollgremium in seinen jährlichen Berichten über Überwachungsmaßnahmen

115 Zur Differenzierung von strategischer Fernmeldeaufklärung und Individualkontrolle siehe *Hochreiter*, Die heimliche Überwachung internationaler Telekommunikation, München 2002, S. 18 ff.; *Gazeas*, Übermittlung (Fn. 110), S. 173 ff.; *Löffelmann*, in: *Dietrich/Eiffler* (Fn. 38), 6. Teil, § 5 Rn. 117 ff.

116 Plenarprotokoll 18/90 vom 4.3.2015, 8555.

117 Siehe dazu auch *Rath*, Datendeal mit der NSA, taz vom 28.8.2015, abrufbar unter: http://www.taz.de/!5227943/ (Stand: 12.2.2016); *Biermann*, Diese Spähsoftware findet jedes Passwort, ZEIT-Online vom 27.8.2015, abrufbar unter: http://www.zeit.de/digital/datenschutz/2015-08/bfv-verfassungsschutz-was-kann-xkeyscore (Stand: 12.2.2016).

nach dem G10 dem Bundestag vorgelegt hat. Beispielsweise genehmigte die G10-Kommission dem BfV im Jahr 2013 insgesamt lediglich 159 Überwachungsmaßnahmen auf der Grundlage von § 3 G10, die sich gegen weniger als 700 Betroffene richteten.[118]

Weitaus schwieriger ist dagegen der Vorwurf rechtswidriger „weitreichender nachträglicher Auswertung überwachter Telekommunikation". Hierzu ist zunächst ein Blick auf die nachrichtendienstliche Praxis zu werfen: Ausweislich des „EFI-Konzepts" soll eine Vielzahl von Daten aus unterschiedlichsten Herkunftsbereichen zusammengeführt und ausgewertet werden. Dies betrifft zunächst Inhaltsdaten, die das BfV aus Individualüberwachungsmaßnahmen auf der Grundlage von § 3 G10 erlangt hat (z.B. SMS, E-Mailkommunikation, Chatprotokolle), aber auch Verkehrsdaten (z. B. Nummern und Kennungen der beteiligten Anschlüsse oder übertragene Datenmengen), die der Behörde von den Telekommunikationsdienstleistern gem. § 8a Abs. 2 S. 1 Nr. 4 BVerfSchG infolge eines Auskunftsersuchens übermittelt worden sind. Nach Maßgabe des „EFI-Konzepts" soll es dabei nicht bleiben:

> *„Die Analyse großer Datenmengen erstreckt sich über den Bereich der TKÜ hinausgehend auf alle dem BfV aus unterschiedlichsten Quellen zugänglichen Daten (u.a. Asservate infolge von vereinsrechtlichen Verbotsverfahren).*"

Insbesondere ist in diesem Zusammenhang von einer Einbeziehung öffentlich zugänglicher Informationen aus dem Internet[119] auszugehen. Auch an personenbezogene Daten anderer Behörden (z.B. der Polizei), die dem BfV gem. § 18 BVerfSchG i.V.m. einer bereichsspezifischen Ermächtigung[120] übermittelt werden können, ist zu denken.

Ein solches Aufarbeiten von Informationen ist nachrichtendienstliches Kerngeschäft, denn zu den gesetzlichen Aufgaben des BfV zählt nicht nur die Erhebung von Daten, sondern insbesondere auch deren Auswertung (§ 3 Abs. 1 BVerfSchG). Als „Auswertung" wird das Vergleichen, Zuordnen, Kombinieren und Verknüpfen von Informationen mit dem Ziel angesehen, ein möglichst umfassendes Bild über den jeweils interessierenden Sachverhalt zu bekommen.[121] Viele Informationen müssen insbesondere erst auf ihren Wahrheitsgehalt überprüft werden. Dies gilt v.a. für Informationen von menschlichen Quellen. Die wertende und vergleichende Betrachtung mit Informationen anderer Herkunft ermöglicht es beispielsweise, die Zuverlässigkeit von V-Personen i.S.v. § 9b BVerfSchG zu beurteilen. Grundsätzlich

118 Vgl. BT-Drucks. 18/3709 S. 5.

119 Siehe hierzu *Roth*, in: *Schenke/Graulich/Ruthig*, Sicherheitsrecht des Bundes, München 2014, BVerfSchG, § 8 Rn. 10 f.; 54; *Wolf*, Big Data (Fn. 62), S. 43 ff.

120 Es bedarf einer doppelten gesetzlichen Ermächtigung, vgl. BVerfGE 130, 151 (184).

121 Vgl. *Droste*, Verfassungsschutzrecht (Fn. 50), S. 89 f.; *Gazeas*, Übermittlung (Fn. 110), S. 75 f.; *Roth*, in: *Schenke/Graulich/Ruthig* (Fn. 119), BVerfSchG, §§ 3, 4 Rn. 91.

gilt: Je vielfältiger die Quellen sind, umso belastbarere Aussagen lassen sich in Bezug auf bestimmte Beobachtungsgegenstände treffen (sog. All-Source Intelligence).[122] Bei der Auswertung kommen unterschiedlichste Methoden zum Einsatz, wie beispielsweise Simulations- oder Szenariotechniken.[123] Auch systematische Auswertungsverfahren, die der „Rasterfahndung" der Strafverfolgungsbehörden ähneln, werden – etwa im Zusammenhang der Extremismusbeobachtung oder der Spionageabwehr – verwendet.[124] Das von den Bloggern kritisierte Anlegen von Bewegungsprofilen und Beziehungsnetzwerken erfolgt insoweit im Rahmen des gesetzlichen Auswertungs*auftrags*.

Fraglich ist indes, ob hierfür im Recht der Nachrichtendienste auch eine *Befugnis* eingeräumt wird. Es verbietet sich spätestens seit der Volkszählungsentscheidung des Bundesverfassungsgerichts,[125] von der gesetzlichen Festlegung von Verwaltungsaufgaben auf Ermächtigungen zu Eingriffen in das Grundrecht auf informationelle Selbstbestimmung zu schließen. Vielmehr sind hinreichend bestimmte Befugnisse zu regeln. Für die Auswertung von personenbezogenen Daten bestehen mit den §§ 8 Abs. 1 S. 1, 10 ff. BVerfSchG Rechtsgrundlagen. Danach darf das BfV unter näher bezeichneten Voraussetzungen personenbezogene Daten verarbeiten (z. B. speichern oder löschen) und nutzen. Auch das Anlegen von automatisierten Verbund- und Amtsdateien ist gem. §§ 6, 10 und 14 BVerfSchG zulässig. Zusammen genommen bedeutet dies, dass bei der Auswertung grundsätzlich Daten in verschiedenen Dateien recherchiert und miteinander verknüpft werden dürfen, sofern bei einem Sachverhalt tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen vorliegen und dies zur „Erforschung und Bewertung" derselben erforderlich ist. Das Erfordernis der Erforderlichkeit mahnt dazu, den Auswertungsvorgang auf so wenige Daten wie möglich zu beschränken.[126] Kann beispielsweise eine Erkenntnis bereits aus für jedermann zugänglichen Quellen zuverlässig gewonnen werden, verbietet sich die Einbeziehung heimlich – mit nachrichtendienstlichen Mitteln – erhobener Informationen.[127]

122 Siehe *Lowenthal*, Intelligence (Fn. 49), S. 91 f.; *Omand*, Securing the State, New York 2010, S. 149 ff.

123 Zu Methoden der „Intelligence Analysis" siehe z.B. die Beiträge in *Lahnemann/Arcos* (eds.), The Art of Intelligence, Lanham 2014 sowie *Beebe/Pherson*, Cases in Intelligence Analysis, Los Angeles 2012; *Omand*, Securing the State (Fn. 122), p. 139.

124 Vgl. *Droste*, Verfassungsschutzrecht (Fn. 50), S. 90, 442. Siehe dazu auch *Gusy*, Geheimdienstliche Aufklärung und Verfassungsschutz, in: *Koch* (Hrsg.), Terrorismus – Rechtsfragen der äußeren und inneren Sicherheit, Baden-Baden 2002, S. 93 (98 ff.).

125 BVerfGE 65, 1 ff.

126 Skeptisch *Bergemann*, Die Freiheit im Kopf – neue Befugnisse für die Nachrichtendienste, NVwZ 2015, S. 1705 (1705 f.).

127 In diesem Sinne BVerwGE 110, 126 (138).

Weitere Eingrenzungen für die Auswertung sieht das Gesetz nicht vor.[128] Das Bundesverfassungsgericht hat jedoch darauf hingewiesen, dass Daten durch ihre systematische Verknüpfung einen zusätzlichen Aussagewert erhalten können, aus dem sich eine für das Grundrecht auf informationelle Selbstbestimmung spezifische Gefährdungslage für die Freiheitsrechte oder die Privatheit des Betroffenen ergibt.[129] Dabei ist insbesondere eine automatische Auswertung unter Verwendung spezieller Datenverarbeitungssoftware (Data Mining) verfassungsrechtlich nur unter engen Voraussetzungen möglich.[130] Unzulässig ist nach der Rechtsprechung des Bundesverfassungsgerichts jedenfalls, dass Daten derart miteinander verknüpft werden, dass sie sich zu einem „teilweise oder weitgehend vollständigen Persönlichkeitsprofil" zusammenfügen lassen.[131] Das käme einer „Rundumüberwachung" gleich, die in den absoluten Kernbereich privater Lebensgestaltung eingreifen und die Menschenwürde verletzen würde.[132]

Wenngleich Bedenken bereits hinsichtlich der tatsächlichen Möglichkeit bestehen, „den" Menschen in seiner „ganzen" Persönlichkeit zu registrieren,[133] erscheint im vorliegenden Fall jedenfalls zweifelhaft, ob sich aus „Beziehungsnetzwerken" und „Bewegungsprofilen" ein „umfassendes Persönlichkeitsprofil" i.S.d. Verfassungsgerichtsrechtsprechung konturieren lässt. In seiner GPS-Entscheidung hat das Bundesverfassungsgericht in der Anordnung von insgesamt 13 parallelen Überwachungsmaßnahmen von großer Intensität keine unzulässige „Rundumüberwachung" erkennen können.

Im Einzelnen wurden angeordnet:[134]

- Videoüberwachung des Eingangsbereichs des vom Beschwerdeführer genutzten Wohnhauses seiner Mutter einschließlich eines am Grundstück vorbeiführenden Verbindungswegs
- Visuelle Langzeitobservation durch das Landeskriminalamt
- Videogestützte Langzeitbeobachtung durch den Verfassungsschutz des Landes Nordrhein-Westfalen
- Observierung des Wohnhauses des Mitangeklagten durch den Verfassungsschutz der Freien und Hansestadt Hamburg

128 Kritisch gesehen von *Bergemann*, in: *Lisken/Denninger* (Hrsg.), HdbPolR, 5. Auflage, München 2012, Teil H, Rn. 44, 98 f.; *Löffelmann*, in: *Dietrich/Eiffler* (Fn. 38), 6. Teil, § 6 Rn. 62 f.

129 BVerfGE 120, 35 (361 f.); BVerwG NVwZ 2011, S. 161 (163).

130 Vgl. *Löffelmann*, in: *Dietrich/Eiffler* (Fn. 38), 6. Teil, § 6 Rn. 55; *Bergemann*, Freiheit im Kopf (Fn. 126), S. 1705 f.

131 BVerfGE 65, 1 (42); 115, 320 (350).

132 Vgl. BVerfGE 109, 279 (323); BVerfGE 112, 304 (319).

133 Vgl. *Hornung*, Die kumulative Wirkung von Überwachungsmaßnahmen, in: *Albers/Weinzierl* (Hrsg.), Menschenrechtliche Standards in der Sicherheitspolitik, Baden-Baden 2010, S. 65 (72 f.); *Schwabenbauer*, Heimliche Grundrechtseingriffe, Tübingen 2013, S. 295 m.w.N.

134 Vgl. BVerfGE 112, 304 (306 f.).

- Versehen des Pkw des Mitangeklagten, den der Beschwerdeführer ebenfalls verwendete, mit einem Peilsender durch das Bundeskriminalamt
- Später: Ersatz des Peilsenders durch eine GPS-gestützte Observation
- Abhören des Betriebsfunks des Mitangeklagten
- Überwachung des vom Beschwerdeführer mitgenutzten Telefonanschlusses seiner Mutter
- Überwachung der nahe gelegenen Telefonzelle
- Überwachung des Telefonanschlusses des Mitangeklagten
- Öffnung und Prüfung der Postsendungen des Beschwerdeführers
- Ausschreibung des Beschwerdeführers, des Mitangeklagten und der von ihnen genutzten Fahrzeuge zur polizeilichen Beobachtung
- Abhören und Aufzeichnen des in den Pkw des Mitangeklagten und der Mutter nicht öffentlich gesprochenen Wortes

Im Vergleich hierzu ist nicht zu erkennen, dass die Auswertungspraxis der „EFI-Referatsgruppe" intimere und umfassendere Einblicke ermöglichen würde. Bereits die Datenerhebung, die der Auswertung vorangeht, ist Beschränkungen unterworfen. Nach § 8a Abs. 2 S. 1 BVerfSchG ist beispielsweise die Einholung von Auskünften bei Luftfahrtunternehmen oder Telekommunikationsdiensten nur zulässig, soweit dies zur Sammlung und Auswertung von Informationen erforderlich ist. Zudem müssen Tatsachen die Annahme rechtfertigen, dass schwerwiegende Gefahren für die in § 3 Abs. 1 BVerfSchG genannten Schutzgüter vorliegen. § 8b BVerfSchG trifft verfahrensrechtliche Schutzvorkehrungen, wie etwa die Einschaltung der G10-Kommission. Dem Anlegen von umfassenden Persönlichkeitsprofilen soll auf diese Weise bereits bei der Datenerhebung vorgebeugt werden.[135] Der Auswertung der erhobenen Daten werden über §§ 8 Abs. 1 S. 1, 10 ff. BVerfSchG nochmals einzelfallorientierte Grenzen gezogen. Die Daten dürfen – bei gebotener restriktiver Auslegung[136] – nicht einfach wahllos und anlasslos miteinander kombiniert werden. Die Zweckbindung sowie die Eingrenzung der Datenarten und des betroffenen Personenkreises in der gem. § 14 BVerfSchG notwendigen Dateianordnung schließen eine großflächige Speicherung in einer Datei aus. Mit Blick auf die fortschreitende Digitalisierung des Alltags mag darüber diskutiert werden können, ob es zukünftig weiterer gesetzlicher Sicherungen bedarf.[137] Das Bundesverfassungsgericht hat bisher jedenfalls keinen Anlass gesehen, spezifische gesetzliche Regelungen zur Vermeidung einer Persönlichkeitsprofilbildung einzufordern.[138]

135 Vgl. *Mallmann*, in: *Schenke/Graulich/Ruthig* (Fn. 119), BVerfSchG, §§ 8a Rn. 2.

136 In diesem Sinne – bezogen auf die Novelle des BVerfSchG – auch *Bergemann*, Freiheit im Kopf (Fn. 126), S. 1705.

137 Siehe dazu *Bergemann*, in: *Lisken/Denninger* (Fn. 128), Teil H, Rn. 98 ff.

138 Vgl. BVerfGE 112, 304 (319 f.).

Festzuhalten ist nach alledem, dass das BfV de lege lata nicht ermächtigt ist, umfassende Persönlichkeitsprofile zu erstellen. Unterhalb dieser Schwelle bestehen jedoch für die verknüpfende Auswertung von Daten Rechtsgrundlagen in §§ 8 Abs. 1 S. 1, 10 ff. BVerfSchG. Aus dem „EFI-Konzept" kann eine Verletzung dieser gesetzlichen Vorgaben nicht abgeleitet werden. Grundrechtsverstöße lassen sich demzufolge nicht erkennen. In Ermangelung eines Verstoßes gegen die freiheitlich demokratische Grundordnung liegt deshalb auch kein illegales Staatsgeheimnis i.S.v. § 93 Abs. 2 StGB vor.

VII. Ergebnis

Die Rekonstruktion legt – trotz ihrer Beschränkung auf offen verfügbare Quellen – nahe, dass zumindest in einem Fall ein Staatsgeheimnis i.S.v. § 93 StGB unter „Netzpolitik.org" veröffentlicht wurde. Die Ermittlungsbehörde konnte jedenfalls insoweit von einem Anfangsverdacht ausgehen und Ermittlungen nach §§ 94 ff. StGB einleiten.[139]

D. Staatsgeheimnisqualität als Identifizierungsproblem

Zur Einleitung eines Ermittlungsverfahrens ist die Staatsanwaltschaft bekanntlich gem. § 152 Abs. 2 StPO verpflichtet, sofern zureichende tatsächliche Anhaltspunkte vorliegen. Diese Schwelle ist vergleichsweise schnell überwunden. Trotz Anfangsverdachts gelangt die weit überwiegende Zahl der Ermittlungsverfahren niemals zu Anklage oder Strafbefehlsantrag. Über 70% der Verfahren werden – ggf. unter Auflage – eingestellt.[140] Es spricht demgemäß einiges dafür, auch bei Ermittlungen wegen des Verdachts einer Straftat nach §§ 94 ff. StGB den Strafverfolgungsbehörden Vertrauen in die Erfüllung ihres gesetzlichen Auftrags entgegenzubringen.

Es kann allerdings nicht von der Hand gewiesen werden, dass sich der Fall jedenfalls dann verkompliziert, sofern sich der Verdacht gegen Vertreter/-innen der Presse richtet. Zwar gibt es keine pressespezifische Immunität, von Strafverfolgung verschont zu bleiben. Gleichwohl kann grundsätzlich nicht ausgeschlossen werden, dass die Einleitung eines Ermittlungsverfahrens die Akkusationsfunktion des investigativen Journalismus nachteilig betrifft. Die Arbeitsfelder investigativer Journalisten/-innen zeichnen sich in der Regel durch eine hohe gesellschaftliche und politische Relevanz aus.[141] Das Enthüllungsinteresse gilt etwa Misswirtschaft, Korrupti-

139 Siehe zur Einleitung des Ermittlungsverfahrens im vorliegenden Fall näher *Trentmann*, Der Fall netzpolitil.org – Lehrstück für den Rechtsstaat, JR 2015, S. 571 (571).

140 Vgl. Statistisches Bundesamt, abrufbar unter: https://www.destatis.de/DE/Publikationen/Thematisch/Rechtspflege/GerichtePersonal/Staatsanwaltschaften2100260147004.pdf?__blob=publicationFile (Stand: 12.2.2016).

141 Zum Begriff des investigativen Journalismus siehe *Eichhoff*, Investigativer Journalismus aus verfassungsrechtlicher Sicht, Tübingen 2010, S. 11 ff.

on oder Amtsmissbrauch. Recherche und Veröffentlichung überwinden üblicherweise Widerstände und Barrieren: Zur Aufdeckung verborgener Sachverhalte werden Quellen nutzbar gemacht, die nicht allgemein zugänglich sind.[142] Es entspricht gerade dem Wesen des Investigativjournalismus, interne, u.U. sogar geheime Dokumente aufzuspüren und sie zu verwenden. Stünde zu befürchten, dass aus diesem Grunde regelmäßig ein strafrechtliches Ermittlungsverfahren – mit allen Begleiterscheinungen (wie z.B. Offenlegung von Informanten) – eingeleitet werden würde, ist nicht auszuschließen, dass dies auf Dauer einschränkenden Einfluss auf die journalistische Arbeit haben könnte. Der Verhinderung solcher Einschüchterungseffekte hat der Gesetzgeber – als Konsequenz der Cicero-Entscheidung des BVerfG[143] – durch die Einführung des § 353b Abs. 3a StGB Rechnung getragen, wonach die journalistische Beihilfe zur Verletzung eines Dienstgeheimnisses straflos gestellt wurde.[144]

Für den Fall eines Staatsgeheimnisses i.S.d. § 93 StGB ist eine derartige täterschaftliche Einschränkung aus gutem Grunde nicht vorgesehen. Während das geschützte Rechtsgut bei § 353b StGB das Vertrauen der Allgemeinheit in die Verschwiegenheit amtlicher Stellen ist, zielen die §§ 94 ff. StGB auf die Sicherheit der Bundesrepublik Deutschland vor Beeinträchtigungen von außen. Mit Blick auf das Schädigungspotential einer Gefährdung der äußeren Sicherheit dürfte unstreitig sein, dass für eine pauschale Strafffreistellung für Journalisten/-innen im Falle von §§ 94 ff. StGB kein Raum bleibt.[145] Demgemäß sind investigative Recherchen und Veröffentlichungen, die Staatsgeheimnisse zum Gegenstand haben, im Wesentlichen auf den Schutz von § 93 Abs. 2 StGB angewiesen. In Bezug auf das Vorliegen eines illegalen Staatsgeheimnisses dürfte aber – wie der vorliegende Fall illustriert – nicht selten ein Identifizierungsproblem vorliegen. Dem Laien ist die mitunter komplizierte Beurteilung von Verstößen gegen die freiheitlich demokratische Grundordnung kaum möglich. Juristischer Sachverstand wird oft – etwa bei kleineren Zeitungen, Bloggern/-innen oder „freien Autoren/-innen" – nicht zur Verfügung stehen. Praktisch hat dies zur Folge, dass die Journalistin oder der Journalist die rechtliche Einschätzung aus der Laiensphäre heraus selbst vornehmen muss und sich dadurch in höherem Maße dem Risiko strafrechtlicher Ermittlungen aussetzt. Eine fehlerhafte rechtliche Bewertung schützt in der Regel bekanntlich nicht vor Strafe. Auch die irrige Annahme eines illegalen Staatsgeheimnisses ist unter den Voraussetzungen des § 97b StGB strafbar.

142 Ausführlich dazu *Eichhoff*, Investigativer Journalismus (Fn. 141), S. 17 ff.

143 BVerfGE 117, 244 ff.

144 Siehe näher dazu BT-Drucks. 17/3355.

145 Zu diesem Ergebnis kommt auch (aus journalistischer Sicht) *Huff*, lto vom 10.8.2015, abrufbar unter: http://www.lto.de/recht/hintergruende/h/verrat-staatsgeheimnis-keine-ausnahme-fuer-journalisten/ (Stand: 12.2.2016).

Einer normativen Lösung erscheint das Problem kaum zugänglich. Weitergehende Privilegierungen und pauschale Schutzklauseln für Journalisten/-innen scheiden insbesondere mit Blick auf das hohe Schutzgut der §§ 94 ff. StGB aus. Für eine zumindest geringe Verbesserung könnte sorgen, den Gedanken der freiwilligen Selbstkontrolle der Presse nutzbar zu machen, dem sich der Deutsche Presserat seit seiner Gründung 1957 verpflichtet hat. Gegenwärtig fungiert der Presserat v.a. als Beschwerdeinstanz für Verstöße gegen den sog. Pressekodex.[146] Ergänzend dazu haben viele Medienhäuser inzwischen Leseranwälte/-innen, Medienräte, Leserobleute oder Ombudspersonen eingerichtet, die sich in unabhängiger Kritik üben und/oder zwischen Redaktionen und Rezipienten/-innen vermitteln sollen.[147] Medienkritik in diesem Sinne darf insofern als berufsethisches Korrektiv der Presse verstanden werden. Der Präambel des Pressekodexes folgend umfasst die Berufsethik der Presse u.a. die Pflicht, „im Rahmen der Verfassung und der verfassungskonformen Gesetze das Ansehen der Presse zu wahren". Rechtsverstöße (z.B. Urheberrechtsverletzungen) sind demgemäß berufsethisch nicht vertretbar und können einen Beschwerdegrund darstellen. Zu Beschwerden würde im Fall von Rechtsverstößen seltener Anlass bestehen, wenn die freiwillige Selbstkontrolle bereits präventiv einsetzte. Für Journalisten/-innen, die nicht auf ein hauseigenes Justiziariat zurückgreifen können, könnte unabhängige juristische Fachkompetenz – etwa in Gestalt einer Fachreferentin oder eines Fachreferenten bei der Geschäftsstelle des Presserates – eingerichtet werden. Dadurch blieben Journalisten/-innen bei schwierigen Rechtsfragen wie der Beurteilung der Illegalität eines Staatsgeheimnisses nicht auf sich allein gestellt.

E. Schluss

Die vorstehenden Ausführungen haben vor Augen geführt, dass Exklusion und Vertraulichkeit im Ausnahmefall berechtigt sein können. In Bezug auf die unter „Netzpolitik.org" veröffentlichten Dokumente war zumindest in einem Fall aus guten Gründen ein Staatsgeheimnis i.S.v. § 93 StGB anzunehmen. Die Prüfung hat allerdings auch die Schwierigkeiten für Journalisten/-innen offengelegt, ein Staatsgeheimnis bzw. dessen Illegalität zu identifizieren. Eine eingehende fachliche Begutachtung unter Einbeziehung praktischer Erfahrungswerte ist regelmäßig unersetzlich. Wer sich trotzdem zu pauschalen, politischer Mode folgenden Bewertungen hinreißen lässt, läuft Gefahr, Glaubwürdigkeit einzubüßen.

146 Vgl. dazu Deutscher Presserat (Hrsg.), Jahrbuch 2012, Konstanz 2012, S. 177 ff.

147 Zu den Hintergründen siehe *Fengler*, Medienjournalismus in den USA, Konstanz 2002, S. 161 ff.