Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

Bundesministerium der Justiz und für Verbraucherschutz
Referate II A 2 und II B 7
Mohrenstraße 37
11017 Berlin

per E-Mail an:

poststelle@bmjv.bund.de

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
FON
FAX (0228) 997799-5550
E-MAIL referat32@bfdi.bund.de
BEARBEITET
INTERNET www.datenschutz.bund.de
DATUM Bonn, 16.01.2020
GESCHÄFTSZ. 32-642/041#1435

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

BETREFF **Referentenentwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität**
HIER Stellungnahme

Zu dem oben genannten Gesetzentwurf wurde ich nicht in die Ressortabstimmung eingebunden, obwohl mir – wie auch schon mehrfach in anderen Gesetzgebungsverfahren – zugesagt wurde, mich entsprechend der gemeinsamen Geschäftsordnung der Bundesministerien zu beteiligen. Zu dem Entwurf nehme ich nach einer ersten Durchsicht wie folgt Stellung.

I. Allgemein

Der Entwurf enthält gravierende Eingriffe in Grundrechte. Es ist teilweise zweifelhaft, ob diese mit dem Grundgesetz vereinbar sind (insb. Zugriff auf Daten, die den Zugang zu Online-Diensten ermöglichen wie z.B. Passwörter). Auch im Übrigen bestehen erhebliche Zweifel, ob die mit dem vorliegenden Entwurf verfolgten Ziele erreicht werden. Bereits die Grundkonzeptionen der Meldepflicht und der Rolle des BKA werfen erhebliche Fragen auf. Insgesamt ist fraglich, ob überhaupt ein schlüssiges Konzept vorliegt, um dem Phänomen der rechtsextremistischen Hasskriminalität effektiv zu begegnen. Ich rege an, zunächst empirisch zu untersuchen, wie die zuständigen Einrichtungen und Behörden in Bund und Ländern aufgestellt sind, denn neue gesetzliche Vorschriften helfen nicht bei bestehenden Vollzugsdefiziten

In der jüngeren Vergangenheit sind mir viele zahlreiche Gesetzentwürfe vorgelegt worden, die in kurzen Abständen immer wieder die Strafprozessordnung betrafen. Zu nennen sind etwa die Entwürfe für ein „Gesetz zur Modernisierung des Strafverfahrens“, für ein „Gesetz

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679“ oder für ein „Gesetz zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze“. Immer wieder betreffen die Entwürfe datenschutzrechtliche Fragestellungen. Gerade aus dieser Sicht stellt sich die Frage, welchem durchgängigen Konzept diese Gesetzgebungstätigkeit folgt. Dies habe ich zuletzt in meiner Stellungnahme vom 11.10.2019 zum Entwurf eines Gesetzes zur Bekämpfung der Unternehmenskriminalität ausgeführt.

II. Meldesystem

Mit der Einrichtung einer föderalen Struktur in Deutschland wurde ein Schlussstrich unter die vormalige „Sicherheits“-architektur gezogen und die ausführende Verantwortung für die innere Sicherheit den Ländern zugewiesen. Auf der Ebene des Bundes sollte es nach dem Willen des Grundgesetzes keine starke Bundespolizeibehörde mehr geben. Die Polizeigewalt sollte in den Ländern liegen. Parallel wurden im Bereich von Rundfunk und Presse Aufsichtsstrukturen geschaffen, die möglichst nur Eingriffe durch unabhängige Gremien regeln sollten, nicht jedoch durch Vollzugsbehörden im klassischen Sinne. Deshalb entstanden Rundfunkräte und Institutionen der freiwilligen Selbstkontrolle, z.B. der Presserat, später in dieser Tradition die Medienanstalten der Länder.

Über diese könnte heute ebenfalls ein „Meldewesen“ für problematische Inhalte organisiert werden – sofern dies überhaupt erforderlich und nicht bereits vorhanden ist. Dass derartige Alternativen nicht umfassend untersucht und gegebenenfalls evaluiert worden sind, ist bereits strukturell zu kritisieren. Schon aus diesem Grunde lehne ich die neu gefassten Datenübermittlungen ab.

Geplant ist, dass Anbieter von Telemediendiensten – insbesondere sozialen Netzwerken – eine Meldepflicht an das BKA auferlegt wird. Nach Beschwerden müssen diese zunächst intern prüfen, ob die von Nutzern hochgeladenen und über die Mediendienste verbreiteten Inhalte gegen bestimmte im Gesetz genannte Vorschriften verstoßen.

Damit wird der Schwerpunkt der praktischen Tätigkeit zunächst nicht bei den Ländern liegen, sondern zentral zum Bund verschoben. Die betroffenen Straftaten – bzw. hier: Sachverhalte mit strafrechtlichem Anfangsverdacht – bewegen sich aber hier in einem rechtsdogmatisch höchst komplexen Umfeld. So ist oftmals schwer zu beurteilen, ob eine Meinungsäußerung etwa noch als Wahrnehmung berechtigter Interessen gemäß § 193 StGB zu subsumieren ist. Insbesondere ist auf eine komplexe, durch die Rechtsprechung des Bundesverfassungsgerichts zur Meinungsfreiheit entwickelte, Dogmatik zurückzugrei-

fen. Beleidigungsdelikte sind allerdings insofern nach derzeitigem Stand von der Meldepflicht wohl nicht erfasst, was diese Problematik ein wenig entschärft. Im Ergebnis ist aber zu hinterfragen, in welchen Fällen „konkrete Anhaltspunkte“ für die genannten Straftaten vorliegen und wie die Anbieter der sozialen Netzwerke dies künftig beurteilen sollen.

III. Weitere Datenverarbeitung und Auskunftsverfahren

1. Ausgangspunkt: Telemedienanbieter

Die Auskunft zu Nutzungs- und Bestandsdaten wird in § 15a TMG neu definiert und erweitert. Dies gilt insbesondere in Bezug auf Zugangsdaten und Passwörter. Diese Erweiterungen halte ich für unverhältnismäßig.

Zu den Bestandsdaten werden nach der geplanten Regelung auch Daten gezählt, „mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird“. Dies sind vor allem – aber ggf. nicht nur – Passwörter, Access Tokens, Geheimnisse für Zwei-Faktor-Authentifizierungs-Apps (2FA) und andere Daten, die dazu dienen, die nutzende Person zu authentifizieren oder ihr Zugang zu Angeboten und Diensten zu ermöglichen. Nach dem sog. Doppeltürmodell des BVerfG ist der geplante § 15a TMG nur eine Übermittlungsnorm („Übermittlungstür“). Sie setzt auf der Seite der Empfängerbehörde als Gegenstück zur Übermittlungsnorm eine Erhebungsnorm voraus („Empfängertür“, dazu siehe unten).

Bereits auf der Übermittlungsebene im geplanten § 15a TMG stellen sich verschiedenste Fragen. Zunächst ist darauf hinzuweisen, dass eine Vielzahl von Diensten erfasst sein kann. Neben E-Mail-Diensten und Cloud-Speichern kann dies etwa auch Online-Händler oder Angebote von Online-Banking betreffen. Auch deren Passwörter wären im Klartext herauszugeben. Hier stellt sich besonders die Frage der Datensicherheit.

Technisch gesehen werden gesetzeskonform arbeitende Anbieter die Passwörter als Hash speichern und deshalb nicht herausgeben können. Diese können nicht für den Zugriff auf Endgeräte oder Speichereinrichtungen verwendet werden. Die im Gesetzesentwurf verlangte Herausgabe kann also nicht umgesetzt werden, ohne von den Diensteanbietern zu verlangen, datenschutzrechtliche Vorgaben zu verletzen. Unklar ist, wie in Fällen der zwei-Faktor-Authentifizierung vorzugehen ist, die z.B. beim Online-Banking durch die neue Zahlungsdiensterichtlinie nunmehr verpflichtend vorgesehen ist.

Nicht geregelt ist, ob sich aus der neuen Vorschrift für die Anbieter eine Pflicht ableiten lässt, nach der die Anbieter im Zweifel die Passwörter so im Klartext speichern müssen,

dass sie diese im Falle einer behördlichen Anforderung herausgeben könnten. Richtigerweise wäre ohne eine ausdrückliche Regelung zu folgern, dass eine Pflicht zur Speicherung der Zugangsdaten in einer durch Dritte leicht aufhebbaren Verschlüsselung oder gar im Klartext nicht bestehen kann. Es ist allerdings auch denkbar, dass Strafverfolgungsbehörden in der Praxis eine andere Auffassung vertreten werden. Dies würde die Datensicherheit und den Datenschutz massiv konterkarieren. Zudem würden Strafverfolgungsbehörden möglicherweise gemäß dem geplanten § 15 Absatz 1 Satz 4 TMG auch die Herausgabe weiterer Daten erzwingen können, die insbesondere brute-force-Entschlüsselungen der übermittelten Passwort-Hashes ermöglichen (z.B. Herausgabe des sog. Pepper-Wertes). Auch dies könnte die Datensicherheit über den Einzelfall hinaus beeinträchtigen. Letztlich müsste man dann in all diesen Fällen fragen, ob die nach der Zahlungsdiensterichtlinie notwendige Sicherheit der Authentifizierung noch gewährleistet ist. Da sich das TMG nicht nur an Verbraucher richtet, ist zudem fraglich, ob etwa Banken dann noch untereinander sicher kommunizieren könnten oder sich die Bundesrepublik aus dem elektronischen Bankenverkehr zurückziehen müsste. Eine Pflicht zu einer einfach aufzuhebenden Verschlüsselung oder gar zur Klartextspeicherung lehne ich ab. Neben den bereits genannten Argumenten (Missbrauchsgefahr, Ermittlungsbehörde könnte unter Identität des Beschuldigten auftreten) verstieße diese gegen höherrangiges Recht. Gemäß Art. 32 DSGVO müssen Anbieter technische und organisatorische Maßnahmen zur Datensicherheit treffen. Hierzu gehört auch die sichere verschlüsselte Speicherung und Übermittlung von Passwörtern. Dies hat auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in der "Orientierungshilfe „Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung" vom 29.03.2019 klargestellt.

Unklar ist, ob sich die Vorschriften auch auf etwaige temporär gespeicherte Session-Cookies o.ä. beziehen, mit denen sich Zugang erlangen lässt. Auch dafür könnte die Formulierung im geplanten § 15a Absatz 1 Satz 4 TMG sprechen. Dieser bestimmt: „Für die Auskunftserteilung sind sämtliche unternehmensinternen Datenquellen zu berücksichtigen“. Nach dem Wortlaut führt dies sogar dazu, dass alle vorhandenen Speicherquellen und -server unabhängig vom Zweck zu durchleuchten wären. Dazu müssten auch Sicherungs- oder Protokolldatenserver einbezogen werden. Selbst Dateien des betrieblichen Datenschutzbeauftragten blieben nicht verschont. Unklar ist, wie die im Ausland gespeicherten Daten betroffen sind. Zu dieser Problematik hat die DSK in einer Entschließung zum Entwurf einer e-Evidence-VO kritisch Stellung genommen.[1]

1 https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/20181107_EntschliessungE_Evidence.pdf; siehe dazu auch

Insgesamt sehe ich den geplanten § 15a Abs. 1 TMG als unverhältnismäßig an.

Neben den bereits genannten Kritikpunkten sind dafür auch die weiteren Verwendungsmöglichkeiten dieser als „Bestandsdaten“ deklarierten Informationen maßgeblich. Der geplante § 15a TMG nennt hierfür nicht nur Behörden, die die an sie übermittelten Daten zulässig erheben dürften, sondern z.B. auch Nachrichtendienste und Behörden zur Verfolgung von Ordnungswidrigkeiten. Ob eine derart eingriffsintensive Erhebungsgrundlage zur Verfolgung von Ordnungswidrigkeiten verfassungsrechtlich überhaupt denkbar wäre, ist zu bezweifeln. Zu den Nachrichtendiensten siehe unten.

2. Verarbeitung beim BKA

a) Meldungen der Anbieter

Die **Datenerhebung** durch das BKA soll unabhängig davon möglich sein, ob ein strafrechtlicher Anfangsverdacht vorliegt oder nicht. Das BKA wird insofern nicht als strafrechtliche Ermittlungsbehörde tätig, sondern soll sich auf die Vorschriften zur Zentralstellenaufgabe stützen. Diese Befugnis setzt aber keinen Anfangsverdacht voraus. Dazu soll die entsprechende Befugnis in § 10 BKAG erweitert werden (Artikel 3 des Entwurfs, dazu siehe unten). Gerade im Umfeld von Presse und Medien ist dies vor allem bei niedrigschwelligen Delikten bedenklich, die nicht von der Meldepflicht umfasst sind, insbesondere bei Beleidigungen (§ 185 StGB). Die Zentralstellenaufgabe greift aber unabhängig von der Meldepflicht.

Die **weitere Verarbeitung** der übermittelten Daten ist unklar, da der Gesetzentwurf keine Regelungsvorschläge enthält. Es ist zu klären, wie das BKA mit den eingehenden Meldungen weiter verfahren soll. Das BKA könnte auf der einen Seite nur kurz prüfen, welche Landesbehörde zuständig ist, den Sachverhalt an das Land abgeben und gleichzeitig die Daten aus dem eigenen Bestand löschen. Auf der anderen Seite könnte das BKA die Daten aber nach dem 2018 neu gefassten BKAG – z.B. als „Prüffall“ gemäß § 18 Abs. 3 BKAG, ggf. auch nach §§ 18 Abs. 1 und 2 BKAG – in das Informationssystem eingeben und Querverbindungen suchen. Die Datenverarbeitung würde dadurch ein höheres Gewicht erhalten. Für die zukünftige beim BKA geführte bundesweite informationstechnische Basis „Polizei 2020“ ist eine Speicherung aller Daten in einem „Datentopf“ vorgesehen, der umfassende Querverbindungen erlaubt. Welche Datenanalysen möglich sein werden, ist derzeit noch völlig unklar.

---

https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Stellungnahmen/Opinion23_2018_eevidence.pdf

Das Verfahren sollte m.E. in der Praxis so ausgestaltet werden, dass das BKA zunächst prüft, ob überhaupt ein Anfangsverdacht vorliegt. Kann dies bejaht werden, sollte es sofort an die zuständige Landespolizei bzw. Staatsanwaltschaft abgeben. Nur wenn diese aufgrund der fehlenden Bestandsdaten nicht bestimmt werden kann, sollte das BKA befugt sein, weitere Daten zu erheben, soweit dies erforderlich ist, um die zuständige Polizeibehörde zu bestimmen. Der geplante Gesetzestext enthält hierzu aber keinerlei Vorgaben.

b) Erweiterte Auskunftsbefugnisse, u.a. Passwörter

Mit der neuen Regelung im TMG korrespondiert die geänderte Erhebung zu Zwecken der Zentralstelle. Diese war bislang für Telekommunikations-Bestandsdaten in § 10 BKAG geregelt und wird jetzt auf Telemediendaten erweitert. Für sie ist ein Anfangsverdacht im Sinne der Strafprozessordnung nicht erforderlich. Auch sonst werden keine besonderen Verdachts- oder Gefahrenmomente gefordert. Genügend ist, dass die Daten für folgende Aufgaben erforderlich sind: „Aufgaben als Zentralstelle nach § 2 Absatz 2 Nummer 1 und Absatz 6 zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung“, daneben Zeugenschutz und Personenschutz. Aus diesem Grund hatte ich bereits in der Vergangenheit die bisherigen Vorschriften kritisiert, zuletzt in meiner Stellungnahme gegenüber dem Bundesverfassungsgericht. Schon nach alter Rechtslage konnte das BKA Passworte zu Telekommunikationsdiensten herausverlangen (betrifft PIN und PUK).

Die Erhebungen in der Zentralstellenfunktion hatte ich im Jahr 2017 kontrolliert und dabei insbesondere die unzureichende Dokumentation von Maßnahmen kritisiert. Allerdings hatte ich mit Verweis auf die anstehende Prüfung des Vorgangsbearbeitungssystems beim BKA keine Beanstandung ausgesprochen. Zu weiteren Punkten verweise ich auf den Bericht.[2]

Für die TMG-Daten soll nach dem Entwurf jetzt eine ähnliche Regelung gelten. Auch hier kann das BKA Passwörter herausverlangen. Es ist zwar – nur für Passwörter – ein Richtervorbehalt vorgesehen. Jedoch hat etwa eine im Auftrag des BMJV durchgeführte Evaluation der besonders eingriffsintensiven Telekommunikationsüberwachung gezeigt, dass nur 23,5 Prozent der richterlichen Beschlüsse als substantiiert begründet gewertet werden

[2] Der Bericht ist aufgrund einer IFG-Anfrage unter folgendem Link verfügbar: https://fragdenstaat.de/anfrage/kontrolle-beim-bka/403928/anhang/BfDI_Prfbericht_BKA_geschwrzt_geschwaerzt.pdf; siehe dazu auch 27. TB Nr. 9.3.6.1

können.[3] Entscheidend sind im Übrigen nicht die verfahrensmäßige Absicherung, sondern die materiellen Schwellen, die eingezogen sind. Insbesondere kann der Richtervorbehalt Bestimmtheitsdefizite nicht kompensieren (BVerfGE 113, 348, 378). Einzige materielle Voraussetzung wird neben dem „Zentralstellenzweck“ oder „sonst Zwecken der Auswertung“ sein, dass zusätzlich die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. In einem Interview verweist die Ministerin darauf, dass der Zugriff auf die Zugangsdaten nur in eng begrenzten Anwendungsfällen des Terrorismusverdachts vorkommen werde. Dies ist im Gesetzentwurf jedoch nicht entsprechend geregelt: vielmehr finden sich nur die genannten niedrigen Schwellen und auf der Ebene des TMG eine Öffnung auch für die Nachrichtendienste, denen deutlich weitere Aufgaben im Vorfeld von Gefahren zugewiesen sind. Es liegt aber in der Verantwortung des Gesetzgebers, eine verhältnismäßige Vorschrift zu schaffen und er darf dies nicht der Praxis überlassen.

Die Vorschriften zu denTelekommunikationsbestandsdaten waren bereits einmal angepasst worden, nachdem das Bundesverfassungsgericht die Parallelregelung in der StPO zu beurteilen hatte. Jetzt soll gelten, dass *zusätzlich die gesetzlichen Voraussetzungen für die Nutzung der Daten* vorliegen. Deshalb müssen zugleich die Voraussetzungen für die TKÜ vorliegen. Das ist aber schon insoweit inkongruent, als zu Zwecken der Zentralstelle niemals eine TKÜ durchgeführt werden kann, sondern nur zu anderen Zwecken.

Welche Voraussetzungen für die Nutzung der Daten vorliegen müssen, ist hier schwieriger zu beurteilen als im Bereich der Telekommunikation. Bei den bislang von § 10 Abs. 1 S. 2 BKAG umfassten Telekommunikationsdaten ist immerhin klar, dass die Inhalte nur über eine gesetzliche Befugnis zur Telekommunikationsüberwachung erhoben werden können. Hier aber sehe ich das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme betroffen. Denn der Sache nach geht es um den Zugriff auf die auf einem solchen System gespeicherten Daten. Denkbar wäre zum einen der offene Zugriff. Dafür kommen insoweit wohl die Regelungen zur Beschlagnahme in der StPO in Betracht. Die Maßnahme muss dafür der betroffenen – d.h. den Account besitzenden – Person gegenüber bekannt sein. Heimlich ist ein solcher Zugriff aber nur als Online-Durchsuchung vorstellbar. Beides kann das BKA aber in seiner Zentralstellenfunktion nicht durchführen.

In jedem Fall liegen die den Zugang ermöglichenden Daten der Behörde in einer Weise vor, die tatsächlich eine heimliche Nutzung ermöglicht. Im Falle nur offener Maßnahmen wäre dies zwar rechtlich unzulässig, aber technisch nicht ausgeschlossen.

---

[3] Albrecht, Dorsch, Krüpe, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer Ermittlungsmaßnahmen, Abschlussbericht, MPI-Freiburg 2003, S. 447.

Deshalb ist in beiden Fällen der Aspekt der Datensicherheit zentral. Wo soll das Passwort beim BKA hinterlegt werden? Wer erhält Kenntnis? An welche Behörde darf das BKA das Passwort reversibel verschlüsselt oder gar im Klartext übermitteln? An welcher Stelle bzw. in welchem Informationssystem legt die Empfängerbehörde es ab? Bei der klassischen Online-Durchsuchung besteht die rechtliche Anforderung, dass alle Ermittlungsschritte und Datenzugriffe zu protokollieren sind. Es muss stets nachvollziehbar sein, welche Daten die Behörde ausgelesen oder gar verändert hat. So muss technisch ausgeschlossen werden, dass etwa die Polizeibehörde selbst – sei es absichtlich oder versehentlich – Beweise verändert oder Daten „im Namen" des Beschuldigten gespeichert oder irgendwohin weitergeleitet hat. All dies ist nicht möglich, wenn der Behörde das Passwort im Klartext vorliegt. Es wird dann für die betroffene Person kaum je praktisch nachweisbar sein, dass sie nicht selbst gehandelt hat. Sobald das Passwort mehr als einer Person bekannt wird, kommen alle diese Personen als Tatverdächtige in Betracht, sobald danach Straftaten mit dem betreffenden Account begangen werden. Dies schließt Polizeibeamte, Staatsanwälte und Richter nicht aus. Insofern stellen sich die Fragen der Datensicherheit auch zum Schutz der Mitarbeitenden von Polizei, Staatsanwaltschaft und Gerichten.

Wenn überhaupt, müsste die Übergabe und Nutzung von Passwörtern oder sonstigen Zugangsmöglichkeiten für die Online-Durchsuchung in der jeweiligen Spezialbefugnis geregelt werden, also insb. in § 100b StPO. Dann würden zumindest die Protokollierungspflichten nach § 100c Abs. 6 StPO i.V.m. § 100b Abs. 4 StPO frühzeitiger greifen.

3. Strafverfolgung

Zur Strafverfolgung werden insbesondere die §§ 100g, 100j StPO für Telemediennutzungs- bzw. Bestandsdaten ergänzt. Für die Passwörter greift formell ebenfalls ein Richtervorbehalt. Materiell ist nur ein Anfangsverdacht einer beliebigen Straftat Voraussetzung. Ein Straftatenkatalog ist nicht vorgegeben. Allerdings ist auch hier die vom BVerfG geforderte Formulierung enthalten, nach der die *gesetzlichen Voraussetzungen für die Nutzung der Daten* vorliegen müssen. Ich sehe hier – wie oben dargelegt – insbesondere die der Online-Durchsuchung als maßgeblich an. Die Rechtsgrundlage kann aber in der Praxis sehr streitig werden. Zum Richtervorbehalt und den materiellen Anforderungen siehe auch oben 2.

Im Übrigen stellen sich hier im Wesentlichen dieselben Probleme, wie bereits zum BKAG ausgeführt.

d) Nachrichtendienste

Die Nachrichtendienstgesetze werden mit dem Entwurf nicht geändert. Ob mit dem für Anfang 2020 erwarteten 2. Referentenentwurf zur Harmonisierung des Verfassungsschutzrechts Parallelnormen eingeführt werden, ist nicht bekannt. In § 15a TMG-E sind die Nachrichtendienste aber ausdrücklich erwähnt. Es ist demnach zu erwarten, dass der Gesetzgeber auch hier niedrigschwellige Zugriffsregelungen anstreben wird. Die Nachrichtendienste dürfen nach dem klassischen Rechtsverständnis aber keine polizeilichen Befugnisse haben. Deshalb war zum Beispiel niemals eine „Wohnungsdurchsuchung“ oder dergleichen vorgesehen, weder offen noch verdeckt. Dies würde sich auch nicht mit dem Selbstbild der Dienste vertragen, die sich selbst – zu Recht – nicht als exekutive Geheimdienste, sondern eben nur als Nachrichtendienste sehen. Eingriffe, die diesem nicht nur gleichkommen, sondern noch eingriffsintensiver den privatesten Bereich berühren, sind folglich dem Recht der Nachrichtendienste traditionell wesensfremd. Namentlich gilt dies für die heimliche Onlinedurchsuchung. Diese steht in der Eingriffsintensität der heimlichen Wohnraumüberwachung gleich. Wenn schon keine offene Wohnungsdurchsuchung möglich ist, dann darf es erst recht keine heimliche geben.

Deshalb stellt sich besonders dringlich die Frage, wozu die Dienste die Passwörter benötigen. Schon bei den eher offen handelnden Behörden ist die Kontrolle, auf welche Weise die Passwörter genutzt werden, nahezu unmöglich (siehe oben). Bei den Nachrichtendiensten stellt sich die Frage nach der Kontrollierbarkeit noch dramatischer.

Mit freundlichen Grüßen
Im Auftrag