BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Entwurf **19915/2020**

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

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

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
FON (0228) 997799-5000
FAX (0228) 997799-5550
E-MAIL referat32@bfdi.bund.de
www.datenschutz.bund.de

DATUM Bonn, 02.03.2020
GESCHÄFTSZ. 32-642/041#1435

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

1. An den
stv. Vorsitzenden
Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages
Herrn Dr. Heribert Hirte

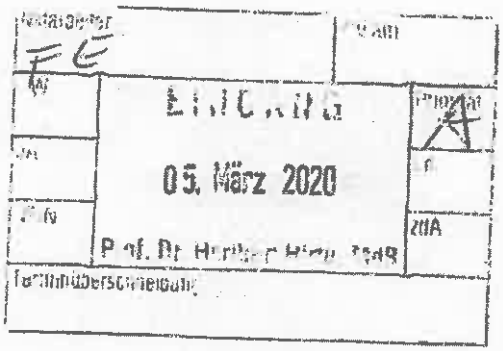
2. An die
Vorsitzende
Ausschusses für Inneres und Heimat
Frau Andrea Lindholz

3. An den Vorsitzenden
des Ausschusses Digitale Agenda
Herrn Manuel Höferlin

4. An den
Vorsitzenden
des Ausschusses für Wirtschaft und Energie
Herrn Klaus Ernst

Platz der Republik 1
11011 Berlin

Deutscher Bundestag
Ausschuss für
Recht und Verbraucherschutz
Ausschussdrucksache
19(6)121
10. März 2020



BETREFF **Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität**
BEZUG BR-Drucksache 87/20
ANLAGEN 1

Sehr geehrter Herr Vorsitzender,

der Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität dürfte in Kürze in Ihrem Ausschuss beraten werden. Vor diesem Hintergrund übersende ich Ihnen meine Stellungnahme zu diesem Gesetzentwurf und wäre Ihnen für eine Einbeziehung in Ihre Beratungen dankbar.

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

Für weitere Fragen stehe ich Ihnen gerne zur Verfügung..

Mit freundlichen Grüßen

Ulrich Kelber

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Bonn, den 26.02.2020

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt die dem Gesetzentwurf zugrunde liegende Auffassung, nach der Betroffene vor Bedrohungen effektiv geschützt werden sollten. Hierbei hilft aber in erster Linie ein effektiver Gesetzesvollzug durch die Sicherheitsbehörden. Zudem helfen nur solche Sicherheitsgesetze, die mit Bedacht erlassen und zielgerichtet ausgestaltet werden. Der vorliegende Entwurf enthält zahlreiche Vorschläge, die deutlich über den Bereich von Hasskriminalität und Rechtsextremismus hinausgehen. Ob der Entwurf seine verfolgten Ziele erreicht, erscheint mir mehr als fraglich.

I. Allgemein

Der Entwurf enthält erhebliche Eingriffe in Grundrechte der Bürgerinnen und Bürger. Es ist zweifelhaft, ob diese in jeder Hinsicht erforderlich und damit verhältnismäßig sind. Bereits die Grundkonzeptionen der Meldepflicht und der Rolle des Bundeskriminalamtes (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. Möglicherweise ist es ohnehin nicht nötig, die bestehende Praxis völlig neu zu gestalten. Beispielsweise haben einzelne Länder

Husarenstraße 30
53117 Bonn
Fon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de

Schwerpunktstaatsanwaltschaften eingerichtet, die als zentrale Anlaufstellen bereits jetzt tätig werden.

In der jüngeren Vergangenheit sind mir zahlreiche Gesetzentwürfe vorgelegt worden, die in kurzen Abständen zum Beispiel immer wieder die Strafprozessordnung betrafen. Zu nennen sind etwa die Entwürfe für ein „Gesetz zur Modernisierung des Strafverfahrens", für ein „Gesetz 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". Deshalb stellt sich die Frage, welchem durchgängigen Konzept diese Gesetzgebungstätigkeit folgt.

II. Meldesystem

Mit der 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, wie 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. Zudem gibt es auf der strafrechtlichen Ebene bereits in den Ländern zentrale Anlaufstellen. Dass derartige Alternativen nicht umfassend untersucht und gegebenenfalls evaluiert worden sind, ist bereits strukturell zu kritisieren.

Geplant ist nun, dass Anbietern 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. Anschließend sollen sie an das BKA melden.

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 in einem rechtsdogmatisch höchst komplexen Umfeld. So ist zu hinterfragen, in welchen Fällen „konkrete Anhaltspunkte" für die genannten Straftaten vorliegen und wie die Anbieter der sozialen Netzwerke dies künftig beurteilen sollen.

§ 3a Abs. 4 Nr. 2 NetzDG-E sieht für die Übermittlung der Anbieter unter anderem vor, die IP-Adresse einschließlich Portnummer, die der Nutzer verwendet hat, an das BKA zu übermitteln, soweit diese vorhanden sind. Diese Daten sind herauszugeben, bevor überhaupt das Vorliegen eines Anfangsverdachts von einer Strafverfolgungs- bzw. Polizeibehörde geprüft wurde. Zu bevorzugen wäre eine Regelung, nach der die Verpflichteten zunächst nur den Inhalt übermitteln und erst nach der Feststellung eines Anfangsverdachtes bzw. einer Gefahrenlage die IP-Adresse einschließlich Portnummer übermitteln. Bis dahin könnten die Daten zunächst im „quick freeze" Verfahren gespeichert werden.

III. Auskunftsverfahren und weitere Datenverarbeitung

1. Ausgangspunkt: Telemedienanbieter („Übermittlungstür")

Neben dieser Meldepflicht will der Entwurf die Auskunft zu Nutzungs- und Bestandsdaten in § 15a TMG neu definieren und erweitern. Dies ist eine allgemeine Regelung, die nicht nur die Meldungen nach dem Netzdurchsetzungsgesetz betrifft, also nicht nur den in der Überschrift genannten Rechtsextremismus und die Hasskriminalität. Sie regelt vielmehr alle Bereiche bis hin zu allgemeinen Ordnungswidrigkeiten.

Nach dem sog. Doppeltürmodell des Bundesverfassungsgerichts sind die geplanten §§ 15a, 15b TMG nur Übermittlungsnormen („Übermittlungstür"). Sie setzen bei den Empfängerbehörden als Gegenstück eine Erhebungsnorm voraus („Empfängertür"). Allgemeine „Übermittlungstür" für die Anbieter von Telemediendiensten ist der neue § 15a TMG-E. Der Zugriff auf Passwörter und andere Daten, die den Zugriff auf Endgeräte oder Speichereinrichtungen ermöglichen, wird in einer eigenen Vorschrift, dem § 15b TMG-E geregelt.

a) Allgemeine Auskunftsregelung, § 15a TMG-E

Der geplante § 15a TMG-E gilt niedrigschwellig für alle Ordnungswidrigkeiten, Straftaten, Gefahren für die Öffentliche Sicherheit und die Übermittlung an Nachrichtendienste. Anders als § 113 Abs. 1 TKG rechtfertigt er es nicht nur, Bestandsdaten zu übermitteln, sondern auch Nutzungsdaten. Das stellt eine höhere Eingriffsqualität dar.

Die Vorschrift enthält eine Formulierung, nach der „alle unternehmensinternen Datenquellen" zu berücksichtigen sind. Damit können umfangreiche Nutzungsprofile herausverlangt werden. Wann dies verhältnismäßig ist, wird sich letztlich anhand der Vorschriften für den Zugriff auf diese Daten entscheiden („Empfängertür"). Gleichwohl wirft die weite Öffnung des § 15a TMG, der auch die Übermittlung bei Ordnungswidrigkeiten zulässt, erhebliche Fragen auf.

b) Zugangsdaten (Passwörter etc.), § 15b TMG-E

Positiv zu bewerten ist zwar, dass der Entwurf in § 15b Abs. 2 TMG-E nun deutlich höhere Übermittlungsschwellen vorsieht. Gleichwohl sehe ich die Regelung weiterhin kritisch.

Zugangsdaten 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 geplanten § 15b TMG stellen sich bereits auf der Übermittlungsebene verschiedene 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 herauszugeben. Hier stellt sich besonders die Frage der Datensicherheit.

Technisch gesehen müssen gesetzeskonform arbeitende Anbieter die Passwörter als Hash speichern und können sie deshalb nicht in einer einfach verwendbaren Form herausgeben. Sie können deshalb nicht unmittelbar für den Zugriff auf Endgeräte oder Speichereinrichtungen verwendet werden.

Nach Kritik in der Ressortabstimmung regelt § 15b Abs. 3 Satz 2 nunmehr, dass die Verschlüsselung „unberührt" bleibt. Wenn das ernst gemeint ist, stellt sich aber die Frage, welchen Sinn die Herausgabe der Zugangsdaten hat. Eine gute Verschlüsselung ist so gestaltet, dass der Provider die Daten ohne Eingabe durch den Kunden nicht selbst entschlüsseln kann. Gemeint sein dürfte also möglicherweise Folgendes:

Gemäß dem geplanten § 15b Abs. 1 S. 2 TMG-E sollen die Provider auch an dieser Stelle „sämtliche unternehmensinternen Datenquellen" nutzen, um den Behörden Zugangsdaten zur Verfügung zu stellen. Danach müssten ggf. alle technischen Daten mit herausgegeben werden, mit denen die Kundenschlüssel generiert werden (z.B. also etwa Verschlüsselungsalgorithmen oder der sog. Pepper-Wert). Diese Informationen ermöglichen insbesondere erleichterte brute-force-Entschlüsselungen der übermittelten Passwort-Hashes.

Auch dies könnte die Datensicherheit über den Einzelfall hinaus beeinträchtigen. Werden solche Daten herausgegeben, kann das gegebenenfalls nicht nur die Zielperson des Verfahrens, sondern alle Kunden betreffen.

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 un-

tereinander sicher kommunizieren könnten oder sich die Bundesrepublik aus dem elektronischen Bankenverkehr zurückziehen müsste.

Eine – ggf. mittelbare – Pflicht zu einer einfach aufzuhebenden Verschlüsselung lehne ich ab. Neben anderen Argumenten (Missbrauchsgefahr, Ermittlungsbehörde könnte unter der 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 unter Berücksichtigung des Stands der Technik 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 im Übrigen, wie etwa in Fällen der zwei-Faktor-Authentifizierung vorzugehen ist, die z.B. beim Online-Banking durch die neue Zahlungsdiensterichtlinie nunmehr verpflichtend vorgesehen ist. Ebenfalls ist unklar, 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 § 15b Abs. 1 S. 2 TMG-E sprechen. 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]

2. Verarbeitung beim BKA („Erhebungstür" und weitere Schritte)

a) Erweiterte Auskunftsbefugnisse

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. Es genügt, 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 ge-

---

1 https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/20181107_EntschliessungE_Evidence.pdf; siehe dazu auch https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Stellungnahmen/Opinion23_2018_eevidence.pdf

genüber 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 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.

Anders als in einem ersten Entwurf soll der geplante § 10 BKAG-E nach erheblicher Kritik nicht mehr den Zugriff auf die Zugangsdaten einschließlich Passwörter regeln. Das ist zu begrüßen. Anwendbar sind deshalb allein die Vorschriften der sog. Online-Durchsuchung.

b) Empfang der Meldungen der Anbieter

Übermitteln die Anbieter ihre Meldungen nach dem NetzDG-E, ist dafür ebenfalls der genannte § 10 BKAG die Rechtsgrundlage. § 10 BKAG setzt keinen Anfangsverdacht voraus. Das BKA soll also unabhängig davon Daten erheben dürfen, 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.

Dazu, wie das BKA mit den Meldungen weiter verfahren soll, enthält der Gesetzestext keine Regelungen. 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 im Jahr 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 „Datenpool" vorgesehen, der umfassende Querverbindungen erlaubt. Welche Datenanalysen möglich sein werden, ist derzeit noch unklar.

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 den Sachverhalt sofort an die zuständige Landespolizei bzw. Staatsanwaltschaft abgeben. Nur wenn diese aufgrund der fehlenden Bestandsdaten nicht bestimmt werden kann, sollte

---

[2] Der Bericht ist 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

das BKA befugt sein, weitere Daten zu erheben, soweit dies erforderlich ist, um die zuständige Polizeibehörde zu bestimmen. Der geplante Gesetzestext enthält hierzu aber keine Vorgaben.

3. Strafverfolgung

Zur Strafverfolgung werden insbesondere die §§ 100g, 100j StPO für Telemediennutzungs- bzw. Bestandsdaten ergänzt.

a) § 100g StPO (Artikel 2 Nr. 2)

Die Vorschrift über Telekommunikationsverkehrsdaten wird es in Zukunft auch erlauben, Telemediennutzungsdaten zu erheben. Beide werden tatbestandlich gleichgestellt. Es ist aber die Frage zu stellen, ob beides dieselbe Eingriffsintensität hat. Zwar ließe sich hier ein unterschiedlicher Anwendungsbereich des Art. 10 GG diskutieren. Zu bedenken ist aber, dass Telemediennutzungsdaten unter Umständen stärkere Aufschlüsse darüber zulassen, mit welchen Inhalten sich die betroffene Person beschäftigt hat. Anders als Telekommunikationsverkehrsdaten lassen Telemediennutzungsdaten ggf. nicht nur den Schluss auf die an einer Kommunikation beteiligten Personen zu, sondern zum Beispiel auch über aufgerufene Webseiten oder Angebote. Daraus lassen sich im Einzelfall umfangreiche Rückschlüsse über die Persönlichkeit der betroffenen Person ziehen.

b) § 100j (Artikel 2 Nr. 3)

Schwelle für die Erhebung von Passwörtern und anderen Zugangsdaten ist nur, dass die Herausgabe „für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist". Materiell ist damit ein Anfangsverdacht einer beliebigen Straftat Voraussetzung. Ein Straftatenkatalog ist nicht vorgegeben. Damit ist die Erhebungstür in § 100j StPO prinzipiell weiter gefasst als die Übermittlungstür in § 15b TMG.

Diese Divergenz ist erklärungsbedürftig. Nicht nachvollziehbar ist, aus welchen Gründen die Ermittlungsbehörde unter niedrigeren Voraussetzungen auf die Daten zugreifen können soll, als die Übermittlungsregelung dies zulässt. Zutreffend verweist § 15b TMG-E auf die Voraussetzungen des § 100b StPO.

Allerdings ist die vom BVerfG für den Bereich der Telekommunikation geforderte Formulierung enthalten, nach der zusätzlich die *gesetzlichen Voraussetzungen für die Nutzung der Daten* vorliegen müssen.

Bei den bislang von § 100j StPO 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. Insofern verweist § 15b TMG folgerichtig auf § 100b StPO, der die Online-Durchsuchung regelt.

Denkbar wäre zwar auch der offene Zugriff. Dafür könnten insoweit wohl die Regelungen zur Beschlagnahme in der StPO in Betracht kommen. Die Maßnahme muss dafür der betroffenen – d.h. den Account besitzenden – Person gegenüber bekannt sein. Heimlich ist ein solcher Zugriff nur als Online-Durchsuchung vorstellbar. Heimlich ist der Zugriff etwa dann, wenn er nur dem Diensteanbieter mitgeteilt wird, nicht hingegen dessen betroffener Kundin oder dem Kunden gegenüber. Möglicherweise ist aber ein solcher offener Zugriff kaum denkbar. Denn die den Zugang ermöglichenden Daten liegen der Behörde in einer Weise vor, die tatsächlich eine heimliche Nutzung von Beginn an ermöglicht. Im Falle nur offener Maßnahmen wäre dies zwar rechtlich unzulässig, aber technisch nicht ausgeschlossen. Solange dies aber nicht ausgeschlossen oder zumindest kontrollierbar ist, kommen hier allein die Vorschriften zur Online-Durchsuchung für den Zugriff in Betracht. Deshalb ist unverständlich, weshalb die Regelung nicht in § 100b StPO verankert ist.

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 aber nicht möglich, sobald der Behörde Benutzerkennung und Passwort im Klartext vorliegen und der Zugriff hierauf nicht technisch streng reglementiert ist. Es würde 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 im Übrigen 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 betreffen die Fragen der Datensicherheit auch den Schutz der Mitarbeitenden von Polizei, Staatsanwaltschaften und Gerichten. Deshalb stellt sich die Frage, wo das Passwort bei der Ermittlungsbehörde hinterlegt werden soll. Wer erhält innerhalb der beteiligten Behörden Kenntnis? An welche weitere Behörde darf die erhebende Behörde das Passwort reversibel verschlüsselt oder gar im Klartext übermitteln? An welcher Stelle bzw. in welchem Informationssystem legt die Behörde es ab? Wie wird revisionssicher protokolliert, von wem, wann, in welcher Form und zu welchem Zweck das Passwort eingesetzt wurde und welche Daten im Zielsystem dabei erhoben, verändert, gelöscht oder übermittelt wurden?

Wenn überhaupt müsste die Übergabe und Nutzung von Passwörtern oder sonstigen Zugangsmöglichkeiten für die Online-Durchsuchung deshalb 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. Im vorliegenden Entwurf ist das Passwort – unabhängig von den Vorgaben des § 100b StPO – nach § 100j StPO zu übermitteln. Damit entstehen die genannten Probleme der Datensicherheit.

Es ist zwar –für Passwörter – in § 100j Abs. 2 StPO 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 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). Vor allem umfasst die richterliche Kontrolle nicht, in welcher Form die Passwörter bei den Ermittlungsbehörden verarbeitet werden und wie ihre Verwendung revisionssicher protokolliert wird.