Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag
Ausschuss für
Recht und Verbraucherschutz

Ausschussdrucksache
18(6)346

29. Mai 2017

Andrea Voßhoff
Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

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

An die
Vorsitzende des Ausschusses für
Recht und Verbraucherschutz
des Deutschen Bundestages
Frau Renate Künast, MdB

mit der Bitte um Weiterleitung an die
Mitglieder

und die
Obleute des Rechtsausschusses und
rechtspolitischen Sprecher der Fraktionen
des Deutschen Bundestages

Frau Elisabeth Winkelmeier-Becker, MdB
Herrn Dr. Stephan Harbarth, MdB
Herrn Dr. Johannes Fechner, MdB
Herrn Harald Petzold, MdB
Frau Halina Wawzyniak, MdB
Frau Katja Keul, MdB

Platz der Republik 1
11011 Berlin

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-100
TELEFAX (0228) 997799-550
E-MAIL arbeitsgruppe22@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 29.05.2017
GESCHÄFTSZ. **22-221-1/004#0165**

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

BETREFF **Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze**
HIER BT-Drs. Drucksache 18/11272 und Formulierungshilfe mit Änderungsantrag zur Einführung einer Quellen-Telekommunikationsüberwachung und einer Online-Durchsuchung in der Strafprozessordnung, A-Drs. 18(6)334
BEZUG Öffentliche Anhörung am 31.05.2017

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

Sehr geehrte Frau Vorsitzende,
sehr geehrte Damen und Herren Abgeordnete,

beiliegend übersende ich Ihnen meine Stellungnahme zu dem oben genannten Gesetzentwurf.

Leider hat es das BMJV unterlassen, mich zu dem mit der Formulierungshilfe eingereichten Änderungsantrag zur Einführung einer Quellen-Telekommunikationsüberwachung und einer Online-Durchsuchung in der Strafprozessordnung zu beteiligen (Ausschussdrucksache 18(6)334 v.15. Mai 2017). Von dem Vorhaben habe ich erst am 17. Mai 2017 durch Medienberichte erfahren. Angesichts der erheblichen datenschutzrechtlichen und verfassungsrechtlichen Bedeutung des Vorhabens ist für mich diese Verfahrensweise nicht nachvollziehbar.

Wegen der kurzen Zeitspanne, die mir für die Prüfung zur Verfügung stand, muss ich mich leider auf einige wenige Eckpunkte beschränken.

Mit freundlichen Grüßen

gez. Andrea Voßhoff

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 29.05.2017

Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum

Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drs. 18/11272

und der

Formulierungshilfe mit Änderungsantrag zur Einführung einer Quellen-Telekommunikationsüberwachung und einer Online-Durchsuchung in der Strafprozessordnung, A-Drs. 18(6)334

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

Der Entwurf beinhaltet verfassungsrechtlich erhebliche Risiken und setzt eine gründliche fachliche Auseinandersetzung voraus.

Das BMJV hat es unterlassen, mich gemäß §§ 26 Abs. 3, 24 Abs. 4 BDSG und § 21 GGO an diesem Entwurf zu beteiligen. Das ist umso bedauerlicher, als ich bereits Anfang April darum gebeten hatte, nachdem die Medien erstmals über entsprechende Pläne berichteten.

In der Ressortabstimmung wurde ich zwar zum ursprünglichen Gesetzentwurf beteiligt (BT-Drs. 18/11272). Erst durch weitere Medienberichte habe ich aber am 17. Mai 2017 von der darüber hinausgehenden Formulierungshilfe erfahren, mit der die sog. **Quellen-Telekommunikationsüberwachung** und die **Online-Durchsuchung** in der Strafprozessordnung eingeführt werden sollen (A-Drs. 18(6)334).

Ich konnte den Entwurf daher nur kursorisch prüfen.

A. Änderungsantrag zu Quellen-TKÜ und Online-Durchsuchung, A-Drs. 18(6)334

I. Quellen-Telekommunikationsüberwachung

Ich teile die Ansicht, nach der für die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) im strafrechtlichen Ermittlungsverfahren eine eigenständige Rechtsgrundlage erforderlich ist, sofern man diese Maßnahme befürwortet. Auf den bisherigen § 100a StPO kann die Maßnahme jedenfalls nicht gestützt werden.

Die vorgeschlagene Regelung führt aber unabhängig davon zu erheblichen datenschutzrechtlichen Risiken und zu einem klaren Verfassungsverstoß. Dies gilt besonders für Artikel 1 Nr. 2, mit dem die Quellen-TKÜ im Einzelfall zur „vollwertigen“ Online-Durchsuchung ausgebaut wird. Im Übrigen habe ich Zweifel, ob sich ein Bedarf für derartige Maßnahmen ergibt, vor allem in dem vorgesehenen Umfang.

1. Anwendungsbereich und Straftatenkatalog

Der Entwurf will die Quellen-TKÜ für den gesamten Straftatenkatalog des § 100a Abs. 2 StPO zulassen. Ich habe erhebliche Zweifel an einem daran bestehenden Bedarf der Strafverfolgungsbehörden.

Das Bundesverfassungsgericht hat auf die besonderen Risiken hingewiesen, die mit einer Quellen-Telekommunikationsüberwachung verbunden sind (BVerfGE 120, 274, 308). Mit der Infiltration des Systems sei „die entscheidende Hürde genommen, um das System insgesamt auszuspähen.“ Diese Gefahren allerdings entstehen nicht nur

durch das gezielte Auslesen des Systems durch Ermittlungsbehörden, sondern auch durch abstrakte Gefährdungen. Diese können entstehen, wenn eine Behörde Sicherheitslücken des betroffenen Systems gezielt ausnutzt und eine Überwachungssoftware einfügt. Eine abstrakte Gefährdung über die konkrete Ermittlungstätigkeit der Behörde hinaus entsteht etwa dann, wenn die Infiltration es – auch unabsichtlich – Dritten ermöglicht, in das System einzudringen, beispielsweise durch eine unzureichende Authentifizierung und Verschlüsselung, durch die es einem unberechtigten Dritten ermöglicht wird, eine Nachladefunktion zu nutzen. Zudem besteht das Risiko, unbeabsichtigt Informationen ohne Bezug zur laufenden Telekommunikation zu erheben. Das Bundesverfassungsgericht hebt deshalb die Gefahr hervor, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden könnten.

Daraus folgt: Die Quellen-TKÜ ist im Vergleich zur herkömmlichen TKÜ sowohl mit zusätzlichem Aufwand für die Ermittlungsbehörden als auch mit hohen rechtlichen und technischen Risiken verbunden. Hier gilt für die Quellen-TKÜ aus technischer Sicht nichts anderes als für die Online-Durchsuchung. Um eine zumindest annehmbare Sicherheit in diesem Bereich zu erreichen, ist ein enorm hoher technischer Aufwand notwendig. Ich rege an, den tatsächlichen Aufwand jeder Maßnahme vom Bundeskriminalamt darstellen zu lassen. Anders als bei den Befugnissen des BKA zur vorbeugenden Terrorismusbekämpfung ist hier offenbar an einen breiten Einsatz „in der Fläche“ gedacht. Dies wird die Risiken schon rein quantitativ deutlich erhöhen. Es ist zu bezweifeln, dass bei einem flächendeckenden Einsatz im Bund und bei den Strafverfolgungsbehörden in allen Bundesländern der dafür notwendige technische Aufwand geschaffen und aufrechterhalten werden kann.

Daher kann ein flächendeckender Einsatz in dem Umfang, in dem die Überwachung der Telekommunikation bislang eingesetzt wird, nicht in Betracht kommen. Der vorgesehene Anlasstatenkatalog ist schon aus diesem Grunde abzulehnen.

2. Laufende Telekommunikation – geplante Grenzüberschreitung

Die Quellen-Telekommunikation grenzt das Bundesverfassungsgericht von der Online-Durchsuchung ab, wenn sie sich auf die „laufende Telekommunikation“ beschränkt. Nur dann ist sie allein ein Eingriff in Artikel 10, nicht jedoch gleichzeitig ein Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme. Letzterer ist an deutlich höhere Voraussetzungen zu binden.

Verfassungswidrig ist deshalb Artikel 1 Nr. 1 Buchst. a):

Danach darf die Behörde auch auf dem System der betroffenen Person gespeicherte Daten auslesen, wenn diese Gegenstand früherer Kommunikation waren. Die vorgeschlagene Formulierung lässt den Datenzugriff nämlich bereits für den Fall einer nur hypothetischen Überwachung zu („wenn sie auch während des laufenden Überwa-

gungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.“).

Wie diese Formulierung nahe legt, können die Strafverfolgungsbehörden deshalb außerhalb der laufenden Kommunikation gespeicherte E-Mail-Postfächer, WhatsApp - Accountdaten, gespeicherte SMS, Anruflisten des Mobiltelefons etc. auslesen.

Damit überschreitet der **geplante § 100a Abs. 1** die Grenzen der Telekommunikationsüberwachung und **wird zur echten Online-Durchsuchung**.

Der extrem weiten Auslegung der verfassungsgerichtlichen Rechtsprechung in der Gesetzesbegründung stimme ich ausdrücklich nicht zu. Selbst dann, wenn man dieser folgen wollte, wäre der vorgeschlagene Normtext nicht verfassungsgemäß:

Auch der Übertragungsvorgang in die Cloud oder aus der Cloud ist ein Telekommunikationsvorgang (z.B. Microsoft Cloud-Dienste, Cloud-Dienste der Deutschen Telekom AG, Apple iCloud und viele andere). Damit können die Ermittlungsbehörden nach dem Wortlaut auch solche Informationen vom Zielrechner auslesen, die die Nutzerin oder der Nutzer zwischenzeitlich bei einem der Dienste gespeichert bzw. wieder zurückgeholt hat (z.B. selbst verfasste Textentwürfe, Tagebücher, Fotos, eingescannte medizinische Berichte, persönliche Unterlagen u.v.m.). Damit erfasst die Vorschrift sozusagen auch die Kommunikation der überwachten Person mit sich selbst. Technisch gesehen kommuniziert diese nämlich mit dem Cloud-Anbieter. Diese Kommunikation wird von der vorgeschlagenen Regelung erfasst.

> ***Beispiel:*** *Der junge Assistenzarzt A, benutzt regelmäßig Fernreisebusse zwischen Köln und Amsterdam. Dort besucht er Museen und hat er Freunde. Von Zeit zu Zeit werden in den Bussen dieser Linie bei grenznahen Kontrollen Betäubungsmittel gefunden. A wird als einer der Passagiere erfasst. Denn er sitzt zufällig auf einem Sitz, unter dem 50g Marihuana versteckt sind. Durch einen Wischtest werden an seiner Hand zudem Drogenspuren entdeckt (er war kurz vor der Abfahrt in einem Amsterdamer Café und hat dort Geldscheine und Türklinken berührt und ein Mohnbrötchen gegessen). Es wird gegen ihn ermittelt. Bei einer Observation wird er gemeinsam mit seinem früheren Schulkollegen B gesehen, der wegen Handels mit Cannabisprodukten vorbestraft ist – wovon A aber nichts weiß. Es wird beobachtet, wie B dem A Geld überreicht (A hatte dem B bei einem Klassentreffen die Getränkerechnung ausgelegt). Daraufhin wird zum 1.1.2020 ein TKÜ-Beschluss gegen A erwirkt. Mit der Quellen-TKÜ werden alle Daten von seinem Rechner heimlich ausgelesen, die A ab diesem Zeitpunkt in der Cloud gespeichert oder offenbar von dort auf seinem Rechner zurückgespeichert hat. Darunter befinden sich auch Notizen und Unterlagen zu einzelnen Patientinnen und Patienten, auch zu solchen, die sich wegen einer Suchterkrankung an A gewandt hatten. Ebenfalls lesen die Behörden die gespeicherte E-Mail-Kommunikation und Messenger-*

Nachrichten mit seiner Freundin heimlich aus. Die Behörde ist der Meinung, sie hätte diese Dokumente in der laufenden Telekommunikation erfassen können, wenn es ihr gelungen wäre, den Trojaner früher auf dem Rechner des A unterzubringen. Allerdings war ihre kriminalistische List zunächst misslungen, weshalb sie den Trojaner erst später als geplant am 28.3. einbringen konnte. Am 31.3. lief der Beschluss aus.

Angesichts des Straftatenkatalogs des § 100a Abs. 2 StPO überschreitet der Entwurf damit klar die verfassungsrechtlichen Anforderungen an die geschützten Rechtsgüter (vgl. BVerfGE 120, 274). Das Bundesverfassungsgericht hat seine Auffassung in der Entscheidung zum BKA-Gesetz nochmals bestärkt:

> *„Das Gesetz lässt jedenfalls keinen Zweifel, dass eine Quellen-Telekommunikationsüberwachung nur bei einer technisch sichergestellten Begrenzung der Überwachung auf die laufende Telekommunikation erlaubt ist. Andernfalls kommt allein ein Vorgehen auf der Grundlage des § 20 k I BKAG in Betracht. (…) Denn maßgeblich ist nicht, ob durch eine technisch aufwändige Änderung des Überwachungsprogramms selbst – sei es durch die Behörde, sei es durch Dritte – dessen Begrenzung auf eine Erfassung der laufenden Telekommunikation aufgehoben werden kann, sondern ob das Programm so ausgestaltet ist, dass es – hinreichend abgesichert auch gegenüber Dritten – den mit der Überwachung betrauten Mitarbeiterinnen und Mitarbeitern des Bundeskriminalamts inhaltlich eine ausschließlich auf die laufenden Kommunikationsinhalte begrenzte Kenntnisnahme ermöglicht.“*

In der Entscheidung zur Online-Durchsuchung hatte das Bundesverfassungsgericht bereits zuvor unmissverständlich klargestellt, in Abgrenzung dazu müsse sich die Befugnis zu einer Quellen-TKÜ auf die „laufende“ Telekommunikation beschränken (BVerfGE 120, 274, 309).

Rechtssystematisch ist die neue Regelung als Erhebung „alternativer Beweise“ eine grundlegende Zäsur. Sie treibt die Figur des „hypothetischen Ersatzeingriffs“ in die verkehrte Richtung auf die Spitze. Bislang geht es dabei um die Verwertung bereits vorhandener Erkenntnisse aus einer rechtswidrigen oder eingriffsintensiveren Maßnahme. Damit soll die Verwertung bereits vorhandener Daten verfassungskonform begrenzt werden. Der Vorschlag geht aber den umgekehrten Weg. Nunmehr soll auch die zukünftige – eigentlich nicht zulässige – heimliche Zwangsmaßnahme doch noch möglich gemacht werden. Die Ermittlungsbehörde soll sie darauf stützen dürfen, dass eine Maßnahme in der Vergangenheit mit anderen rechtlich zulässigen Mitteln hypothetisch möglich gewesen wäre. Das gleicht einer Regelung, die in etwa lautet: *„Die Behörde darf Daten zur Not mit eigentlich unzulässigen Mitteln erheben, die sie auf andere Weise auch rechtmäßig hätte erheben dürfen“.*

3. Verfahrenssicherungen

Die vorgesehenen Verfahrenssicherungen werfen Fragen auf:

Unklar ist, wie lange Protokolldaten aufbewahrt bzw. wann sie gelöscht werden. § 20k Abs. 3 BKAG und § 17 TKÜV beinhalten Regelungen zum Umgang mit den Protokolldaten, der **geplante § 100a Abs. 6** hingegen **nicht**. § 17 TKÜV sieht eine Rechenschaftspflicht gegenüber der Bundesnetzagentur und eine Kontrollbefugnis derselben in Bezug auf Protokolldaten vor. Die Anforderungen an den Umgang mit Protokolldaten der „normalen“ TKÜ sind insoweit also strenger als die bei der Quellen-TKÜ.

Unklar ist auch, welche Geräte oder Kennungen im anordnenden Beschluss anzugeben sind. Schon die in § 100e Abs. 3 Nr. 5 StPO-E gewählte Formulierung zeigt deutlich die **Schwierigkeiten**, **"Geräte" eindeutig zu identifizieren**. Die Zeiten mit „einer Festnetzrufnummer“ sind vorbei und man befindet sich – nochmal – außerhalb der TKÜV. Als Folge ist bereits die Identifikation von Geräten problematisch und sollte auch so dargestellt werden. Ehrlicher wäre es, eine Formulierung zu wählen, die dies klarstellt. So wäre etwa vorzusehen, in Fällen, in denen keine sichere Feststellung oder Zuordnung möglich ist, von der Überwachung abzusehen. Ggf. könnte die Ermittlungsbehörde verpflichtet werden, neu zu prüfen, wie eine sichere Zuordnung erlangt werden kann (zur Identifizierung eines Gerätes müsste man wohl beispielsweise die MAC-Adresse oder andere Kennziffern wie Lizenznummern etc. heranziehen).

II. Online-Durchsuchung

1. Straftatenkatalog

Der Straftatenkatalog bei der Online-Durchsuchung ist beachtlich. Er nennt sage und schreibe 74 Paragraphen. Aus Zeitgründen konnte hier nicht geprüft werden, wie viele Straftatbestände sich daraus im Einzelnen ergeben. Darunter sind auf der einen Seite solche, die den strafrechtlichen Schutz höchstrangiger Rechtsgüter betreffen. Darauf ist die Aufzählung aber nicht beschränkt.

Teilweise sind von der Aufzählung nur Qualifikationstatbestände betroffen (z.B. gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260, 260a StGB). In diesen Fällen ist aber zu hinterfragen, welche Anforderungen an die Verdachtsgrundlage zu stellen sind. So könnte beispielsweise bei einer Hehlerei schnell der Verdacht einer gewerbsmäßigen Hehlerei im Sinne des Katalogs bejaht werden. Das würde zur Anwendung dieses eingriffsintensivsten Ermittlungsmittels führen, auch wenn sich dieser Verdacht später nicht bestätigt.

2. Personenkreis

Abzulehnen ist die geplante Reichweite, mit der auch **nicht verdächtige Personen** erfasst werden.

Wie zwar § 100b Abs. 3 S. 1 StPO-E normiert, darf die Maßnahme sich nur gegen den Beschuldigten richten. Dazu regelt aber § 100b Abs. 3 S. 2 StPO-E eine sehr weitreichende Rückausnahme. Danach ist die Maßnahme auch gegen Dritte zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass der Beschuldigte informationstechnische Systeme der anderen Person benutzt und die Durchführung des Eingriffs in informationstechnische Systeme des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird. Im Umkehrschluss aus § 100b Abs. 3 Nr. 1 StPO-E sind die Dritten, deren Geräte infiltriert sind, nicht einmal namentlich zu nennen. Letztlich hat es damit die Ermittlungsbehörde in der Hand, die Dritten auszuwählen.

Dies würde es ermöglichen, sämtliche gemeinsam genutzte IT zu infiltrieren. Betroffen wäre im Zweifel die gesamte Familie, der gesamte Haushalt, die gesamte Wohngemeinschaft, das Rechenzentrum einer Universität, die gesamte shared-workspace- und co-working-Umgebung, das gesamt Internetcafé, das gesamte Unternehmensnetzwerk und die gesamte sonstige „Benutzung“ fremder IT.

Zu hinterfragen ist, wie weit der Begriff der „Benutzung“ geht. Denkbar wäre es theoretisch auch, Internetplattformen, Cloud-Umgebungen oder ähnliches mit einzubeziehen, wenn die Zielperson, diese mit-„benutzt“. Damit könnten künftig zum Beispiel Internetplattformen „gehackt“ werden, die Kontakt mit sog. Whistleblowern haben.

> ***Beispiel:*** *Die Studentin Juliane B engagiert sich für Freiheitsrechte. Deshalb hat sie eine Plattform aufgebaut, die es Whistleblowern in aller Welt ermöglicht, dort Informationen über Menschenrechtsverletzungen aus ihrem Heimatland zu veröffentlichen. So veröffentlicht auch ein ihr nicht bekannter Nutzer eine vertrauliche Information aus der Bundesrepublik mit Hilfe ihrer Plattform. Davon erfahren die Ermittlungsbehörden und setzen sich mit Juliane B in Verbindung. Diese löscht daraufhin die Daten sofort, da sie Angst hat, eventuell rechtswidrige Aktivitäten zu unterstützen, was sie aber keinesfalls will. Die Ermittler vermuten nun, dass der unbekannte Nutzer die Plattform erneut nutzen wird und setzen ohne Wissen von Juliane B einen Trojaner in dem System ein, mit dem alle Nutzer identifiziert werden können.*

3. Beweiswert und Infiltration

Der Entwurf widmet sich nicht der Frage, welcher Beweiswert den erlangten Daten innewohnt. Ebenfalls sagt er nichts dazu, wie sich die durch die Strafverfolgungsbe-

hörden vorgenommenen Manipulationen an Daten und Geräten im weiteren Verfahren auswirken.

Die strafprozessualen Maßnahmen zur Quellen-TKÜ und zur Online-Durchsuchung unterscheiden sich von den bislang vom Bundesverfassungsgericht beurteilten gefahrenabwehrrechtlichen Maßnahmen. Hier im Strafverfahren geht es darum, Beweise zu erlangen, mit denen die Schuld oder Unschuld einzelner Personen im Strafverfahren bewiesen oder entkräftet werden kann. In der Gefahrenabwehr dagegen geht es darum, eine Gefahr zu beseitigen bzw. ein Rechtsgut zu beschützen und zu bewahren. Die Frage der Schuld oder Unschuld einzelner Personen ist dort zweitrangig.

Die geplanten Maßnahmen sind mit herkömmlichen Durchsuchungsmaßnahmen nicht vergleichbar. Insbesondere muss die Schadsoftware auf dem Gerät der betroffenen Person eingebracht werden. Dies geschieht nach der Gesetzesbegründung „auf technischem Wege oder mittels kriminalistischer List“. Welche Manipulationen genau an dem Gerät vorgenommen oder nicht vorgenommen werden dürfen wird nicht deutlich. Geht es aber um gerichtsfeste Beweise, stellt sich die Frage, wie sich der manipulative Eingriff in informationstechnische Systeme auswirkt.

Die strafprozessualen Vorschriften der Durchsuchung und Beschlagnahme gestatten insoweit nur die Durchsicht, ggf. die Sicherung von Schriftstücken und elektronischen Speichermedien (§ 110 StPO) bzw. die Verwendung als Beweismittel (§ 94 Abs. 1 StPO). Die Regelung des § 110 StPO enthält zudem Restriktionen über den Kreis der zur Durchsicht befugten Beamten. Die Manipulation am Gerät ist daher von den Vorschriften über die Beschlagnahme und Durchsuchung nicht gedeckt. Die heimliche Manipulation würde darüber hinaus mittelbar gegen den Grundsatz der Offenheit nach Art. 13 Abs. 2 GG verstoßen, sofern sie in den Räumen der betroffenen Person geschieht. § 110 Abs. 2 Satz 2 StPO zeigt, dass auch die Regelungen zur Durchsicht beschlagnahmter Papiere bzw. Speichermedien vom Grundsatz der Offenheit geprägt sind.

Nach allgemeinen forensischen Grundsätzen ist jede Manipulation des betroffenen Gerätes zu unterlassen. Es wäre nach bisherigen Standards ein polizeilicher Kunstfehler, ein beschlagnahmtes Gerät unmittelbar zu analysieren, statt nur ein Image der sichergestellten Datenträger auszuwerten.

Daran zeigt sich, mit welcher Grundsätzlichkeit hier in das System der strafprozessualen Ermittlungsbefugnisse eingegriffen wird. Dem manipulativen Eingriff in informationstechnische Systeme ist das Risiko von Fehlern immanent. Es handelt sich nicht um Software, die in einer gesicherten Rechnerumgebung der Polizeibehörde betrieben wird, sondern um eine Software, die technisch sonst nur bei Schadprogrammen zum Einsatz kommt.

Das mag zu rechtfertigen sein, wenn es um die Abwehr einer Lebens- oder Leibesgefahr geht. Hier geht es aber nicht um Gefahrenabwehr. Der Einsatz der Online-Durchsuchung im Strafverfahren ist nicht zu rechtfertigen, solange in einem Strafverfahren das Risiko fehlerhafter Beweise nicht beherrschbar ist.

Dem wichtigen Anliegen einer effektiven Strafverfolgung ist nicht gedient, wenn erlangte Informationen als Verstoß gegen Verfassungsrecht nicht verwertet werden können. Daher sollte ein entsprechender Gesetzesbeschluss nicht übereilt, sondern zunächst sorgfältig diskutiert werden.

4. Kernbereich privater Lebensgestaltung

Die geplanten Regelungen sind das eine. Die andere Frage ist aber, wie dies alles technisch umgesetzt werden soll.

In der Vergangenheit haben schon technische Schwierigkeiten bestanden, bereits erlangte kernbereichsrelevante Daten zu löschen (siehe meinen 24. Tätigkeitsbericht, Nr. 7.4.1). Erst recht dürfte technisch kaum umsetzbar sein, sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Während bei einer Quellen-TKÜ immerhin mit hohem Aufwand ein „Live-Mithören“ organisierbar ist, ist dies bei der Online-Durchsuchung nicht möglich. Es kann niemand „live“ mehrere Gigabyte Download „mithören“ oder „mitlesen“.

5. Statistische Erfassung

Bei der statistischen Erfassung nach § 101b fehlen:

- Dauer der jeweiligen Maßnahme
- Anzahl der "Zugriffe"
- Die Zahl der "nicht erfolgreichen Versuche" des Aufspielens (Abbrüche mit Grund)
- Anzahl der durch Nutzer / Beschuldigter etc. unterbrochenen Überwachungen
- Anzahl der erfassten nicht beschuldigten Personen (Drittbetroffene)
- Anzahl und Art der erfassten IT-Systeme dieser Personen (Systeme Drittbetroffener).

B. Gesetzentwurf BT-Drs. 18/11272

Der in BT-Drs. 18/11272 enthaltene Gesetzentwurf will Bewährungshelfern erweiterte Möglichkeiten geben, personenbezogene Daten an weitere Stellen zu übermitteln. Das stößt auf datenschutzrechtliche Bedenken. Dies gilt ebenso für die Aufhebung des Richtervorbehalts bei der Entnahme von Blutproben.

I. zu Art. 3 Nr. 4, 5

Forderungen für eine erweiterte Übermittlung von Daten der Bewährungshilfe werden bereits seit vielen Jahren erhoben (vgl. etwa Tätigkeitsbericht des Unabhängigen Landeszentrums für Datenschutz 2004, Nr. 4.2.1.). Das **Bundesministerium der Justiz** hat zutreffender Weise im Jahr 2011 ein derartiges Ansinnen des Bundesrates **abgelehnt**.

1. § 481 StPO-E (Art. 3 Nr. 4)

Eine Übermittlung an Polizeibehörden kommt in Betracht, wenn Gefahr im Verzug besteht. In einer derartigen Notsituation muss die Bewährungshelferin oder der Bewährungshelfer schon nach derzeitiger Rechtslage nicht erst die Führungsaufsichtsstelle informieren, sondern kann sich direkt an die Polizeibehörden wenden. In der Praxis ist jedoch zu befürchten, dass es zur „allgemeinen Gefahrenabwehr“ etwa zu Kontrollmitteilungen kommen könnte (vgl. o.g. Tätigkeitsbericht).

Derartige Kontrollmitteilungen o.ä. würden das austarierte System der Führungsaufsicht gefährden. Ebenso würde dies das Vertrauensverhältnis der Bewährungshelferin bzw. des Bewährungshelfers zu ihrem oder seinem Probanden oder der Probandin gefährden – und damit auch den Erfolg der Resozialisierung.

Soweit die Änderung in § 481 StPO-E auf eine konkrete Gefahr für hochrangige Rechtsgüter und die ansonsten nicht rechtzeitige Übermittlung an die Polizeibehörde abstellt, entspricht dies bei entsprechend restriktiver Auslegung hinsichtlich der Übermittlungsvoraussetzungen noch der geltenden Rechtslage. Gefordert ist der Sache nach „Gefahr im Verzug“, was in der Gesetzesbegründung hätte stärker herausgestellt werden können.

Der Inhalt der übermittelten Informationen ist nicht näher begrenzt. Durch den Verweis auf § 481 Abs. 1 Satz 2 StPO-E können die Bewährungshelfer allgemein personenbezogene Daten übermitteln und sogar Akteneinsicht gewähren. Der mit dem Entwurf eingefügte Satz spricht von „Mitteilungen nach Satz 2“. Es ist unklar, aus welchen Gründen zur Abwehr einer konkreten Gefahr Akteneinsicht gewährt werden sollte.

2. § 487 StPO-E (Artikel 3 Nr. 5 b).

Die vorgesehene Erweiterung ist abzulehnen. Sie wird damit begründet, möglicherweise eine doppelte Datenerhebung zu vermeiden oder jedenfalls zu verringern. Zudem solle der Weg über das Gericht und damit die dort zusätzliche Speicherung vermieden werden. Beides überzeugt als Begründung jedoch nicht.

Denn auf der Gegenseite steht die Bedeutung des Vertrauensverhältnisses zwischen den Bewährungshelfern und ihren Probanden. Dies kann verloren gehen, wenn der Proband bzw. die Probandin jederzeit damit rechnen muss, dass die Bewährungshilfe seine bzw. ihre Angaben zu einem späteren Zeitpunkt ohne eine gerichtliche Aufsicht an eine Haftanstalt weitergibt. Die Aufsicht über diesen Datenfluss obliegt bislang den Gerichten.

II. Zu Artikel 3 Nr. 1

Die Aufhebung des Richtervorbehalts bei der Entnahme von Blutproben ist datenschutzrechtlich problematisch. Die entnommenen Proben erlauben Aussagen über den Gesundheitszustand des Betroffenen (sensitive Daten).

Begründet wird die Änderung mit zunehmenden Anwendungsschwierigkeiten in der Justiz. Eine vertiefte richterliche Prüfung könne aufgrund der regelmäßig hohen Eilbedürftigkeit und „anhand der von der Polizei vor Ort regelmäßig nur telefonisch mitgeteilten Informationen“ kaum erfolgen.

Mit derselben Begründung ließen sich auch alle anderen in der Strafprozessordnung vorgesehenen Richtervorbehalte abschaffen. Wenn die Justiz nicht hinreichend ausgestattet ist, ihren Aufgaben nachzukommen, darf dies nicht dazu führen, Verfahrenssicherungen abzuschaffen. Die Begründung weist selbst darauf hin, dass die Gerichte offenbar deshalb in Schwierigkeiten geraten, weil sich die Rechtsprechung in den letzten Jahren geändert habe. Bei dieser Rechtsprechung handelt es sich maßgeblich um die des Bundesverfassungsgerichts, die einem Leerlaufen des Richtervorbehalts entgegenwirken wollte (vgl. BVerfG, Beschluss vom 11. 6. 2010 - 2 BvR 1046/08, NZV 2010, 628).

Die dargelegten Gründe allein tragen die Neuregelung nicht.

gez. Andrea Voßhoff