BUNDESKANZLERAMT VERFASSUNGSDIENST

GZ ● BKA-602.001/0002-V/5/2016
ABTEILUNGSMAIL ● SLV@BKA.GV.AT
BEARBEITERINNEN ● DR. MELINA OSWALD, LL.M.
MAG. STEFANIE DÖRNHÖFER, LL.M. (DATENSCHUTZ)
PERS. E-MAIL ● MELINA.OSWALD@BKA.GV.AT
STEFANIE.DOERNHOEFER@BKA.GV.AT
TELEFON ● +43 1 53115-202372
IHR ZEICHEN ●BMJ-S430.010/0001-IV 3/2016

An das
Bundesministerium für
Justiz

Museumstraße 7
1070 Wien

Antwort bitte unter Anführung der GZ an die Abteilungsmail

Entwurf eines Bundesgesetzes mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden;
Begutachtung; Stellungnahme

Zu dem mit der do. oz. Note übermittelten Gesetzesentwurf nimmt das Bundeskanzleramt-Verfassungsdienst wie folgt Stellung:

I. Allgemeines

Es wird angeregt, künftig bereits in das Aussendungsschreiben einen Hinweis aufzunehmen, ob bzw. inwieweit das Vorhaben dem Konsultationsmechanismus (vgl. die Vereinbarung zwischen dem Bund, den Ländern und den Gemeinden über einen Konsultationsmechanismus und einen künftigen Stabilitätspakt der Gebietskörperschaften, BGBl. I Nr. 35/1999) unterliegt. Bejahendenfalls ist gemäß Art. 1 Abs. 4 der erwähnten Vereinbarung eine Frist zur Stellungnahme von mindestens vier Wochen vorzusehen.

Es wird darauf hingewiesen, dass die Übereinstimmung des im Entwurf vorliegenden Bundesgesetzes mit dem Recht der Europäischen Union vornehmlich vom do. Bundesministerium zu beurteilen ist.

II. Inhaltliche Bemerkungen

Zu Art. 1 (Änderung der Strafprozessordnung 1975):

Zu Z 8 (§ 137 Abs. 3):

Im Hinblick auf die Anforderungen, die sich nach dem jüngsten Urteil der Großen Kammer des EGMR, 4.12.2015, Zakharov v Russia, Appl. No. 47.143/06 = NLMR 6/2015, 509, aus Art. 8 EMRK in Bezug auf gesetzliche Regelungen zur Telefonüberwachung ergeben, sollte die Anordnung eines höchstzulässigen Zeitraums, für den die Überwachungsmaßnahme angeordnet werden darf, überprüft werden.

Zu Z 10 (§ 138 Abs. 5):

Nach den Erläuterungen sollen Rechtsmittelbelehrungen auch einen Hinweis auf die Möglichkeit der Geltendmachung von Ersatzansprüchen nach § 148 StPO enthalten. Dies findet im vorgeschlagenen Gesetzestext keinen Niederschlag.

Zu Z 11 (§ 140 Abs. 1 Z 4):

Nach § 140 Abs. 1 Z 4 in der geltenden Fassung dürfen Ergebnisse u.a. in den Fällen der § 135 Abs. 2 Z 2 bis 4 nur zum Nachweis einer vorsätzlich begangenen strafbaren Handlung, derentwegen die Ermittlungsmaßnahme angeordnet wurde oder hätte angeordnet werden können, verwendet werden. Nach der vorgeschlagenen Änderung entfällt der Verweis auf § 135 Abs. 1 Z 4 (Auskunft über Daten einer Nachrichtenübermittlung, wenn zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der bestimmter Straftaten dringend verdächtig ist, ermittelt werden kann). Es stellt sich die Frage, warum die Einschränkung der Zulässigkeit der Verwendung von Beweismitteln für diesen Fall entfällt. Dies sollte in den Erläuterungen ausgeführt werden.

III. Datenschutzrechtliche Bemerkungen

Zu Art. 1(Änderung der Strafprozessordnung 1975):

Vorbemerkung:

Mit der geplanten Ermittlungsmaßnahme wird in die Grundrechte der Betroffenen auf Achtung des Privatlebens und auf Datenschutz (§ 1 DSG 2000, Art. 8 EMRK, Art. 7 und 8 GRC) sowie in das Fernmeldegeheimnis (Art. 10a StGG) eingegriffen. Im Lichte der besonderen Eingriffsintensität dieser Maßnahme und im Hinblick auf die Verpflichtungen, die sich nach der Rechtsprechung des EuGH und des Verfassungsgerichtshofes aus dem Grundrecht auf Datenschutz ergeben, wäre es zur Wahrung der Verhältnismäßigkeit der vorgeschlagenen Maßnahme insbesondere erforderlich, Umfang, Art und Form der Ermittlungsmaßnahme unmittelbar im Gesetzestext klarer festzulegen und angemessene Vorkehrungen zum Schutz personenbezogener Daten zu treffen.

Zu Z 4 (§ 134 Z 4a):

Aus dem Entwurfstext geht der Umfang der geplanten Maßnahme nicht klar hervor:

1. Während die Definition des § 134 Z 4a dem Wortlaut nach auf eine reine Echtzeitüberwachung (von Nachrichten und sonstigen Daten, die im Wege eines Computersystems „übermittelt und empfangen“ werden) abstellt, deuten andere Bestimmungen des Entwurfes darauf hin, dass auch eine darüber hinausgehende Ermittlung von auf dem Computersystem vorhandenen Daten beabsichtigt ist (vgl. Pkt. 3 der Anmerkungen zu § 136a [Z 6 des Entwurfes]). Auch der Begriff der „sonstigen Daten“ erscheint zu unbestimmt und bedarf einer näheren Präzisierung (vgl. etwa § 136a Abs. 3 Z 1).

2. Darüber hinaus ist unklar, ob der Begriff der „Nachrichtenübermittlung“ lediglich Kommunikationsvorgänge zwischen (zumindest) zwei Kommunikationsteilnehmern erfasst oder auch andere Arten der Übertragung von Daten vom überwachten Computersystem aus erfasst werden sollen (etwa das bloße Erstellen und Speichern [ohne späteres Absenden] einer Nachricht oder eines Dokuments auf einem externen Server [Cloud] oder auf einer lokalen Festplatte im Heimnetzwerk). Auf technischer Ebene findet auch in diesen Fällen eine Übertragung von Daten zwischen unterschiedlichen Computersystemen statt, ohne dass von vornherein

erkennbar sein muss, ob es überhaupt einen vom Absender unterschiedlichen Empfänger geben soll.

Gegenüber der klassischen Nachrichtenüberwachung gemäß § 134 Z 3 ergibt sich hier eine zusätzliche Abgrenzungsproblematik, weil der Gegenstand der Überwachung nicht ein bestimmter Anschluss (Kommunikationsweg) ist, sondern ein Computersystem, das nicht nur zur Kommunikation nach außen genutzt werden kann, sondern auch für weitere (lokale) Zwecke (zB Sicherung von Daten in der Cloud oder im Heimnetzwerk, Besuch von Websites, Herunterladen von Musik, Updates usw.).

Die Definition der „Überwachung von Nachrichten“ (§ 134 Z 3) verweist auf § 92 Abs. 3 Z 7 des Telekommunikationsgesetzes 2003 – TKG 2003, demzufolge eine „Nachricht“ „jede Information [ist], die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird“. Schon der Begriff „Nachricht“ impliziert, dass es sich um eine Form der Kommunikation zwischen mehreren Beteiligten, nämlich einem Absender und (mindestens) einem vom Absender verschiedenen Empfänger, handelt. Wenngleich § 134 Z 4a selbst keinen solchen expliziten Verweis auf § 92 Abs. 3 Z 7 TKG 2003 enthält, ist aus systematischen Gründen und mangels anderslautender Anordnung des Gesetzgebers davon auszugehen, dass der Begriff der „Nachricht“ in § 134 Z 4a jenem des § 134 Z 3 entspricht; die Verwendung desselben Begriffs in diesen nahe verwandten Kontexten mit unterschiedlichen Bedeutungsinhalt wäre im Sinne der Rechtsklarheit jedenfalls abzulehnen.

Den Erläuterungen lässt sich hingegen implizit entnehmen, dass die geplante Ermittlungsmaßnahme neben solchen Kommunikationsvorgängen im herkömmlichen Sinn auch andere Arten der Übertragung von Daten erfassen soll: In den Erläuterungen zu § 134 Z 4a und 5 (Z 4 und 5 des Entwurfes) werden insbesondere das „Hoch- und Herunterladen von Dokumenten in eine bzw. aus einer Cloud“, im Allgemeinen Teil der Erläuterungen explizit die Dienste „iCloud“ und „Dropbox“ genannt. Die genannten Beispiele sind jeweils Fälle, in denen der „Kommunikationsvorgang“ in zwei vollkommen unabhängige Vorgänge auseinanderfällt: Einerseits die Übertragung von Daten aus dem Computersystem in eine Cloud; andererseits der (spätere) Abruf durch den Absender selbst oder eine von ihm verschiedene Person. Bei derartigen „Übermittlungen“ von Daten (wie der

Ablage in einer Cloud) ist vorab nicht erkennbar, ob diese (im Sinne des Begriffs „Kommunikation“) für einen anderen Empfänger bestimmt sind.

Es sollte klargestellt werden, dass nur Nachrichten zwischen mehreren Kommunikationsteilnehmern Gegenstand der Überwachung sind.

Zu Z 6 (§ 136a):

1. Es ist unklar, ob die Installation des Überwachungsprogramms ausschließlich lokal (dh. durch physischen Zugriff auf das Computersystem) oder auch mittels „Fernzugriff“ („remote“) erfolgen kann. Den Erläuterungen zufolge soll letztere Variante unzulässig sein; diese Einschränkung ist aus dem Gesetzestext jedoch nicht ableitbar und wird auch in den Erläuterungen teilweise relativiert (so soll etwa eine Veränderung des Funktionszeitraumes über Fernzugriff möglich sein; siehe dazu Pkt. 2.). Eine Installation mittels Fernzugriff wäre mit erheblichen zusätzlichen Unsicherheitsfaktoren verbunden; insbesondere ist fraglich, ob auf diese Weise sichergestellt werden kann, dass es sich um die richtige Person bzw. das richtige Computersystem handelt. Die Einschränkung, dass das Überwachungsprogramm nur im Rahmen eines physischen Zugriffs auf das zu überwachende Computersystem installiert werden darf, müsste daher jedenfalls im Gesetzestext verankert werden.

2. Unklar ist generell, ob die Überwachung im Rahmen einer „one-way“-Verbindung erfolgen soll (dh. das Überwachungsprogramm übermittelt die ermittelten Daten an die überwachende Behörde, ein Zugriff in die andere Richtung ist nicht möglich) oder ob eine „two-way“-Verbindung eingerichtet werden soll (dh. die überwachende Behörde kann über das Überwachungsprogramm auf das Computersystem zugreifen, zB um Daten aus Adressbüchern zu ermitteln). Den Erläuterungen zu den §§ 144 Abs. 3, 145 Abs. 3 und 4 und 147 Abs. 1 bis 3a (Z 12 bis 16 des Entwurfes) zufolge sollen Veränderungen des Funktionszeitraumes des Überwachungsprogramms auch „ohne neuen direkten Zugriff“ (worunter wohl nur ein Fernzugriff verstanden werden kann) möglich sein, was jedenfalls eine „two-way“-Verbindung erfordern würde.

Im Gesetzestext wäre daher einerseits klar und abschließend festzulegen, ob und in welchem Umfang die Überwachung Zugriffsmöglichkeiten auf das Computersystem umfasst, andererseits müssten entsprechende Datensicherheitsvorkehrungen verankert werden.

3. Gemäß § 136a Abs. 3 Z 1 darf das Überwachungsprogramm nicht nur im Wege des Computersystems übermittelte und empfangene Daten erfassen, sondern auch „jene Daten, die Rückschlüsse auf die Namen oder die sonstigen Identifizierungsmerkmale der Inhaber oder Verfügungsberechtigten“ erlauben; den Erläuterungen zufolge soll dadurch ein Zugriff auf Adressbücher und Kontaktverzeichnisse (Skype, WhatsApp usw.) zur Identifizierung des Benutzers ermöglicht werden. Dies geht jedoch über eine Echtzeitüberwachung von Nachrichten (vgl. § 134 Z 4a: „Daten, die … übermittelt und empfangen werden“; siehe auch Pkt. 1. der Anmerkungen zu dieser Bestimmung) klar hinaus, zumal offenbar nicht nur die „äußeren Verbindungsdaten“ tatsächlich stattfindender Kommunikationsvorgänge erfasst werden sollen, sondern auch Daten, die (unabhängig von einer konkreten Nachrichtenübermittlung) auf dem Computersystem gespeichert sind (in den Erläuterungen wird explizit auf „in Adressbüchern und Kontaktverzeichnissen der jeweiligen Anwendung gespeichert[e]“ Daten Bezug genommen). Es sollte daher eine eindeutige Regelung getroffen werden.

Fraglich ist, wie „Daten, die Rückschlüsse auf die Namen oder die sonstigen Identifizierungsmerkmale der Inhaber oder Verfügungsberechtigten der an der Nachrichtenübermittlung beteiligten Computersysteme erlauben“ von anderen auf dem Computersystem gespeicherten Daten unterschieden werden können und ob nicht eine Durchsuchung des gesamten Computersystems erforderlich wäre, um festzustellen, ob bzw. wo derartige Daten gespeichert sind. Letzteres dürfte zudem nicht von § 136a Abs. 3 Z 1 gedeckt sein, demzufolge „gewährleistet“ sein muss, dass das Überwachungsprogramm „ausschließlich“ die in dieser Bestimmung genannten Daten erfasst.

4. Im Hinblick auf § 136a Abs. 3 Z 2 stellt sich die Frage, ob die unwiderrufliche Funktionsunfähigkeit oder vollständige Entfernung des Überwachungsprogramms gewährleistet werden kann (siehe dazu die Anmerkungen zu § 145 Abs. 4 [Z 13 des Entwurfes]).

Näher erläutert werden müsste in diesem Zusammenhang auch, was unter einer „dauerhaften Schädigung oder Beeinträchtigung des Computersystems oder der in ihm gespeicherten Daten“ zu verstehen ist.

Zu Z 8 (§ 137 Abs. 3 erster Satz):

Bei der Möglichkeit, die Ermittlungsmaßnahme auch für einen vergangenen Zeitraum anzuordnen, handelt es sich offenbar um einen Fall der „Online-Durchsuchung“ mit dem Ziel, gespeicherte Daten zu ermitteln, der von der Definition des § 134 Z 4a nicht erfasst ist (siehe dazu Pkt. 3. der Anmerkungen zu § 136a [Z 6 des Entwurfes]).

Zu Z 13 (§ 145 Abs. 4):

1. § 145 Abs. 4 sieht eine Protokollierung mit dem Ziel einer lückenlosen Nachvollziehbarkeit jedes Zugangs zum Computersystem und jeder nachträglichen Veränderung daran vor; zu diesem Zweck sind „die erforderlichen Sicherungskopien herzustellen“. Den Erläuterungen zu § 145 Abs. 4 ist zu entnehmen, dass die Protokollierungspflicht sich ausschließlich auf den behördlichen Zugang und Veränderungen am Überwachungsprogramm bezieht; diese Einschränkungen können jedoch dem Gesetzestext nicht entnommen werden:

§ 145 Abs. 4 lässt offen, ob nur der überwachenden Behörde zuzurechnende Zugriffe (vgl. Pkt. 2 der Anmerkungen zu § 136a) und Veränderungen erfasst werden sollen oder auch der Zugang (zB lokaler Login, externer Zugang, Zugriff im Netzwerk usw.) und Veränderungen (zB lokale Erstellung eines Dokuments, Installation eines Programms durch den Benutzer) durch andere Personen. Zudem bezieht sich der Begriff „Veränderungen“ dem Wortlaut des § 145 Abs. 4 nach nicht auf das Überwachungsprogramm, sondern auf das Computersystem (insofern widersprechen somit die Erläuterungen dem Gesetzestext).

Im Hinblick darauf, dass jeglicher Vorgang auf einem Computersystem dieses in irgendeiner Weise „verändert“ (indem Daten abgerufen, gespeichert, verknüpft usw. werden), würde auch dies zu einer massiven Ausweitung des Überwachungsgegenstandes führen. Auch die Verpflichtung zur Herstellung von „Sicherungskopien“ würde sich somit auf das gesamte Computersystem beziehen, was zusätzlich zur Überwachungsmaßnahme gemäß § 134 Z 4a einen eigenständigen, schwerwiegenden Grundrechtseingriff bewirken würde.

Vor diesem Hintergrund müssten daher im Gesetzestext Einschränkungen verankert werden, durch die sichergestellt wird, dass es im Rahmen der Protokollierung nicht zu einer faktischen Ausdehnung des Überwachungsgegenstandes kommt.

2. Für die Verhältnismäßigkeit der Ermittlungsmaßnahme wäre es jedenfalls erforderlich, dass das Überwachungsprogramm nach Beendigung der Maßnahme vollständig und unwiderruflich entfernt bzw. deaktiviert wird. Dabei ist auch zu beachten, dass das Überwachungsprogramm direkt am Gerät installiert wird, sodass bei einer Weitergabe (Verkauf) des Gerätes an unbeteiligte Dritte auch diese mit den Risiken eines kompromittierten Computersystems belastet würden.

Zu Z 17 (§ 148 erster Satz):

Im Hinblick auf die verschuldensunabhängige Haftung des Bundes für vermögensrechtliche Nachteile, die durch die Durchführung einer Überwachung gemäß § 136a entstanden sind, erscheint eine Eingrenzung entstandener Schäden durch die Nichtgeheimhaltung bzw. unzulässige Ermittlung von Daten schwierig. Schäden können insbesondere auch dadurch entstehen, dass sich Dritte des Überwachungssystems bedienen, um selbst missbräuchlich Daten zu verwenden (zB Abfangen von TANs beim E-Banking). Problematisch erscheint in diesem Zusammenhang generell, dass durch das Kompromittieren des Computersystems – insbesondere auch durch die Möglichkeit eines allfälligen Fernzugriffs und damit verbundene Manipulationsmöglichkeiten – die Vertraulichkeit und Authentizität von als sicher geltenden Verfahren im Zusammenhang mit der Übermittlung von Daten (verschlüsselte Verbindung, elektronische Signatur) beeinträchtigt wird.

IV. Legistische und sprachliche Bemerkungen

Zu Art. 1 (Änderung der Strafprozessordnung 1975):

Zu Z 2 (Inhaltsverzeichnis):

Der derzeitige Eintrag zum 5. Abschnitt des 8. Hauptstücks lautet: „Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Auskunft über Vorratsdaten sowie Überwachung von Nachrichten und von Personen“.

Zu Z 11 (§ 140 Abs. 1 Z 4):

Die Novellierungsanordnung sollte lauten wie folgt: „§ 140 Abs. 1 Z 4 lautet:“.

Zu Z 13 (§ 145 Abs. 4):

Die Novellierungsanordnung sollte lauten wie folgt: „Dem § 145 wird folgender Abs. 4 angefügt:“

Anstatt auf § 136a Abs. 3 sollte präziser auf § 136a Abs. 3 Z 2 verwiesen werden.

Zu Z 16 (§ 147 Abs. 3a):

Im letzten Satz ist vor „Anordnung“ und „gerichtliche Bewilligung“ jeweils der bestimmte Artikel „die“ einzufügen.

Zu Z 18 (§ 514 Abs. 32):

Die Novellierungsanordnung sollte wie folgt lauten: „Dem § 514 wird folgender Abs. 32 angefügt:“.

Zwischen „136a“ und „137“ hat das „und“ zu entfallen.

Es ist auch das Inkrafttreten des Eintrags zum 5. Abschnitt des 8. Hauptstücks im Inhaltsverzeichnis und der Überschrift des 5. Abschnitts des 8. Hauptstücks anzuordnen.

Zu Art. 2 (Änderung des Staatsanwaltschaftsgesetzes):

Zu Z 1 und Z 2 (§ 10a Abs. 1 und 2):

Die Schreibweise der Anführungszeichen ist zu überprüfen („ anstatt ,„).

Zu Z 3 (§ 42 Abs. 20):

Die Novellierungsanordnung sollte wie folgt lauten: „Dem § 42 wird folgender Abs. 20 angefügt:“.

V. Zu den Materialien

Zum Allgemeinen Teil der Erläuterungen:

Im Allgemeinen Teil der Erläuterungen ist anzugeben, worauf sich die Zuständigkeit des Bundes zur Erlassung der vorgeschlagenen Neuregelungen gründet (Punkt 94 der Legistischen Richtlinien 1979).

Auf S. 4 von 7 sollte die Formatierung des Textes überprüft werden.

Zur Textgegenüberstellung:

Auf das Rundschreiben des Bundeskanzleramtes-Verfassungsdienst vom 10. Dezember 2015, GZ 600.824/0001-V/2/2015[1] (betreffend Legistische Richtlinien; Gestaltung von Textgegenüberstellungen) wird hingewiesen, insbesondere auf folgende Regeln und Hinweise:

– Die zwischen den Fassungen bestehenden Textunterschiede sind durch Kursivschreibung hervorzuheben, dergestalt dass in der Spalte „Geltende Fassung“ entfallende (auch: durch andere ersetzte) Passagen, in der Spalte „Vorgeschlagene Fassung:“ die neuen Passagen hervorgehoben werden.
  Die Kursivschreibung kann, *wenn und soweit* dies dem Verständnis und der Lesbarkeit dient, mehr als die exakten Textunterschiede umfassen; d.h. großflächige Kursivschreibung gleichbleibender Passagen ist zu vermeiden.

Es fehlt die Textgegenüberstellung zu Art. 1 Z 1 und 2.

Diese Stellungnahme wird im Sinne der Entschließung des Nationalrates vom 6. Juli 1961 auch dem Präsidium des Nationalrates zur Kenntnis gebracht.

12. Mai 2016
Für den Bundesminister für
Kunst und Kultur, Verfassung und Medien:
HESSE

Elektronisch gefertigt

[1] https://www.ag.bka.gv.at/at.gv.bka.wiki-bka/index.php/Datei:BKA-600.824_0001-V_2_2015_Legistische_Richtlinien;_Gestaltung_von_Textgegen%C3%BCberstellungen;_Rundschreiben_des_BKA-VD.docx

Unterzeichner	serialNumber=1026761,CN=Bundeskanzleramt,C=AT
Datum/Zeit	2016-05-12T12:15:20+02:00
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bka.gv.at/verifizierung
Hinweis	Dieses Dokument wurde amtssigniert.