REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817. 455/0002-DSR/2016
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für Justiz

Per Mail:
team.s@bmj.gv.at

Betrifft: Entwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden
Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner **229. Sitzung am 29. April 2016 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Allgemeines

Laut den Erläuterungen ergibt sich aus der Sicht des Bundesministeriums für Justiz Folgendes:

Der vorliegende Entwurf schlägt vor, die **Anordnung der Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, als neue Ermittlungsmaßnahme für den Bereich schwerster Kriminalität (organisierte Kriminalität und Terrorismus) in die StPO einzuführen.**

Mit gemeinsamem Vortrag an den Ministerrat vom 17. Oktober 2007 zum Thema „Erweiterung des Instrumentariums zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen („Online-Durchsuchung“)“ kündigten die damalige Bundesministerin für Justiz Dr. Maria Berger und der damalige Bundesminister für Inneres Günther Platter die Einsetzung einer Arbeitsgruppe mit dem Ziel der Klärung der technischen Voraussetzungen und der Möglichkeiten der Steuerung des Einsatzes der sogenannten „Online-Durchsuchung“ unter Berücksichtigung der

Erfahrungen mit solchen Ermittlungsmaßnahmen in anderen Staaten samt der Klärung der rechtlichen Fragen unter besonderer Berücksichtigung datenschutzrechtlicher, rechtsvergleichender und europarechtlicher Aspekte an.
Gegenstand des Ministerratsvortrages war die Durchführung einer „Online-Durchsuchung“. Darunter wurde der Einsatz von Programmen verstanden, die unbemerkt auf einem Computer installiert werden und es ermöglichen, den Inhalt gespeicherter Daten auszulesen, den E-Mail-Verkehr zu überwachen oder das Aufsuchen bestimmter Internetseiten zu ermitteln, ohne dass es der Inhaber merkt.
Dieser interdisziplinären Arbeitsgruppe unter Leitung von o. Univ. Prof. Dr. Bernd-Christian Funk gehörten Vertreterinnen und Vertreter des Bundesministeriums für Justiz, des Bundesministeriums für Inneres, des Bundesministeriums für Landesverteidigung, des Bundesministeriums für Verkehr, Innovation und Technologie, des Bundeskanzleramt-Verfassungsdienstes, der Bundesrechenzentrum GmbH, der ISPA Internet Service Providers Austria, der Höchstgerichte, der Rechtswissenschaft sowie Standesvertreter der Richter und Staatsanwälte und der Chief Information Officer – CIO des Bundes an.
Nach intensiver viermonatiger Tätigkeit legte die Arbeitsgruppe im März 2008 einen umfassenden Schlussbericht vor, in dem sie zum Ergebnis kam, dass eine derartige Ermittlungsmaßnahme nach geltendem Recht nicht zulässig ist. Gleichzeitig wurden Überlegungen vorgezeichnet, wie die gesetzliche Grundlage für eine solche Maßnahme und die Sicherungs- und Rechtsschutzmaßnahmen ausgestaltet sein sollten.
Der nunmehr vorgelegte Entwurf baut auf den rechtlichen Überlegungen auf, beschränkt sich im Gegensatz dazu allerdings auf eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden. Da er somit einen weitaus geringeren Anwendungsbereich umfasst, ist nicht die Gesamtheit der für eine Online-Durchsuchung als notwendig angedachten Sicherungsmaßnahmen erforderlich.
Seit Abschluss der Arbeitsgruppe ist es aufgrund des technischen Fortschrittes zu einer breiten Verwendung neuer Kommunikationsmittel und generell zu einer Änderung des Kommunikationsverhaltens gekommen. Vermehrt werden anstelle herkömmlicher Telefonie und Kurznachrichten internetbasierte Kommunikationsmöglichkeiten verwendet, die auch eine Verschlüsselung der übertragenen Daten ermöglichen (WhatsApp, Skype). Der Umstand, dass sich Täter

zunehmend bewusst dieser Kommunikationsmöglichkeiten bedienen, macht es aus Sicht des Bundesministeriums für Justiz notwendig, die Strafverfolgungsbehörden mit adäquaten Möglichkeiten auszustatten, um mit diesen technischen Entwicklungen zumindest annähernd Schritt zu halten. Eine Anpassung der Ermittlungsmethoden an die technischen Entwicklungen und das geänderte Kommunikationsverhalten erscheint auch deshalb indiziert, weil den verfügbaren Informationen zufolge die Kommunikation der Attentäter von Paris im November 2015 nicht auf dem Wege der Kommunikation über Kurznachrichten oder Sprachtelefonie, sondern vielmehr internetbasiert über Spielekonsolen erfolgte.

Zur Ermöglichung einer wirksamen Strafverfolgung unter größtmöglicher Wahrung der Grundrechte und der Verhältnismäßigkeit sei daher die Einführung einer neuen Ermittlungsmaßnahme zur Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, aus Sicht der Strafverfolgungsbehörden notwendig. Sie soll jedoch auf den Bereich schwerster Kriminalität (organisierte Kriminalität und Terrorismus) beschränkt bleiben.

Es wird daher im vorliegenden Entwurf nunmehr vorgeschlagen, die bereits vorhandenen Ermittlungsmaßnahmen um die Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, zu ergänzen und damit auch neue Formen der Kommunikation unter Verwendung von Verschlüsselungssoftware zu erfassen. Im Einzelfall sollen durch diese Maßnahme Kommunikationsinhalte auf dem von der Maßnahme betroffenen Gerät noch vor einer eventuellen Verschlüsselung bzw. nach einer allfälligen Entschlüsselung überwacht und die Kommunikationspartner der Person, gegen die sich die Überwachung richtet, und somit gegebenenfalls auch Mittäter identifiziert werden können. **Die Ermittlung von sonst auf dem Computersystem gespeicherten Daten ist – im Gegensetz zu dem von der oben erwähnten Arbeitsgruppe verfassten Schlussbericht des Jahres 2008 – ausdrücklich nicht erfasst.**

Der Entwurf nimmt auch Bezug auf die Kritik des VfGH in seinem Erkenntnis (27.6.2014, G 47/2012, G 59/2012, G 62/2012, G 70/2012, G 71/2012) über die Aufhebung der Regelungen über die Vorratsdatenspeicherung in TKG, SPG und StPO, wonach bei jenen Bestimmungen nicht sichergestellt worden sei, dass die Auskunft über Vorratsdaten nur im Fall eines Verdachts der Begehung schwerer Straftaten angewendet werden könne. Der Vorschlag sieht daher vor, dass die

Regelungen über die Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, **nur bei Vorliegen eines dringenden Verdachts der Begehung schwerster Straftaten zur Anwendung gelangen** (siehe im Folgenden). Aufgrund der Eingriffsintensität orientiert sich der Entwurf an den Voraussetzungen und Regelungen der optischen und akustischen Überwachung von Personen (sogenannter „Lauschangriff“). **Vorgeschlagen werden in den Erläuterungen folgende Voraussetzungen:**

– Gleicher Anwendungsbereich wie bei der optischen und akustischen Überwachung von Personen unter Verwendung technischer Mittel gemäß § 136 Abs. 1 Z 3 StPO, d.h.: Notwendigkeit zur Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder des Verbrechens der kriminellen Organisation oder der terroristischen Vereinigung (§§ 278a und 278b StGB) oder zur Aufklärung oder Verhinderung von im Rahmen einer solchen Organisation oder Vereinigung begangener oder geplanter strafbarer Handlungen oder zur ansonsten aussichtslosen oder wesentlich erschwerten Ermittlung des Aufenthalts des wegen einer solchen Straftat Beschuldigten. Zusätzlich muss die Person, gegen die sich die Überwachung richtet, des mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens nach § 278a oder § 278b StGB dringend verdächtig sein oder auf Grund bestimmter Tatsachen anzunehmen sein, dass ein Kontakt einer solcherart dringend verdächtigen Person mit der Person hergestellt werde, gegen die sich die Überwachung richtet;
– Anordnung der Staatsanwaltschaft, die vor ihrer Durchführung durch das Gericht zu genehmigen ist und der Kontrolle des Rechtsschutzbeauftragten unterliegt;
– besondere Anordnung der Staatsanwaltschaft für den Fall, dass ein Eindringen in eine Wohnung erforderlich ist, die im Einzelnen einer Genehmigung durch das Gericht bedarf;
– strenge Beachtung des Verhältnismäßigkeitsgrundsatzes;
– Kontrolle der Durchführung durch Rechtsschutzbeauftragten der Justiz;
– Verständigung sämtlicher Personen, deren Daten ermittelt wurden und umfängliche Beschwerdemöglichkeiten;
– strenge Vernichtungsregelungen von unzulässig ermittelten oder für die Untersuchung nicht bedeutsamen Daten sowie Beschränkung der Verwertbarkeit von Zufallsfunden;

– eine verschuldensunabhängige Haftung des Bundes für Schäden, die durch eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, verursacht wurde (§ 148 StPO);
– Aufnahme in den jährlichen Bericht über besondere Ermittlungsmaßnahmen, dem Nationalrat, Datenschutzrat und der Datenschutzbehörde vorzulegen ist.
Das Bundesministerium für Justiz berichtet dem Parlament jährlich über den Einsatz dieser Ermittlungsmaßnahme (vgl. Gesamtbericht über den Einsatz besonderer Ermittlungsmaßnahmen). Aus den bisherigen Berichten ergibt sich in einer Gesamtschau, dass die Maßnahme der optischen und/oder akustischen Überwachung nach § 136 Abs. 1 Z 2 und 3 StPO in der Praxis maßvoll eingesetzt wird. Im Jahr 2012 kam es in zwei Verfahren zu einer optischen und akustischen Überwachung nach § 136 Abs. 1 Z 3 StPO („großer Späh- und Lauschangriff“), im Jahr 2013 in insgesamt drei Verfahren. Der sog. „kleine Späh- und Lauschangriff“ nach § 136 Abs. 1 Z 2 StPO gelangte im Jahr 2012 in drei Verfahren, im Jahr 2013 in einem Verfahren und im Jahr 2014 in 6 Verfahren zur Anwendung. Es ist daher zu erwarten, dass auch die Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, ebenso maßvoll angewendet werden wird.

Allgemeines aus den Erläuterungen zum Vorschlag:

Nach den Erläuterungen soll die Überwachung von Nachrichten in §§ 134 Z 3, 135 Abs. 2 StPO geregelt werden. Sie umfasst das Ermitteln von Nachrichten, die über ein Kommunikationsnetz (§ 3 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) übermittelt werden und erfasst grundsätzlich auch internetbasierte Telekommunikation. Tatsächlich lässt sich aus Sicht des Bundesministeriums für Justiz eine Veränderung des Kommunikationsverhaltens erkennen, sodass sich laufend mehr Personen internetbasierter Dienste wie WhatsApp oder Skype anstelle der „klassischen“ Telefonie und des Short Messaging Service (SMS) bedienen, die (v.a. im Fall der Nutzung von WLAN) eine kostengünstige Alternative darstellen. Darüber hinaus werden Daten oftmals über Cloud-Speicher wie z. B. iCloud oder Dropbox ausgetauscht, ohne dass es zu einer „klassischen“ Nachrichtenübertragung kommt. Bei vielen internetbasierten Diensten besteht die Möglichkeit, die zu übertragenden Daten zu verschlüsseln. Im Fall der Verschlüsselung ist es anderen Personen nicht möglich, vom Inhalt der Kommunikation Kenntnis zu erlangen; dies habe insbesondere den Nachteil, dass

auch Strafverfolgungsbehörden mit den bestehenden gesetzlichen Möglichkeiten eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, nicht möglich ist. Auch eine Mitwirkung des Betreibers würde eine Überwachung nicht möglich machen, weil die Verschlüsselung unmittelbar zwischen den an der Kommunikation beteiligten Computersystemen erfolgt und in der Regel auch der jeweilige Betreiber nicht über den für eine Entschlüsselung erforderlichen Schlüssel verfügt. Der Umstand der lückenhaften Überwachungsmöglichkeiten werde daher zunehmend von Verdächtigen und Beschuldigten genützt, um gezielt einer Überwachung zu entgehen, wenn diese die Befürchtung haben, Subjekt einer Überwachung zu werden. Eine Überwachung dieser Kommunikationsformen sei derzeit lediglich möglich, wenn eine optische und akustische Überwachung im Rahmen der strengen Voraussetzungen der §§ 136 ff StPO angeordnet werden kann, was jedoch einen weitaus schwereren Grundrechtseingriff für den Überwachten mit sich brächte, weil davon nicht nur die im Wege des betreffenden Computersystems übermittelten Nachrichten überwacht wurden.

Internetbasierte Kommunikation werde oft zum Nachrichtenaustausch mit Personen im Ausland genutzt, was insbesondere in Ermittlungsverfahren wegen der (versuchten) Beteiligung an einer terroristischen Vereinigung nach § 278b Abs. 2 StGB und wegen Ausbildung für terroristische Zwecke nach § 278e StGB von großer ermittlungstechnischer Bedeutung ist, befinden sich doch die „Terrorcamps“ in den Kampfgebieten selbst (Syrien, Afghanistan, …) oder deren Nachbarstaaten. Die Sammlung von stichhaltigem Beweismaterial, das eine (geplante) Reise ins Ausland zur Beteiligung an einer terroristischen Vereinigung („foreign fighters“) und terroristischen Ausbildungen belegt, kann von den Strafverfolgungsbehörden derzeit nur schwer bewerkstelligt werden, weil die Durchführungen von Ermittlungen im Wege von Rechtshilfeersuchen, z. B. nach Syrien, nahezu unmöglich sei. Wie bei den jüngsten Anschlägen offenkundig wurde, werden diese Kommunikationswege aber auch zur Vorbereitung terroristischer Straftaten im europäischen Raum und zur Koordinierung von Tätergruppierungen verwendet.

Die Bedrohung durch terroristische Straftaten (§§ 278b bis 278f StGB) in Österreich spiegelt sich auch sehr deutlich in der Zahl der von der Staatsanwaltschaft eingeleiteten Ermittlungsverfahren wieder: während die Anzahl der Verfahren zuvor noch 75 (2012) bzw. 62 (2013) betrug, erhöhte sie sich im Jahr 2014 beinahe um das

Doppelte im Vergleich zum Vorjahr und lag bei 115. Im Jahr 2015 sind bei den Staatsanwaltschaften 200 Verfahren wegen Beteiligung an einer terroristischen Vereinigung nach § 278b StGB angefallen, 49 Anklagen wegen § 278b StGB wurden eingebracht. Bis März 2016 sind bereits 30 Verfahren angefallen, 8 Anklagen wurden eingebracht; es ist daher auch in diesem Jahr mit einem massiven Anstieg der Verfahren wegen terroristischer Straftaten zu rechnen.

2) Datenschutzrechtlich relevante Bestimmungen:

Vorbemerkung:

In den Erläuterungen zu diesem Gesetzesvorschlag verweist das Bundesministerium für Justiz auf die deutsche Rechtslage nach dem BKA-Gesetz. Der Datenschutzrat verweist auf die jüngst ergangene Entscheidung des deutschen Bundesverfassungsgerichts (AZ. 1 BvR 966/09 und BvR 11400/09), mit der dieser Teile des BKA-Gesetzes für verfassungswidrig erklärt hat. Dabei wurden verschiedene Ermittlungsmaßnahmen überprüft, darunter auch der Zugriff auf informationstechnische Systeme (§ 20k BKAG). Zu prüfen ist aus Sicht des Datenschutzrates durch das Bundesministerium für Justiz, ob die durch den vorliegenden Gesetzesentwurf vorgesehene Grundrechtseingriffe aufgrund dieser deutschen höchstrichterlichen Entscheidung neu zu bewerten sind.

Weiters verweist der Datenschutzrat auf die heftige Diskussion in Deutschland über den Einsatz der staatlichen Spähsoftware „Bundestrojaner“, da dessen technische Fähigkeiten von Experten als begrenzt angesehen werden. („Quellen-Telekommunikationsüberwachung [TKÜ“]).

Damit stellt sich auch für Österreich die Frage, wie eine gesetzeskonforme Funktionalität des Überwachungsprogramms technisch sichergestellt werden kann (z.B. unwiderrufliche Deaktivierung des Überwachungsprogrammes).

Mit der geplanten Ermittlungsmaßnahme wird nach Ansicht des Datenschutzrates **erheblich** 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 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**.

Der Datenschutzrat weist grundsätzlich darauf hin, dass bei der technischen Umsetzung der Software die rechtlichen Vorgaben dieser Novelle und des DSG 2000 zu beachten sind.

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. Da bei derartigen „Übermittlungen“ von Daten (wie der Ablage in einer Cloud) vorab nicht erkennbar ist, ob diese (im Sinne des Begriffs „Kommunikation“) für einen anderen Empfänger bestimmt sind, würde dies mangels Abgrenzbarkeit bedeuten, dass **sämtlicher Datenverkehr, der über das überwachte Computersystem abgewickelt wird** (dh. auch der Besuch von Websites, die Speicherung von Daten in einer Cloud zu eigenen Zwecken, das Herunterladen

von Musik und Dokumenten usw.) **Gegenstand einer Überwachung gemäß § 134 Z 4a ist**.

Eine solche Ermittlungsmaßnahme würde **qualitativ erheblich über eine Nachrichtenüberwachung gemäß § 134 Z 3 hinausgehen** und der damit verbundene **Eingriff in das Grundrecht auf Datenschutz** wäre in der Folge **wesentlich schwerwiegender.** Auch vor dem Hintergrund, dass viele Computersysteme von mehreren Personen genutzt werden und folglich auch diese einer umfassenden Überwachung unterliegen würden, erscheint ein solcher Grundrechtseingriff unverhältnismäßig, weshalb klargestellt werden sollte, dass **nur Nachrichten zwischen mehreren Kommunikationsteilnehmern Gegenstand der Überwachung sind.**

Zu Z 6 (§ 136a):

Auch **Art und Form** der Ermittlungsmaßnahme erscheinen aus datenschutzrechtlicher Sicht unzureichend geregelt und sollten im Gesetzestext näher determiniert werden:

1. Insbesondere 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 ist; 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, muss 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. Diese Möglichkeit ist jedoch mit erheblich höheren Risiken eines Missbrauchs durch Dritte, einer Manipulation usw. verbunden.

Im Gesetzestext wäre daher einerseits klar und abschließend festzulegen, ob und in welchem Umfang die Überwachung **Zugriffsmöglichkeiten auf das Computersystem** umfasst, andererseits müssen 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 handelt sich somit – entgegen dem ausdrücklichen Wortlaut der Erläuterungen – um einen Fall der „**Online-Durchsuchung**“. Eine **gesetzliche Grundlage für solche Zugriffe ist nicht ersichtlich** (vgl. die Definition in § 134 Z 4a); zudem unterscheidet sich die Eingriffsqualität einer solchen „Online-Durchsuchung“ erheblich von einer reinen „Online-Nachrichtenüberwachung“, was im Rahmen der

Verhältnismäßigkeitsprüfung zu berücksichtigen ist und zudem **im Gesetz ausdrücklich verankert und klar geregelt werden** müsste.

Fraglich ist auch, 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 erscheint aus datenschutzrechtlicher Sicht jedenfalls unverhältnismäßig und 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 überhaupt 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: Unklar ist etwa, ob dies schon die Verwendung von Speicherplatz, Leistung und Bandbreite durch das Überwachungsprogramm umfasst. Darüber hinaus stellt sich die Frage, ob bereits der Verlust der Vertraulichkeit durch die Aushebelung einer Verschlüsselung eine Schädigung darstellt. Im Hinblick darauf, dass § 136a Abs. 3 Z 3 (mit geringfügig abweichendem Wortlaut) auch jegliche „Schädigung oder dauerhafte Beeinträchtigung dritter Computersysteme, die nicht der Überwachung unterliegen“, verbietet, ist davon auszugehen, dass diese Begriffe sehr weit zu verstehen sind.

5. Aus dem Blickwinkel der **Datensicherheit** ist zu prüfen, welche zusätzlichen **Risiken für das überwachte Computersystem** (sowie allfällige dritte Computersysteme) durch die Installation des Überwachungsprogramms geschaffen werden (zB Nutzung des Überwachungsprogramms durch Dritte, um selbst Zugriff auf das Computersystem zu erlangen; Abfangen der zwischen dem Überwachungsprogramm und der Behörde, die die Überwachung durchführt,

übertragenen Daten). Je nach Ausgestaltung des Überwachungssystems variiert das Risiko hinsichtlich missbräuchlicher Datenverwendungen durch Dritte, Manipulationsgefahr usw. erheblich. Im Hinblick auf die besondere Eingriffsintensität dieser Ermittlungsmaßnahme und die besonderen Risiken, die damit verbunden sind, müssen **angemessene Datensicherheitsmaßnahmen** verankert werden.

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 9 (§ 138 Abs. 1):

1. In den Erläuterungen wird im Hinblick auf die **Bezeichnung des zu überwachenden Computersystems** (§ 103 Abs. 1 Z 2) ausgeführt, dass die „häufig gar nicht mögliche Individualisierung des Computersystems“ nicht in jedem Fall notwendig sei und dieses durch die (Gattungs-)Bezeichnung des Computersystems, zB PC, Laptop, Smartphone des zu Überwachenden, zu bezeichnen sei. Knüpfe diese Ermittlungsmaßnahme an ein bereits bekanntes Identifizierungsmerkmal (zB Rufnummer eines Smartphones) an, so sei dieses anzuführen.

Diese in den Erläuterungen umschriebenen Vorgaben erscheinen unzureichend, zumal eine **eindeutige Bezeichnung** – etwa in einem Mehrpersonenhaushalt, in dem mehrere Computersysteme vorhanden sind – nicht gewährleistet sein dürfte. Die Rufnummer eines Smartphones als Identifizierungsmerkmal ist im vorliegenden Zusammenhang jedenfalls ungeeignet: Gegenstand der Überwachung ist nämlich ein Computersystem (zB Smartphone) und nicht ein bestimmter Anschluss (Rufnummer, die einer bestimmten SIM-Karte zugeordnet, jedoch vom verwendeten Gerät unabhängig ist).

2. Durch den Entfall der **Bezugnahme auf das Endgerät** in § 138 Abs. 1 Z 3 werden die Anforderungen an die Bezeichnung des Überwachungsgegenstandes wesentlich reduziert; die Bezeichnung eines bestimmten Endgerätes wäre dann nämlich nicht einmal in jenen Fällen erforderlich, in denen es sich um eine gezielte Überwachungsmaßnahme handelt. Eine präzise Bezeichnung des betroffenen

Gerätes wäre in diesen Fällen jedenfalls geboten; erforderlichenfalls wäre für die Anordnung einer „Funkzellenabfrage“, die mehrere Endgeräte betrifft, eine zusätzliche Regelung vorzusehen.

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.

2.1. Zunächst stellt sich die grundsätzliche **Frage**, ob eine **unwiderrufliche Funktionsunfähigkeit oder vollständige Entfernung des Überwachungsprogramms tatsächlich und in jedem Fall gewährleistet** werden kann. Ein direkter Zugriff zur Entfernung des Überwachungsprogramms könnte etwa in jenen Fällen scheitern, in denen das überwachte Computersystem zwischenzeitig an einen Dritten weitergegeben wurde oder aus anderen Gründen nicht mehr lokalisierbar ist.

Den Erläuterungen zufolge soll das Überwachungsprogramm auch mit einem mit der Dauer der gerichtlichen Anordnung übereinstimmenden „**Funktionszeitraum**“ versehen werden, nach dessen Ablauf das Programm ohne weiteren Eingriff funktionsunfähig wird. Auch ein solcher „**Selbstzerstörungsmechanismus**“ kann jedoch möglicherweise eine unwiderrufliche, vollständige Funktionsunfähigkeit nicht in jedem Fall gewährleisten. In den Erläuterungen wird in diesem Zusammenhang zwar das Sonderproblem der Erstellung eines Backups während der Überwachung, das zu einem späteren Zeitpunkt wieder eingespielt wird und das Überwachungsprogramm auf diese Weise reaktivieren könnte, angesprochen, jedoch lässt sich den Ausführungen keineswegs entnehmen, dass diese Fragen auf technischer Ebene tatsächlich verlässlich gelöst sind oder gelöst werden können. Zu denken ist hier etwa an Fälle, in denen der Überwachungszeitraum nachträglich (nach Erstellung des Backups) verkürzt wurde oder keine Internetverbindung des überwachten Gerätes mehr besteht. Soweit den Erläuterungen zufolge die Möglichkeit einer **nachträglichen Anpassung des voreingestellten Funktionszeitraumes „ohne neuen direkten Zugriff“** (dh. durch Fernzugriff) möglich sein soll, wird auf Pkt. 2. der Anmerkungen zu § 136a (Z 6 des Entwurfes) verwiesen.

2.2. Eine **Überprüfung der unwiderruflichen Funktionsunfähigkeit bzw. vollständigen Entfernung des Überwachungsprogramms** dürfte ohne neuerlichen physischen Zugang zum überwachten Gerät generell **nicht möglich** sein, zumal beide Fälle voraussetzen, dass keine Fernzugriffsmöglichkeit auf das Computersystem (mehr) besteht. Aus der bloßen Tatsache, dass kein Zugriff mehr

besteht oder das Überwachungsprogramm keine Daten mehr übermittelt, kann aber keineswegs geschlossen werden, dass das Überwachungsprogramm unwiderruflich funktionsunfähig ist bzw. vollständig entfernt wurde. In den Erläuterungen sollte daher dargelegt werden, wie gewährleistet werden kann, dass diese Anforderungen tatsächlich erfüllt werden.

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.

9. Mai 2016
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt