Verein Arbeitskreis Vorratsdaten Österreich
(AKVorrat.at)
ZVR: 140062668
Kirchberggasse 7/5
1080 Wien
info@akvorrat.at

Wien, 12. April 2016

Betreff:

Stellungnahme des Arbeitskreis Vorratsdaten Österreich im Begutachtungsverfahren zum

Entwurf des Bundesministeriums für Justiz eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden sollen (192/ME XXV. GP)

Für den AKVorrat: Mag.iur. Alexander Czadilek, Rolf-Dieter Kargl (LL.M), Ing. Dr.iur. Christof Tschohl

Der AK Vorrat nimmt zu den vorliegenden Änderungen der Strafprozessordnung 1975 (Artikel I) und des Staatsanwaltschaftsgesetzes (Artikel II) wie folgt Stellung:

I. Vorwort

Mit dem geplanten Bundesgesetz zur Änderung der Strafprozessordnung 1975 und des Staatsanwaltschaftsgesetzes soll eine Ermittlungsmaßnahme Einzug in den österreichischen Rechtsbestand halten, die in vielerlei Hinsicht **äußerst kritikwürdig** ist und **mehr Probleme schafft, als sie löst**.

Für die Beurteilung der Maßnahme *"Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden"* ist es letztlich gleichgültig, wie man die dazu eingesetzte Software nennt (Überwachungs- oder Spionagesoftware, Bundes- oder Staatstrojaner).

Die Kritik bezieht sich insbesondere auf folgende Punkte:

- Der Einsatz der Überwachungssoftware wäre ein **unverhältnismäßiger Grundrechtseingriff** (detaillierte Analyse im Besonderen Teil).
- Um die intendierte Funktionalität der Überwachungssoftware sicherzustellen, braucht diese ein Privilegierungsniveau am Zielsystem, das nur durch Ausnutzung von kritischen Sicherheitslücken erreicht werden kann. Derartige Sicherheitslücken werden zumeist für viel Geld auf **illegalen Märkten** gehandelt. Einerseits werden diese Märkte bei Ankauf der Lücken **durch österreichische Steuergelder finanziert**, andererseits wird die **gesamte IT-Sicherheit unterminiert**, da die Bundesregierung Interesse daran haben muss, dass (durch die Überwachungssoftware ausgenutzte) kritische Sicherheitslücken nicht geschlossen werden, um die Funktionalität dieser Software zu gewährleisten.[1] Somit ist jeder in Österreich lebende Mensch, der einen Personal-Computer, ein Smartphone, ein Tablet oder eine Spielekonsole verwendet, von dem in Begutachtung gegebenen Gesetz unmittelbar betroffen.

[1] Zur Problematik siehe z.B.: die Artikel vom 14.06.2013 und 09.11.2014, Die Zeit Online über die Pläne des deutschen BND,
kritische Sicherheitslücken einzukaufen, abrufbar unter http://www.zeit.de/digital/internet/2014-11/bnd-zero-day-exploit-sicherheit oder über den Handel mit Sicherheitslücken, abrufbar unter http://www.zeit.de/digital/datenschutz/2013-06/geheimdienste-kaufen-zero-day/komplettansicht.

- **Entgegen den Äußerungen des Bundesministers** für Justiz[2] und entgegen den Erläuternden Bemerkungen[3] **schließt** der **Gesetzestext**[4] ***nicht*** **aus**, dass die Überwachungssoftware per **Ferninstallation** (remote installation) auf das Zielsystem aufgespielt wird.

- Als eines der größten Probleme erscheint die sehr wahrscheinliche Entdeckung der Überwachungssoftware durch auch nur einigermaßen technisch versierte Benutzer. Diese birgt das Risiko in sich, dass Kriminelle die Ermittler ganz bewusst auf falsche Fährten locken, um vom tatsächlich geplanten Vorhaben abzulenken. Der **Einsatz** der **Überwachungssoftware** selbst kann somit eine erhebliche **Gefahr für die öffentliche Sicherheit** darstellen.

- Die Überwachung übermittelter Nachrichten kann logisch gar nicht von der **Durchsuchung lokal gespeicherter Dateien am Zielsystem** getrennt werden, wenn die Überwachungssoftware verwertbare Ermittlungsergebnisse liefern soll (dies wird in unserer Stellungnahme anhand zahlreicher Beispiele aufgezeigt). Laut dem Gesetzestext und den Materialien soll der Einsatz der Überwachungssoftware nur zulässig sein, wenn übermittelte Kommunikationsinhalte vor oder nach einer allfälligen Verschlüsselung überwacht werden. Die Ermittlung von sonst auf dem Computersystem gespeicherten Daten ist davon (mit Ausnahmen) nicht erfasst. Durch die zahlreichen Möglichkeiten, lokale Dateien vor der Übermittlung durch Kommunikationssoftware (z.B.: WhatsApp, Skype) zu verschlüsseln, wäre eine Überwachungssoftware, die keine lokale Durchsuchung von Dateien zulässt, ohne jeden Nutzen. Wird die lokale Durchsuchung jedoch zugelassen, wäre dies jedenfalls eine unzulässige, weil **unverhältnismäßige Grundrechtsverletzung**, wie schon die interministerielle Arbeitsgruppe im Jahr 2008 festgestellt hat.[5]

---

[2] APA Interview BM für Justiz Dr. Wolfgang Brandstetter am 26.03.2016, in dem dieser davon spricht, "dass er keinen Bundestrojaner wolle". "Der mit der SPÖ akkordierte Gesetzesentwurf, der nächste Woche in Begutachtung geht, *enthält keine Überwachungsmöglichkeit durch Eindringen von Computersystemen von außen mittels Spionagesoftware* und Internetüberwachung," so der Justizminister.

[3] 192/ME XXV. GP Erläuterungen S 4 zu Z 4 und 5 und S 5 zu Z 6.

[4] §§ 134 Z 4a und 136a Abs. 2 StPO (Ministerialentwurf).

[5] BMJ/BMI Interministerielle Arbeitsgruppe „Online-Durchsuchung“ Bericht Endfassung, 13.03.2008, S 26.

- Der bloße Verweis in § 145 Abs. 4 StPO (Ministerialentwurf) auf eine geeignete **Protokollierung**, um die Verwertbarkeit von Beweisen zu gewährleisten (ohne eine Normierung einer Ermächtigung zu einer Durchführungsverordnung), **entspricht weder** dem **allgemeinen Determinierungsgebot** gemäß Art 18 B-VG, **noch** genügt er **rechtsstaatlichen Anforderungen an** die **gesetzlichen Rahmenbedingungen bei Grundrechtseingriffen**.
- Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) bekommt mit der neuen Ermittlungsmaßnahme ein unausgereiftes Werkzeug in die Hand, das im Zusammenspiel mit einer rechtsstaatlich äußerst bedenklichen und unseres Erachtens verfassungswidrigen gesetzlichen Grundlage zur Datenermittlung (Polizeiliches Staatsschutzgesetz) eingesetzt werden wird.[6]

Der **Arbeitskreis Vorratsdaten Österreich ruft** das **Bundesministerium für Justiz** dringend **auf**, den in Begutachtung gegebenen **Gesetzesentwurf zurückzuziehen**. Nicht nur wurden eine grundrechtliche Wirkungsfolgenabschätzung und eine Evaluierung schon bestehender Maßnahmen verabsäumt, es hat auch den Anschein, dass man sich auf technischer Ebene nicht ausreichend mit der Materie auseinandergesetzt hat. Für die Software sollen pro Jahr EUR 450.000,- an Steuergeldern aufgewendet werden. Dieser Summe stehen zahlreiche Probleme und ein mehr als zweifelhafter Nutzen gegenüber.

Generell ist zu kritisieren, dass der **Gesetzesentwurf offenbar monatelang unverändert in der Schublade gelegen ist[7] und nur wenige Tage nach den Attentaten von Brüssel Ende März 2016 veröffentlicht wurde**. Man hat also ganz bewusst die **Angst der Bevölkerung vor Terroranschlägen genutzt**, um dieses Gesetz als notwendige Maßnahme präsentieren zu können.

---

[6] Gem. § 12 Abs. 1 PStSG darf das BVT alle tat- und fallbezogenen Informationen, die aufgrund der StPO ermittelt wurden, in der "Gefährderdatenbank" verarbeiten. Siehe dazu im Detail die Kritik unten zu Z 4 bis 6 des Begutachtungsentwurfs.

[7] Artikel von Erich Möchel auf orf.at vom 04.11.2015, http://fm4.orf.at/stories/1764335/.

Bundestrojaner: Probleme entlang des gesamten Lebenszyklus

2

- Kauf:
  Förderung eines vorrangig durch Kriminelle genutzten „Schwarzmarktes" für nicht geschlossene Sicherheitslücken
- Auffinden:
  Aufwendig und kostenintensiv

3

- Macht die Software was sie soll?
  (Nur bei Einsatz quelloffener Software durch die Behörde wirklich überprüfbar)

4

- Überwachungssoftware selbst eignet sich unter Umständen als Einfallstor für weitere Angreifer

6

- Die Überwachungssoftware muss dem Zielsystem und den dort vorhandenen Schutzmaßnahmen angepasst werden
- Zwischen Beobachtung des Zielsystems und Installation können Updates das Zielsystem entscheidend verändern
- Zugriff zum Zwecke des Ausspähens bei verschlüsselten Systemen im Standardfall nicht möglich

7

- Trojaner verändert Zielrechner, obwohl dessen Daten als Beweise dienen sollen
- Sicherheit des Zielrechners dauerhaft beeinträchtigt
- Installation verlangt pro Zielsystem (Windows, Mac, iPhone, Android) mindestens eine Sicherheitslücke

9

- Überwachen nicht gesendeter Nachrichten gleicht einer Gedankenüberwachung.
  Noch nicht Gesagtes kann gegen Beschuldigte verwendet werden
- Problem, Beweise dem zu Überwachenden zuzuordnen, wenn mehrere Benutzer einen Computer verwenden

11

- Überwachung kann entdeckt werden und den gegenteiligen Effekt haben
  (z.B. Beweisvernichtung)

12

- Nachladen beliebigen Codes, revisionssicherer Audit-Trail muss geschaffen werden

13

- Kann im Nachhinein neue Befehle bekommen, Beweise zu fälschen, zu platzieren oder zu vernichten

14

- Bei Backup könnte der Trojaner wieder aufgespielt werden
- Systemzeit ist unzuverlässig

II. Einleitung - Legitimierbarkeit

Im Zusammenhang mit geheimer Überwachung und elektronischer (Kommunikations-) Datenverarbeitung hat der Verfassungsgerichtshof im Erkenntnis zur Vorratsdatenspeicherung[8] auf den Punkt gebracht, worum es geht: ***„Der Einzelne und seine freie Persönlichkeitsentfaltung sind nicht nur auf die öffentliche, sondern auch auf die vertrauliche Kommunikation in der Gemeinschaft angewiesen; die Freiheit als Anspruch des Individuums und als Zustand einer Gesellschaft wird bestimmt von der Qualität der Informationsbeziehungen (vgl. Berka, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT, 2012, Band I/1, 22).“***

In den Materialien[9] wird auf den Schlussbericht[10] der Arbeitsgruppe "Online-Durchsuchung" vom März 2008 Bezug genommen, in dem die Verfasser zum Ergebnis kommen, dass der Einsatz von Programmen, 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 bemerkt, nach geltendem Recht nicht zulässig ist. Die nun geplante Einführung einer neuen Ermittlungsmaßnahme, nämlich die "Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden" (sog **“Quellen-Telekommunikationsüberwachung“**) durch eine spezielle Überwachungssoftware stellt nach Ansicht des BMJ keine heimliche Durchsuchung des elektronischen Geräts des Betroffenen dar, da die Ermittlung von sonst auf dem Computersystem gespeicherten Daten nicht Gegenstand dieses Gesetzesvorschlages ist. Dem ist entgegenzuhalten, dass die Installation, der Betrieb und das Verstecken einer Überwachungssoftware solche Zugriffsrechte auf dem Zielsystem benötigt, welche dem Trojaner jede beliebige Funktionalität erlauben inklusive des Durchsuchens, Manipulierens und Erstellens von Dateien. Im vorliegenden Entwurf ausdrücklich genannt und erlaubt wird der Zugriff auf Adressbücher und Kontaktverzeichnisse (z.B.: Outlook, Skype, WhatsApp). Auch wenn das BMJ unter einer solchen Durchsuchung

[8] VfGH 27.06.2014, G47/2012.
[9] 192/ME XXV. GP Erläuterungen S 1.
[10] BMJ/BMI Interministerielle Arbeitsgruppe „Online-Durchsuchung“ Bericht, Endfassung vom 09.04.2008.

eines Computersystems nach Spuren zur Identifizierung einer Person oder sonstiger Dateien keine "Online-Durchsuchung" verstehen will, ist aus technischer Sicht eine Trennung von "Online-Überwachung" und "Online-Durchsuchung" nicht möglich.

An dieser Stelle wird ein weiteres schwerwiegendes Problem der vereinfachten Herangehensweise des Gesetzgebers deutlich: Technisch kann eine Überwachungssoftware niemals nur Kommunikationsinhalte überwachen, sondern muss, um dem Ziel des Gesetzgebers gerecht zu werden, nämlich den gedanklichen Inhalt übermittelter Kommunikation zu erfassen, immer in der Lage sein, auch sonstige Vorgänge auf dem Zielsystem zu beobachten. Dies ist der einfachen Tatsache geschuldet, dass eine Verschlüsselung dieser Inhalte zu einem beliebigen Zeitpunkt vor der eigentlichen Übermittlung stattfinden kann, der Vorgang der Übermittlung selbst also keinen zweckgemäßen Anknüpfungspunkt für die Datenermittlung darstellt. Auch ohne die entsprechende Absicht des Gesetzgebers kann daher aufgrund der technischen Gegebenheiten die staatliche Überwachung auch bereits formulierte aber noch nicht kommunizierte bzw. übermittelte Gedanken erfassen.

Zahlreiche Missbrauchsfälle in Deutschland[11] und ein Urteil[12] des deutschen Bundesverfassungsgerichts machen deutlich, dass es sich bei der Online-Durchsuchung bzw. -Überwachung um eine höchst riskante und mit schwerwiegenden Eingriffen verbundene Ermittlungsmaßnahme handelt. Mit Hilfe der Installation einer Software auf dem elektronischen Gerät des Betroffenen kann dieser überwacht werden, ohne davon Kenntnis zu erlangen. Dies erscheint im Lichte der im Regelfall offenen Ermittlungen der StPO bedenklich. Der ursprüngliche Geist der StPO von 1873 war vom Grundgedanken einer "offenen" Strafverfolgung geprägt, da man damals gerade den in den Metternichschen Polizeistaat eingebetteten und dem Betroffenen und der Öffentlichkeit gegenüber geheimen Inquisitionsprozess überwunden hatte.[13] Weitere Kritikpunkte, welche noch in Kapitel III behandelt werden, sind die diversen Möglichkeiten der betroffenen Zielgruppen, sich vor diesen Maßnahmen zu schützen und die Tatsache,

[11] Siehe http://www.berliner-zeitung.de/archiv/bka-reform---das-bundeskriminalamt-soll-per-gesetz-mehr-befugnisse-bei-der-terrorabwehr-bekommen--neue-fahndungsmethoden-sollen-die-jagd-auf-staatsfeinde-erleichtern--beamter-unter-verdacht,10810590,10501420.html und http://www.spiegel.de/netzwelt/netzpolitik/0,1518,807820,00.html.
[12] BVerfG 27.02.2008, 1BvR 370/07.
[13] Schmoller, Geändertes Erscheinungsbild staatlicher Verbrechensbekämpfung?, ÖJZ 1996, 21.

dass die Überwachungssoftware eine Schadsoftware ist, welche von einem Anti-Virus-Programm bei (der sehr wahrscheinlichen) Erkennung blockiert wird. Zudem kann der Betroffene die Software bei Erkennen manipulieren oder z.B.: bewusst falsche Beweise platzieren, um die Ermittler auf eine falsche Fährte zu locken und das tatsächliche Vorhaben parallel in Ruhe ausführen zu können. In so einem Fall wäre der Einsatz der Überwachungssoftware selbst ein erhebliches Risiko für die öffentliche Sicherheit.

Im Ergebnis handelt es sich sowohl bei der Online-Durchsuchung als auch bei der Online-Überwachung um einen intensiven Eingriff in die Grundrechte der Betroffenen. Solche Eingriffe sind nur zulässig, wenn sie dem Grundsatz der Verhältnismäßigkeit entsprechen. Der Verhältnismäßigkeitsgrundsatz verlangt, dass Ermittlungsmaßnahmen und deren gesetzliche Grundlangen durch öffentliche Interessen legitimiert sind. „*Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.*“[14]

In den Erläuternden Bemerkungen zum vorliegenden Gesetzesentwurf wird die stetige Gefahr des Terrors hervorgehoben. Die neuartige Ermittlungsmaßnahme soll vor allem dem Zweck dienen, Menschen, welche in den Nahen Osten reisen wollen, zu überwachen, da sich diese möglicherweise in Terrorcamps zu potentiellen Terroristen ausbilden lassen könnten.[15] Es stellt sich somit die Frage, ob eine geplante Reise in bestimmte Gebiete bereits als konkreter Verdacht für die Ausbildung für terroristische Zwecke (§ 278e Abs. 2 StGB) oder die Beteiligung an einer terroristischen Vereinigung (§ 278b Abs. 2 StGB) gewertet wird und somit die Grundlage für den Einsatz der

[14] BVerfG 27.02.2008, 1BvR 370/07.
[15] 192/ME XXV. GP Erläuterungen S. 3.

Überwachungssoftware darstellt. Das Problem einer solchen "Stöberfahndung" ist, dass der Anwendungsbereich für die Ermittlungsmaßnahme sehr weit wird und der Einsatz überhaupt erst zur Schaffung von Verdachtslagen führen kann (dies würde jedoch dem Wortlaut des Gesetzestextes widersprechen). Die jüngere Vergangenheit in Österreich hat gezeigt, dass die bestehenden Antiterrorbestimmungen sehr oft angewendet wurden[16], um die Voraussetzungen für Ermittlungsmethoden zu schaffen, die sonst nicht angewendet werden dürften, weil die Strafdrohung der möglichen Grunddelikte ohne Terrorismuszusammenhang oft nicht die notwendigen Schwellen überschreitet. Der Verhältnismäßigkeitsgrundsatz wird dadurch zusehends in Frage gestellt.

III. Bemerkungen zu den einzelnen Bestimmungen

Bundesgesetz, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden

Der Nationalrat hat beschlossen:

Inhaltsverzeichnis

Artikel 1 Änderung der Strafprozessordnung 1975

Die Strafprozessordnung 1975, BGBl. Nr. 631/1975, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 112/2015, wird wie folgt geändert

1. Im Inhaltsverzeichnis lautet die Überschrift des 5. Abschnitts des 8. Hauptstücks:

„Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Überwachung von Nachrichten und von Personen sowie Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“

2. Im Inhaltsverzeichnis wird im 5. Abschnitt des 8. Hauptstücks die Wendung „§ 135 Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung sowie Überwachung von Nachrichten“ *durchdie Wendung* „§ 135 Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Überwachung von Nachrichten und von Personen sowie Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“ *ersetzt.*

3. Die Überschrift des 5. Abschnittes des 8. Hauptstückes lautet:

„Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Überwachung von Nachrichten und von Personen sowie Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“

4. In § 134 wird nach der Z 4 folgende Z 4a eingefügt:

„4a. „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“ das Ermitteln von Nachrichten und sonstigen Daten (§ 74 Abs. 2 StGB), die im Wege eines Computersystems (§ 74 Abs. 1 Z 8 StGB) übermittelt und empfangen werden, durch Installation eines Überwachungsprogramms im Computersystem ohne Kenntnis des Inhabers eines solchen Systems oder sonstiger Verfügungsbefugter,“

[16] z.B.: Tierschützerprozess in Wr. Neustadt; Uni Brennt AktivistInnen; Anti-Akademikerball-DemonstrantInnen.

5. § 134 Z 5 lautet:

„5. „Ergebnis“ (der unter Z 1 bis 4a angeführten Beschlagnahme, Auskunft oder Überwachung) der Inhalt von Briefen (Z 1), die Daten einer Nachrichtenübermittlung oder des Inhalts übertragener Nachrichten (Z 2 und 3), die Bild- oder Tonaufnahme einer Überwachung (Z 4) und der Inhalt übertragener Nachrichten oder sonstige Daten, die durch eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden (Z 4a), ermittelt wurden.“

6. Nach § 136 wird folgender § 136a samt Überschrift eingefügt:

„Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden

§ 136a. (1) Die Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, ist unter den Bedingungen des § 136 Abs. 1 Z 3 und Abs. 4 zulässig, wenn der Eingriff in das Computersystem notwendig ist, um die Überwachung und Aufzeichnung von Nachrichten in unverschlüsselter Form zu ermöglichen.

(2) Soweit dies zur Durchführung der Ermittlungsmaßnahme unumgänglich ist, ist es zulässig, in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume einzudringen, Behältnisse zu durchsuchen und spezifische Sicherheitsvorkehrungen zu überwinden, um auf das Computersystem zuzugreifen.

(3) Eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, ist überdies nur dann zulässig, wenn gewährleistet werden kann, dass das Überwachungsprogramm

1. ausschließlich jene Daten erfasst, die im Wege des Computersystems übermittelt und empfangen werden, sowie jene Daten, die Rückschlüsse auf die Namen oder die sonstigen Identifizierungsmerkmale der Inhaber oder Verfügungsbefugten der an der Nachrichtenübermittlung beteiligten Computersysteme erlauben,
2. nach Beendigung der Ermittlungsmaßnahme funktionsunfähig ist oder ohne dauerhafte Schädigung oder Beeinträchtigung des Computersystems und der in ihm gespeicherten Daten entfernt werden kann, und
3. keine Schädigung oder dauerhafte Beeinträchtigung dritter Computersysteme, die nicht der Überwachung unterliegen, bewirkt.“

Kommentar zu Z 4 bis 6 des Entwurfs (§§ 134 Z 4a und 5, 136a StPO)

A. Art 8 EMRK (Recht auf Achtung des Privat- und Familienlebens)

1. Allgemeines

Mit der vorliegenden Bestimmung soll eine Ermittlungsmaßnahme in den österreichischen Rechtsbestand Einzug halten, die äußerst problematisch ist. Von der Anschaffung einer Überwachungssoftware über die Analyse, die Installation, den Betrieb (Durchführung der Überwachung) bis hin zur Deinstallation der Software werden zahlreiche Fragen aufgeworfen.

Entgegen den Äußerungen des Bundesministers für Justiz[17] und entgegen den Erläuternden Bemerkungen[18], dass eine Ferninstallation (remote installation, Aufspielen der Software von außen über das Internet) nicht zulässig sein soll, schließt der Gesetzestext[19] eindeutig *nicht* aus, dass die Überwachungssoftware über Fernzugriff auf

[17] APA Interview BM für Justiz Dr. Wolfgang Brandstetter am 26.03.2016, in dem dieser davon spricht, "dass er keinen Bundestrojaner wolle". "Der mit der SPÖ akkordierte Gesetzesentwurf, der nächste Woche in Begutachtung geht, *enthält keine Überwachungsmöglichkeit durch Eindringen von Computersystemen von außen mittels Spionagesoftware* und Internetüberwachung", so der Justizminister.

[18] 192/ME XXV. GP Erläuterungen S 4 zu Z 4 und 5 und S 5 zu Z 6.

[19] §§ 134 Z 4a und 136a Abs. 2 StPO (Ministerialentwurf).

das Zielsystem gespielt wird (arg § 134 Z 4a StPO: "durch Installation eines Überwachungsprogramms im Computersystem ohne Kenntnis des Inhabers[...]" und § 136a Abs. 2 StPO). Nach dem Wortlaut des § 136a Abs. 2 StPO soll die Installation der Software durch physischen Zugriff und allfälliges Eindringen in Räumlichkeiten nicht der Regelfall sein, vielmehr ist ein solches Vorgehen nur zulässig „soweit dies zur Durchführung der Ermittlungsmaßnahme unumgänglich ist“. Bei der Interpretation einer Norm ist zu allererst auf den Bedeutungsgehalt der Worte Bedacht zu nehmen, erst, wenn dieser nicht eindeutig ermittelt werden kann, ist auf andere Interpretationsmethoden (historische Interpretation - Blick in die Materialien) abzustellen, was hier aber gar nicht notwendig ist. Wenn der Gesetzgeber die Ferninstallation tatsächlich nicht zulassen will, muss dies im Gesetzestext normiert sein. Eine Erwähnung in den Materialien ist nicht ausreichend.

Der alternative Einbau von Hardware-Komponenten zur Überwachung im Computersystem (z.B.: Hardware-Keylogger) ist vom Gesetzestext jedenfalls nicht gedeckt (arg § 134 Z 4a StPO "durch Installation eines Überwachungs*programms*[...]"). Wenn es für die Durchführung der Ermittlungsmaßnahme unumgänglich ist, soll es auch zulässig sein, in Wohnungen und andere vom Hausrecht geschützten Räume einzudringen und auch spezifische Sicherheitsvorkehrungen (z.B.: Passwortschutz des Computersystems) zu überwinden, um auf das System zugreifen zu können.

Um ein Funktionieren der Überwachungssoftware sicherzustellen (von der physischen oder Ferninstallation bis zum laufenden Betrieb), braucht es ein Privilegienniveau (Zugriffsrechte) am Computersystem, das nur durch die Ausnutzung kritischer Sicherheitslücken erreicht werden kann. Auch um Updates einspielen zu können, welche notwendig sind, um das kontinuierliche Funktionieren der Software sicherzustellen, braucht es administrative Rechte am Computersystem, die es zulassen, jeden beliebigen Code nachzuladen. Der mittel- oder unmittelbare Einkauf von Wissen über solche Sicherheitslücken am Schwarzmarkt bzw. "Grauen Markt"[20] und dessen Finanzierung durch österreichische Steuergelder ist keinesfalls zu rechtfertigen und abzulehnen. Um

[20] In der jüngeren Vergangenheit ist regelrecht ein eigenes Geschäftsmodell entstanden, anstatt Sicherheitslücken den Herstellern von Software bekanntzugeben, das Wissen zu Profit zu machen. Kunden solcher Unternehmen sind nicht nur europäische Behörden, sondern auch Diktaturen in Afrika und im Nahen Osten.

den Betrieb der Überwachungssoftware zu gewährleisten und laufende Ermittlungen nicht zu gefährden, muss die Bundesregierung auch ein Interesse daran haben, dass benutzte kritische Sicherheitslücken nicht geschlossen werden. Damit wird die gesamte IT-Sicherheit in Österreich unterminiert und letztendlich ist jeder in Österreich lebende Mensch, der ein Computersystem verwendet, von den geplanten Bestimmungen unmittelbar betroffen. Die Bundesregierung sollte stattdessen vielmehr die Stärkung der Sicherheit von Endgeräten und damit die Datensicherheit aller Benutzer forcieren. Insbesondere im Hinblick auf die Bedeutung von Computersystemen für die moderne Gesellschaft, Wirtschaft und Demokratie und die vielen Berichte über kritische IT-Sicherheitspannen und -gefahren ist die aktive Schwächung der IT-Sicherheit durch staatliches Handeln zutiefst unverantwortlich und der Sicherheit der Bevölkerung nicht zuträglich.

2. Geeignetheit

Aus technischer Sicht kommen berechtigte Zweifel auf, ob der Einsatz der geplanten Überwachungssoftware überhaupt geeignet ist, das legitime Ziel der Bekämpfung und Verfolgung von Terrorismus und (organisierter) schwerer Kriminalität zu verfolgen. Der aktuelle Stand der Technik lässt eine treffsichere, schadlose und zuverlässige Anwendung gar nicht zu. Ausfälle im Rahmen des Einsatzes könnten leicht zu einem Fehlschlagen oder Bekanntwerden der Ermittlungen führen.

Einerseits werden auch nur halbwegs technisch versierte Benutzer des kompromittierten Computersystems die aufgespielte Schadsoftware[21] erkennen[22] und ihr Verhalten dementsprechend ändern, andererseits ist es sehr wahrscheinlich, dass der Einsatz der Überwachungssoftware selbst oder die Ausleitung von Daten durch Anti-Viren-Software oder andere Software, die die Übertragung ausgehender Daten

[21] Nachdem zur Installation und u.U. zum Betrieb kritische Sicherheitslücken ausgenutzt werden müssen, um die entsprechenden Systemprivilegien zu erhalten, muss die Überwachungssoftware als solche bezeichnet werden.

[22] Laut Kaspersky Lab ist es sehr wahrscheinlich, dass „Kriminelle, die etwas zu verbergen haben, durchaus in der Lage sind, sich vor solchen Trojanern zu schützen".
http://www.kaspersky.com/de/downloads/pdf/faq_online-durchsuchungen_kaspersky_labs.pdf.

unterdrückt, erkannt[23] und unterdrückt wird. Kaspersky Lab gab in einer Stellungnahme[24] bekannt, dass, wenn ein Staatstrojaner von einer Antivirus-Software erkannt wird, dieser daran gehindert wird, Daten nach außen zu senden. Ein erhöhtes ausgehendes Datenaufkommen oder eine unerklärt erhöhte CPU-Leistung kann auch von technisch-nicht versierten Benutzern leicht selbst erkannt werden. Sollte der Betroffene die Überwachungssoftware entdecken, könnte er diese missbrauchen und den Ermittlern falsche Ergebnisse liefern (gezielte Beweismanipulation, Legen einer falschen Fährte). Durch diese falschen Ergebnisse wäre die Ermittlung im besten Fall nutzlos. Noch bedenklicher erscheint aber die Tatsache, dass fehlgeleitete Ermittlungen dazu führen können, dass Kriminelle vom tatsächlich geplanten Vorhaben ablenken und dieses in Ruhe verwirklichen können. Der Einsatz der Überwachungssoftware selbst wird somit zu einer erheblichen Gefahr für die öffentliche Sicherheit.

Es kann weiters nicht sichergestellt werden, dass der Überwachte das Computersystem wirklich selbst nutzt, oder ob nicht ein Anderer (z.B.: Mitbewohner) dieses in Verwendung hat (oft werden Benutzerkonten gemeinsam genutzt, bei Smartphones gibt es meistens gar keine Benutzerverwaltung). In die Privatsphäre dieser Menschen würde auch eingegriffen. Die gewonnenen Beweise würden den Betroffenen vor eine unmögliche Beweisentkräftung stellen und somit könnte es zur Verurteilung von Unschuldigen kommen.

Gegen die Geeignetheit des Mittels zur Zielerreichung sprechen auch die zahlreichen, hinlänglich bekannten, einfachen Umgehungsmöglichkeiten, trotz Einsatzes einer Überwachungssoftware verschlüsselt kommunizieren zu können. Einige sollen hier kurz skizziert werden:[25]

- Verschlüsselung bzw. Entschlüsselung jedweder Datei auf einem Offline-Gerät, Übertragung per überwachtem Gerät

[23] Auch Sicherheits-Apps auf modernen Smartphones können verdächtige Software aufspüren und dem Benutzer melden.
[24] http://www.kaspersky.com/de/downloads/pdf/faq_online-durchsuchungen_kaspersky_labs.pdf.
[25] Auf die hier schlagend werdende Problematik, dass eine Überwachung von Nachrichten iSd § 136a StPO [Ministerialentwurf)] logisch und sinnvoll gar nicht von einer [grundrechtlich nicht zulässigen] Online-Durchsuchung getrennt werden kann, wird im Punkt 4. "Verhältnismäßigkeit" eingegangen.

- jede Datei (Text-, Bild-, Video- oder Audiodatei) kann vor Übergabe an die Kommunikationssoftware verschlüsselt werden (z.B.: verschlüsselte *.zip-Datei) und als Dateianhang übermittelt werden
- ein handgeschriebener Text kann eingescannt und als verschlüsselte PDF-Datei gespeichert und anschließend übermittelt werden
- Verwendung von vorab ausgemachten Codewörtern in der (verschlüsselten) Kommunikation
- eine Datei kann verschlüsselt werden und auf einem physischen Medium verschickt werden

Man muss davon ausgehen, dass die "Zielgruppe", gegen die die Überwachungssoftware eingesetzt werden soll, ausreichend kreativ und motiviert ist, um einer Überwachung unverschlüsselter Nachrichten zu entgehen. Aufgrund der massiven Umgehungsmöglichkeiten und der Vielzahl an verfügbaren verschlüsselten Nachrichtendiensten (Threema, Signal, Telegram, Cypher, etc.), welche alle einzeln überwacht werden müssten, ist schon die Geeignetheit der Maßnahme sehr zweifelhaft.

Viele Argumente sprechen also dafür, dass der Einsatz einer Überwachungssoftware gar kein geeignetes Mittel ist, um das legitime Ziel der Bekämpfung und Verfolgung von Terrorismus und organisierter Kriminalität zu verfolgen.

3. Erforderlichkeit

Weiters ist zu prüfen, ob die geheime Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, überhaupt notwendig ist oder ob andere, gelindere Mittel zum selben Ermittlungserfolg und somit zur Zielerreichung führen würden. In den meisten Fällen der Überwachung von Kommunikationsdiensten ist der Weg, den Dienstanbieter mit einer entsprechenden Rechtsgrundlage um die Auskunft von Inhaltsdaten zu ersuchen (Lawful Intercept), ein gelinderes Mittel.

Schon im Schlussbericht der Interministeriellen Arbeitsgruppe zur Online-Durchsuchung heißt es: „*Ein so schwerwiegender Eingriff wie die geheime Überwachung kann im Strafverfahren nur bei Bestehen eines dringenden Tatverdachts erlaubt werden. Besteht aber ein solcher Verdacht, so können auch andere Ermittlungsmaßnahmen wie eine Hausdurchsuchung angeordnet werden, dann könnte u.U. sogar eine Festnahme erfolgen. Es ist daher zu prüfen, ob diese und ähnliche Möglichkeiten, die die Rechtsordnung schon jetzt bietet, nicht ausreichen, um das Ziel der Strafverfolgung und der Beweissicherung zu erreichen. Dagegen könnte eingewendet werden, dass solche offenen Maßnahmen zur Verhinderung von geplanten Taten möglicherweise nicht ausreichen. Dem ist entgegenzuhalten, dass jemand, der Taten plant und vorbereitet, damit kaum fortfahren wird, wenn ihm die Staatsgewalt (Polizei) klar und deutlich zu erkennen gibt, dass sie um seine Aktivitäten weiß und diese mit Argusaugen beobachtet – ganz abgesehen von der Möglichkeit einer Bestrafung wegen einer allenfalls verwirklichten Vorbereitungstat (z.B. Waffendelikt).*"[26]

Der Einsatz der Überwachungssoftware soll den gleichen Anwendungsbereich haben und nur unter den gleichen Voraussetzungen wie die optische und akustische Überwachung gemäß § 136 Abs. 1 Z 3 und Abs. 4 StPO zulässig sein.[27] In den Materialien wird festgehalten[28], dass der Umstand der lückenhaften Überwachungsmöglichkeiten von Beschuldigten genützt wird, um gezielt einer Überwachung zu entgehen, wenn diese die Befürchtung haben, Subjekt einer Überwachung zu sein. Weiters wird festgehalten, dass eine Überwachung verschlüsselter Kommunikation möglich wäre, "wenn eine optische und akustische Überwachung im Rahmen der strengen Voraussetzungen der §§ 136ff StPO angeordnet werden kann, was jedoch einen weitaus schwereren Grundrechtseingriff für den Überwachten mit sich brächte". Dem letzten Argument ist nicht beizupflichten. Durch die Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, kommt es für den Betroffenen zu einer kompletten Durchleuchtung seiner Person. Der diesbezügliche Grundrechtseingriff ist also mindestens genauso schwer wie bei der optischen und akustischen Überwachung

[26] Interministerielle Arbeitsgruppe BMJ/BMI, Online-Durchsuchung (2008) 34f.
[27] Aufklärung eines mit mehr als zehn Jahren FS bedrohten Verbrechens oder eines Verbrechens gem. §§ 278a und 278b StGB; konkreter Tatverdacht bzw. Annahme der Kontaktherstellung des Überwachten zu einer solchen Person; bestimmte Tatsachen müssen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen.
[28] 192/ME XXV. GP Erläuterungen S 3.

und betrifft sehr wahrscheinlich auch Dritte. Wenn der Gesetzgeber nun davon ausgeht, dass es bereits Ermittlungsmaßnahmen gibt, die zum gleichen, legitimen Ziel führen und tatsächlich ein Mittel darstellen, das gleich oder weniger intensiv in die Grundrechte eingreift, kann die Grundrechtsprüfung nur zur Unverhältnismäßigkeit der geplanten Überwachungsmethode führen. Ein gelinderes Mittel wäre wie eben erwähnt auch die Hausdurchsuchung, nachdem ja schon ein konkreter Tatverdacht gegen den zu Überwachenden bestehen muss. Bei einer solchen könnten auch Beweismittel ohne die Gefahr einer Kompromittierung sichergestellt und eine Tat sehr wahrscheinlich verhindert bzw. verfolgt werden.

In den Materialien heißt es, dass die Ermittlungsmethoden an die technischen Entwicklungen und das geänderte Kommunikationsverhalten angepasst werde müssen. Argumentiert wird damit, dass die Attentäter der Anschläge von Paris im November 2015 internetbasiert über Spielekonsolen kommuniziert hätten. Bemerkenswert dabei ist, dass sich das Ministerium diesbezüglich auf eine Falschmeldung[29] in den Medien bezieht, also einer klassischen "Zeitungsente" aufgesessen ist. Noch bemerkenswerter ist aber, dass diese Falschmeldung bereits im November 2015 als solche entlarvt wurde und sich trotzdem in den Erläuternden Bemerkungen vom 31.03.2016 wiederfindet. Im Übrigen wird davon ausgegangen, dass besagte Attentäter hauptsächlich nicht digital, sondern persönlich kommuniziert haben.

4. Verhältnismäßigkeit im engeren Sinn

Die Verhältnismäßigkeit im engeren Sinn wird anhand einer Abwägung zwischen dem konkreten Eingriff in das Grundrecht des Betroffenen einerseits und dem verfolgten öffentlichen Interesse andererseits geprüft. Nachdem beim Einsatz einer Überwachungssoftware die Trennung von zulässig und unzulässig ermittelten Daten äußerst schwierig ist, ist fraglich, ob im Sinne des Eignungsgebotes die Verhältnismäßigkeit gewährleistet werden kann. Diese hängt nämlich wesentlich von den einschlägigen technologischen Gegebenheiten und konkreten Möglichkeiten der verwendeten Software ab. Die Bedingungen technischer Gefahrlosigkeit und

[29] https://www.washingtonpost.com/news/the-intersect/wp/2015/11/16/everything-the-internet-hoax-machine-tricked-you-into-believing-about-paris/.

Treffsicherheit können nicht als ausreichend erfüllt angesehen werden. Auch in der Relation von Aufwand und Ergebnis erscheint die Verhältnismäßigkeit zweifelhaft. Dies hat schon die Arbeitsgruppe zur Online-Durchsuchung im Jahr 2008 festgestellt.[30]

Um die zahlreichen Möglichkeiten zu verhindern, trotz Einsatzes der Überwachungssoftware verschlüsselt zu kommunizieren, müsste es zu einer echten Online-Durchsuchung des Computersystems kommen. Jede im System gespeicherte Datei müsste einer Überwachung unterliegen, um einen Ermittlungserfolg sicherzustellen. Kein Gedankeninhalt, auch nicht der Inhalt von Mitteilungen, die gar nicht absendet werden, würde vor den Ermittlungsbehörden verborgen bleiben. Die Überwachung dieser höchstpersönlichen Sphäre eines Menschen grenzt an die Einführung einer "Gedankenpolizei". Die Eignung der Ermittlungsmaßnahme wird durch die technischen Safeguards geradezu konterkariert. Gemäß § 136a StPO soll der Einsatz der Überwachungssoftware nämlich nur dann zulässig sein, wenn "gewährleistet werden kann, dass das Überwachungsprogramm ausschließlich jene Daten erfasst, die im Wege des Computersystems übermittelt und empfangen werden[...]". Diese Abgrenzung gleicht der deutschen Rechtslage zur Quellen-Telekommunikationsüberwachung. Anhand des dortigen Diskurses der letzten Jahre zeigt sich auch die enorme Schwierigkeit, eine technische Lösung zu implementieren, welche dieser Anforderung genügt.[31] Soweit bereits lokal verschlüsselte Dateien über Kommunikationsdienste verschickt werden, ist der Einsatz der Überwachungssoftware zur Bekämpfung von Terrorismus und schwerer organisierter Kriminalität völlig nutzlos.

Schwere Eingriffe in die Privatsphäre der Überwachten und etwaiger Dritter, die Unterminierung der gesamten IT- und Datensicherheit in Österreich sowie enorm hoch veranschlagte finanzielle Kosten stehen einer Überwachungsmethode mit äußerst zweifelhaften Ermittlungserfolgen gegenüber. Das BMJ geht davon aus, dass es nicht mehr als sechs Anwendungsfälle der neuen Ermittlungsmaßnahme pro Jahr geben[32]

---

[30] Interministerielle Arbeitsgruppe BMJ/BMI, Online-Durchsuchung (2008) 70.
[31] Siehe http://www.ccc.de/system/uploads/189/original/BKAG_Stellungnahme.pdf, http://www.ccc.de/system/uploads/103/original/Schaar-Bericht.pdf und https://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf.
[32] Leiter der Strafrechtssektion im BMJ Christian Pilnacek zum Standard, 10.04.2016, http://derstandard.at/2000034552505/Kritik-Zeitungsente-dient-als-Begruendung-fuer-Bundestrojaner.

und diese nur sehr maßvoll eingesetzt werden wird.[33] Wenn dem tatsächlich so sein sollte, wäre, nachdem für den Einsatz der Überwachungssoftware ja bereits ein konkreter Tatverdacht vorliegen muss, eine Observation bzw. eine Hausdurchsuchung und Beschlagnahme des Computersystems in diesen wenigen Fällen das gelindere und sogar effektivere Mittel zur Verfolgung oder Verhinderung von Straftaten. Nach Aussage des BMJ haben die Ermittler einerseits bekräftigt, dass sie die Überwachungssoftware für ihre Tätigkeit unbedingt brauchen[34], andererseits haben die Experten des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT) versichert[35], dass es für die Software technisch möglich sei, die Überwachung von übermittelten Nachrichten von der Überwachung des Internet-Surf-Verhaltens zu trennen. Wenn man diese Aussagen gemeinsam betrachtet, zeigt sich (deutlicher als in den Erläuterungen) die Motivation für die Einführung der Maßnahme. Es liegt die Vermutung nahe, dass es dem Gesetzgeber bei dieser Maßnahme weniger darum geht, konkret geplante Anschläge zu verhindern, sondern ein Mittel in die Hand zu bekommen, das es im Wege der „Stöberfahndung" ermöglicht, Netzwerke und Strukturen in diversen Milieus zu erforschen. Hauptsächlich eingesetzt werden wird die Software nicht von der Kriminalpolizei zur Verfolgung von Straftaten, sondern zur präventiven Einschätzung von Verdachtslagen durch das BVT (dies lässt der Gesetzestext zu, va iVm §§ 278a ff StGB und dem PStSG). Im Hinblick auf die öffentliche Sicherheitsdebatte, die gesamteuropäische Situation und die hohen finanziellen Kosten der Überwachungssoftware wäre es auch sehr verwunderlich, wenn § 136a StPO wirklich nur ca. sechs Mal pro Jahr zur Anwendung kommen würde. Auszugehen ist demnach von einem viel häufigeren Einsatz der Maßnahme, vielen Verfahrenseinstellungen und wenigen Anklagen. Gemäß § 12 Abs. 1 Polizeiliches Staatsschutzgesetz (PStSG) dürfen aber alle tat- und fallbezogenen Daten, die aufgrund der StPO ermittelt wurden, in der neuen "Gefährderdatenbank" verarbeitet werden. Die Dimension der Datenspeicherung wird bewusst, wenn man bedenkt, dass die Überwachungssoftware Zugriff auf Kontakt- und Adressverzeichnisse haben soll und nach dem PStSG auch Daten von Kontakt- und

[33] 192/ME XXV. GP Erläuterungen S 3.
[34] Sprecherin des BMJ Katharina Holzinger am 25.03.2016, http://derstandard.at/2000033576610/Staatstrojaner-Justizminister-will-Spionagesoftware-fuer-Terror-Ermittler.
[35] Leiter der Sektion Strafrecht im BMJ Christian Pilnacek am 10.04.2016, http://derstandard.at/2000034552505/Kritik-Zeitungsente-dient-als-Begruendung-fuer-Bundestrojaner.

Begleitpersonen gespeichert werden dürfen. Schon bei der Einführung der Vorratsdatenspeicherung (VDS) wurde seitens des Gesetzgebers versichert, die neuen Befugnisse nur sehr maßhaltend im Bereich schwerer Kriminalität einzusetzen, tatsächlich wurden diese aber ausschließlich für Ermittlungen bei minderschweren Delikten in Anspruch genommen, die keinerlei terroristischen oder schwerkriminellen Zusammenhang aufwiesen. Problematisch ist insbesondere, dass im PStSG die Löschungsverpflichtungen und Informationspflichten nur unzureichend normiert sind und zudem das Rechtsschutzsystem massive Defizite aufweist. Auch dürfen Daten mit ausländischen Nachrichtendiensten ausgetauscht werden, was dann problematisch ist, wenn es diesbezüglich gar keinen Rechtsschutz gibt. Die Vermutung der Schaffung eines "Verdachtsauffindungstools" drängt sich auf. Statt unter diesem Etikettenschwindel die Freiheitsrechte potentiell aller in Österreich lebenden Menschen[36] zu beschneiden, sollte intensiv in Human Intelligence investiert werden, also die hochspezialisierte Ausbildung von Beamten, um in solchen Milieus erfolgreich ermitteln zu können. Den Sicherheitsbehörden hingegen ein äußerst unausgereiftes Werkzeug zusammen mit (Daten-)Ermittlungsbefugnissen aufgrund einer rechtsstaatlich höchst bedenklichen und unseres Erachtens verfassungswidrigen gesetzlichen Grundlage (PStSG) in die Hand zu geben, ist demokratiepolitisch unverantwortlich.

Insgesamt kann festgehalten werden, dass die geplante Ermittlungsmethode einen nicht verhältnismäßigen Eingriff und somit eine Verletzung des Grundrechts auf Achtung des Privatlebens gemäß Art 8 EMRK darstellt.

B. Grundrecht auf Datenschutz (DSG 2000)

In Österreich findet man mit dem § 1 DSG 2000 eine Bestimmung, die in Verfassungsrang steht, und den Spielraum der Gesetzgebung für die Online-Überwachung wesentlich beschränkt.

[36] Siehe dazu die Bemerkungen zur Anwendung der Antiterrorbestimmungen in der jüngeren österreichischen Vergangenheit auf S 8 dieser Stellungnahme.

Des Weiteren enthält das DSG 2000 Regelungen über die Betroffenenrechte und den damit verbundenen Rechtsschutz.[37]

Gem. § 1 Abs. 2 DSG 2000 dürfen personenbezogene Daten ohne Zustimmung des Betroffenen von staatlichen Behörden nur verwendet und somit in das Grundrecht eingegriffen werden, wenn der Eingriff auf Grund eines Gesetzes und aus den in Art 8 Abs. 2 EMRK taxativ aufgezählten Gründen (also besonders wichtigen öffentlichen Interessen) notwendig ist. Außerdem muss der Eingriff verhältnismäßig sein und gemäß § 1 Abs. 2 letzter Satz DSG 2000 das gelindeste Mittel zur Zielerreichung darstellen. Für die legistische Ausgestaltung von Eingriffsermächtigungen bedeutet dies, dass erstens unter mehreren geeigneten und erforderlichen Mitteln nur jenes mit der geringsten Eingriffsintensität verfassungsrechtlich zulässig ist und zweitens auch dieses gelindeste Mittel insgesamt in einem angemessenen Verhältnis zum angestrebten Zweck stehen muss.[38] Für Daten, die ihrer Art nach besonders schutzwürdig sind (§ 4 Abs. 2 DSG 2000), dürfen Gesetze Eingriffe nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Hierbei ist vor allem an die durchlaufende Protokollierung, Verschwiegenheitsverpflichtungen, Zweckbindungen, Verwendungsbeschränkungen und Informations- bzw. Rechtsschutzmechanismen zu denken. Im Falle einer Online-Quellen-Telekommunikationsüberwachung können die zu ermittelnden Daten im Vorhinein nicht determiniert werden, sodass auch sensible Daten in die Ermittlungsergebnisse einfließen können. Dabei kann es sich auch um sensible Daten von unbeteiligten Dritten handeln. Im vorhergehenden Kapitel wurde schon die Geeignetheit eines solchen Eingriffs behandelt, wo man zu dem Ergebnis kam, dass vieles gegen die Geeignetheit des Mittels und zudem einiges gegen die Verhältnismäßigkeit spricht.

[37] § 26-34 Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000) idF BGBl. I Nr. 83/2013.
[38] Interministerielle Arbeitsgruppe BMJ/BMI, Online-Durchsuchung (2008) 73f.

7. In § 137 Abs. 1 lautet der zweite Satz:
„Die übrigen Ermittlungsmaßnahmen nach den §§ 135, 136 und 136a sind von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen, wobei das Eindringen in Räume nach § 136 Abs. 2 oder § 136a Abs. 2 jeweils im Einzelnen einer gerichtlichen Bewilligung bedarf."

Kommentar zu Z 7:

Hier wird die allgemeine Problematik schlagend, dass in der Praxis oft allzu leichtfertig die genehmigungsbedürftigen Ermittlungsmaßnahmen auf Antrag der Staatsanwaltschaft durch den Haft- und Rechtsschutzrichter ohne besondere Prüfung durch diesen genehmigt wird (sogenannte "Stampiglien-Bewilligung"). Diskussionswürdig ist die Frage, ob bei besonders eingriffsintensiven Ermittlungsmaßnahmen nicht ein Richtergremium zur Genehmigung wünschenswerter wäre als eine Einzelrichtergenehmigung, nachdem eine Entscheidung im Kollegium die Qualität und Maßhaltigkeit der Genehmigung erhöhen würde. Überhaupt wäre hier eine Evaluierung der Genehmigungspraxis sowie der Ermächtigungen des Rechtsschutzbeauftragten der Justiz gem. § 147 StPO von allgemeinem Interesse.

8. In § 137 Abs. 3 lautet der erste Satz:
„Ermittlungsmaßnahmen nach den §§ 135, 136 und 136a dürfen nur für einen solchen künftigen, in den Fällen der §§ 135 Abs. 2 und 136a auch vergangenen, Zeitraum angeordnet werden, der zur Erreichung ihres Zwecks voraussichtlich erforderlich ist."

9. § 138 Abs. 1 lautet:
„(1) Anordnung und gerichtliche Bewilligung einer Beschlagnahme von Briefen nach § 135 Abs. 1 haben die Bezeichnung des Verfahrens, den Namen des Beschuldigten, die Tat, deren der Beschuldigte verdächtig ist, und ihre gesetzliche Bezeichnung sowie die Tatsachen, aus denen sich ergibt, dass die Anordnung oder Genehmigung zur Aufklärung der Tat erforderlich und verhältnismäßig ist, anzuführen; Anordnung und Bewilligung nach den §§ 135 Abs. 2 und 3, 136 und 136a haben überdies zu enthalten:

1. die Namen oder sonstigen Identifizierungsmerkmaie des Inhabers der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Person, deren Überwachung angeordnet wird, oder des Inhabers oder Verfügungsbefugten des Computersystems, dessen Überwachung angeordnet wird,
2. die für die Durchführung der Ermittlungsmaßnahme in Aussicht genommenen Örtlichkeiten sowie das Computersystem, das überwacht werden soll,
3. die Art der Nachrichtenübertragung, die technische Einrichtung oder die Art der voraussichtlich für die optische und akustische Überwachung zu verwendenden technischen Mittel,
4. den Zeitpunkt des Beginns und der Beendigung der Überwachung,
5. die Räume, in die auf Grund einer Anordnung eingedrungen werden darf,
6. im Fall von §§ 136 Abs. 4 und 136a Abs. 1 die Tatsachen, aus denen sich die schwere Gefahr für die öffentliche Sicherheit ergibt."

10. § 138 Abs. 5 lautet:
„(5) Nach Beendigung einer Ermittlungsmaßnahme nach den §§ 135 Abs. 2 und 3, 136 und 136a hat die Staatsanwaltschaft ihre Anordnung und deren gerichtliche Bewilligung dem Beschuldigten und den von der Durchführung der Ermittlungsmaßnahme Betroffenen unverzüglich zuzustellen. Die Zustellung kann jedoch aufgeschoben werden, solange durch sie der Zweck dieses oder eines anderen Verfahrens gefährdet wäre. Wenn die

Ermittlungsmaßnahme später begonnen oder früher beendet wurde als zu den in Abs. 1 Z 4 genannten Zeitpunkten, ist auch der Zeitraum der tatsächlichen Durchführung mitzuteilen."

11. In § 140 Abs. 1 lautet die Z 4:

„4. in den Fällen der §§ 135 Abs. 1, Abs. 2 Z 2 und 3, Abs. 3 Z 2 bis 4 und 136a nur zum Nachweis einer vorsätzlich begangenen strafbaren Handlung, derentwegen die Ermittlungsmaßnahme angeordnet wurde oder hätte angeordnet werden können."

Kommentar zu Z 11:

§ 281 Abs. 1 Z 3 iVm § 281 Abs. 3 StPO stellt einen relativen Nichtigkeitsgrund dar. Das bedeutet, wenn eine Bestimmung (z.B.: § 140 Abs. 1 Z 4 StPO) in der Hauptverhandlung missachtet worden ist, diese Missachtung nachteilige Auswirkungen auf das Urteil für den Angeklagten haben muss. Man kann auf einfachste Art und Weise die Konsequenzen einer Nichtigkeitsrüge umgehen. Wenn andere Beweise gesammelt werden, muss das Gericht sich bei der Urteilsbegründung also nicht mehr auf die an sich nicht verwertbaren Beweise stützen. Ein kurzes Beispiel soll dies verdeutlichen. Gegen Person A wird wegen Beteiligung an einer terroristischen Vereinigung ermittelt. Dabei werden Beweise zufällig gefunden, dass Person A eine Sachbeschädigung begangen hat (Strafrahmen sechs Monate Freiheitsstrafe). Die Ermittlungsmethode hätte für die Sachbeschädigung nicht angeordnet werden dürfen. Diese Ergebnisse dürfen auch nicht verwertet werden (§ 140 Abs. 1 Z 4 StPO). Wenn die Ermittler aber nun Zeugen oder die Kommunikationsteilnehmer vernehmen oder Person A selbst ein Geständnis ablegt, dann haben die an sich nicht verwertbaren Ergebnisse keinen Einfluss mehr auf das Urteil. Es liegen demnach Kontrollbeweise vor, auf welche sich das Gericht stützen kann und eine Rüge der Nichtigkeit gemäß § 281 Abs. 1 Z 3 StPO ist nicht mehr erfolgreich.

Beweismittel, welche einem Verwertungsverbot unterliegen, dürfen zwar in die Hauptverhandlung nicht eingebracht werden, wenn sie aber dennoch vorgebracht werden, dann bedarf es zur Geltendmachung des relativen Nichtigkeitsgrundes (§ 281 Abs. 1 Z 3 StPO) einer nachteiligen Auswirkung dieses Beweismittels auf das Urteil. Problematisch erscheint, dass es durchaus vorkommen kann, dass ein Urteil zwar – formal einwandfrei – nur auf eine belastende Zeugenaussage gestützt wird, ein unzulässiger Weise vorgekommenes weiteres Beweismittel aber stillschweigend den Ausschlag für den Schuldspruch des Angeklagten gegeben hat.[39] In diesem Fall wird eine

[39] Siehe dazu OGH 02.12.1998, 14 Os 62/98.

Rüge der Nichtigkeit keinen Erfolg haben. Besonders problematisch ist das beim Geschworenenverfahren, da der Schuldspruch im Urteil nicht begründet werden muss.

Positiv anzumerken ist, dass § 136a StPO zu den Verwertungsverboten in § 140 Abs. 1 Z 4 StPO aufgenommen wurde. Wie in den oben genannten Fällen kann das Verwertungsverbot in Verbindung mit dem relativen Nichtigkeitsgrund aber einfach ad absurdum geführt werden.

12. *In § 144 Abs. 3 und in § 145 Abs. 3 wird die Wendung* „des § 135 Abs. 2 bis 3 sowie § 136 Abs. 1 Z 2 und 3“ *durch die Wendung* „der §§ 135 Abs. 2 und 3, 136 Abs. 1 Z 2 und 3 sowie 136a“ *ersetzt.*

13. *In § 145 wird nach Abs. 3 folgender Abs. 4 eingefügt:*

„(4) Während der Durchführung einer Überwachung nach § 136a ist durch geeignete Protokollierung sicherzustellen, dass jeder Zugang zu dem Computersystem und jede nachträgliche Veränderung daran nachvollzogen werden können. Dazu sind die erforderlichen Sicherungskopien herzustellen und die Ergebnisse der Ermittlungsmaßnahme so zu speichern, dass deren Vorführung in einem allgemein gebräuchlichen Dateiformat möglich ist. Nach der Beendigung einer Überwachung nach § 136a ist dafür zu sorgen, dass Vorrichtungen, die der Überwachung dienten, entfernt oder diese funktionsunfähig werden (§ 136a Abs. 3).“

Kommentar zu Z 13:

Laut den Materialien[40] muss technisch gewährleistet werden, dass bei Durchführung der Überwachung keine Dateien des überwachten Computersystems kompromittiert werden, um nicht auf Probleme bei der Beweisverwertung zu stoßen. Dass eine diesbezügliche Gewährleistung technisch äußerst schwierig, wenn nicht unmöglich ist, ist der Tatsache geschuldet, dass auch kaum eine zulässige von einer unzulässigen Datenermittlung getrennt werden kann. Des Weiteren garantieren die in den Materialien vorgesehenen Prüfsummen weder Authentizität noch Vertraulichkeit der ausgeleiteten Daten. Prüfsummen garantieren lediglich die technische Integrität der Daten, das heißt sie dokumentieren die Abwesenheit von technischen Übertragungsfehlern, erlauben aber keine Aussage über die Herkunft der übermittelten Daten. Somit kann die für einen Beweis in einem Gerichtsverfahren notwendige Authentizität eines Datenbestandes nicht nachgewiesen werden.

Die konkrete Ausgestaltung der technischen und organisatorischen Abwicklung der Überwachung soll laut den Materialien[41] in die Zuständigkeit des Bundesministeriums für Inneres fallen. Im Gesetz findet sich keine Ermächtigung zu einer

[40] 192/ME XXV. GP Erläuterungen S 6.
[41] 192/ME XXV. GP Erläuterungen S 6.

Durchführungsverordnung. Durch diesen lapidaren Verweis in den Erläuternden Bemerkungen wird weder dem allgemeinen Determinierungsgebot gemäß Art 18 B-VG entsprochen noch genügt er rechtsstaatlichen Anforderungen an die gesetzliche Grundlage bei Grundrechtseingriffen. Die genaue technische Umsetzung ist jedenfalls relevant für die Beurteilung der Verhältnismäßigkeit der Ermittlungsmaßnahme.

Das Erfordernis Sicherheitskopien herzustellen, ist mehrdeutig. Es kann auch so verstanden werden, dass Sicherungskopien aller auf dem Computersystem gespeicherten Daten herzustellen sind, denn dies wäre eine geeignete Maßnahme um "jede nachträgliche Veränderung daran" nachzuvollziehen. Die Verwertung und Löschung einer derartigen Sicherungskopie bleibt ungeregelt. Die Verwertung einer derartigen Sicherungskopie würde zudem einer uneingeschränkten "Online-Durchsuchung" entsprechen.

14. In § 147 Abs. 1 wird nach der Z 3 folgende Z 3a eingefügt:

„3a. einer Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, nach § 136a,“

15. In § 147 Abs. 2 lautet der vierte Satz:

„Eine Ermächtigung zu einem Antrag auf Bewilligung einer Überwachung nach § 136 Abs. 1 Z 3 in den ausschließlich der Berufsausübung gewidmeten Räumen einer der in § 157 Abs. 1 Z 2 bis 4 erwähnten Personen oder einer Ermittlungsmaßnahme nach § 136a darf der Rechtsschutzbeauftragte nur erteilen, wenn besonders schwerwiegende Gründe vorliegen, die diesen Eingriff verhältnismäßig erscheinen lassen.“

16. In § 147 wird nach Abs. 3 folgender Abs. 3a eingefügt:

„(3a) Dem Rechtsschutzbeauftragten ist jederzeit Gelegenheit zu geben, sich von der Durchführung der Ermittlungsmaßnahme einen persönlichen Eindruck zu verschaffen; dazu steht ihm die Einsicht in alle Akten, Unterlagen und Daten offen, die der Dokumentation der Durchführung dienen. Gleiches gilt für die Ergebnisse der Ermittlungsmaßnahme. Er kann zu diesem Zweck nach Maßgabe der §§ 126 und 127 auch die Beiziehung eines Sachverständigen verlangen. Der Rechtsschutzbeauftragte hat insbesondere darauf zu achten, dass während der Durchführung Anordnung und gerichtliche Bewilligung nicht überschritten werden und die Ermittlungsmaßnahme nur solange durchgeführt wird, als die Verhältnismäßigkeit gewahrt ist.“

17. In § 148 lautet der erste Satz:

„Der Bund haftet für vermögensrechtliche Nachteile, die durch die Durchführung einer Überwachung von Personen nach §136 Abs. 1 Z3, einer Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, nach § 136a oder eines Datenabgleichs nach § 141 entstanden sind.“

Kommentar zu Z 17:

In der Wirkungsfolgenabschätzung finden sich keine Abwägungen zu etwaigen Kosten, die durch eine Haftung für Schäden durch den Einsatz der Überwachungssoftware an Computersystemen entstehen können.

18. In § 514 wird nach dem Abs. 31 folgender Abs. 32 angefügt:

„(32) §§ 134 Z 4a und 5, 136a und 137 Abs. 1 und 3, 138 Abs. 1 und 5, 140 Abs. 1 Z 4, 144 Abs. 3, 145 Abs. 3 und 4, 147 Abs. 1, 2 und 3a, 148 in der Fassung des Bundesgesetzes BGBl. I Nr. xx/xxxx treten mit 1. Jänner 2017 in

Kraft.“

Artikel 2 Änderung des Staatsanwaltschaftsgesetzes

Das Staatsanwaltschaftsgesetz, BGBl. Nr. 164/1986, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 96/2015, wird wie folgt geändert:

/. *In § 10a Abs. 1 wird nach dem Zitat* „§ 136 Abs. 1 Z2 und 3 StPO“ *die Wendung* „, einer Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, nach § 136a Abs. 1 StPO“ *eingefügt.*

2. In § 10a Abs. 2 wird nach dem Zitat „§ 136 StPO“ *die Wendung* „, eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, nach § 136a StPO“ *und in Abs. 2 Z1 nach der Wendung* „optische oder akustische Überwachung von Personen“ *die Wendung* „, die Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden,“ *eingefügt.*

3. In § 42 wird nach Abs. 19 folgender Abs. 20 angefügt:

„(20) § 10a Abs. 1 und 2 in der Fassung des Bundesgesetzes xx/xxxx tritt mit 1. Jänner 2017 in Kraft.“

Kommentar zu Z 1 bis 3:

Begrüßenswert ist, dass § 136a StPO in die Liste für Berichte an die Oberstaatsanwaltschaften über besondere Ermittlungsmaßnahmen aufgenommen wurde. Allerdings können diese Berichtspflichten die zahlreichen technischen Ungereimtheiten (unklare Trennung von zulässiger und unzulässiger Ermittlung von Dateiinhalten; keine Audit-Möglichkeit bei nicht-offenem Quellcode etc.) und die bestehenden Rechtsschutzdefizite keinesfalls aufwiegen.

IV. Conclusio

A. Rechtspolitische Überlegungen

I. In einer freiheitlichen, sozialen und rechtsstaatlichen Demokratie, die die Freiheit und Würde des Menschen zu ihrem Höchstwert erhoben hat, trägt der demokratisch legitimierte Gesetzgeber die Verantwortung für einen gerechten Ausgleich zwischen Freiheit und Sicherheit. Diese Abwägung unterliegt der nachprüfenden verfassungsgerichtlichen Kontrolle. Gerade in der gegenwärtigen Situation kurz nach den Terroranschlägen in Brüssel wäre der Gesetzgeber gut beraten, nicht in den weltweiten Tenor des Rufs nach immer weitergehenden Überwachungsbefugnissen der Sicherheitsbehörden einzustimmen und unsere hart erkämpften Grundrechte immer mehr einzuschränken. Ziel des internationalen und insbesondere islamistischen Terrors ist es, die rechtsstaatlichen Demokratien westlicher Prägung zu zerstören. Ob die Attentäter ihr Ziel letztlich erreichen, hängt auch davon ab, ob wir uns einschüchtern

und uns unsere Freiheiten nehmen lassen. In seinem Urteil zur Vorratsdatenspeicherung hält der Europäische Gerichtshof unter Anderem fest, dass gemäß Art 6 EU-Grundrechtecharta jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat. Die Intention vieler jüngerer Überwachungsgesetze in der Europäischen Union ist es, für mehr innere und äußere Sicherheit zu sorgen, erreicht wird aber das Gegenteil, nämlich eine Verunsicherung der Bürger und eine Einschränkung unserer Freiheit.

Nach den Anschlägen in Brüssel hat sich wieder einmal gezeigt, dass die Anschläge deshalb nicht verhindert werden konnten, weil es zum Teil zu einem Systemversagen[42] der Ermittlungsbehörden und zum Teil zu menschlichem Versagen gekommen ist, nicht aber weil es an Daten und Ermittlungsergebnissen gefehlt hätte oder die Täter verschlüsselt kommuniziert hätten. In den Erläuterungen des vorliegenden Gesetzesentwurfes wird die Einführung eines Bundestrojaners damit argumentiert, die Attentäter von Paris im November 2015 hätten über Spielekonsolen miteinander kommuniziert. Diese Behauptung hat sich bereits im letzten November als Falschmeldung erwiesen.

[42] Der Spiegel Online vom 30.03.2016, abrufbar unter http://www.spiegel.de/netzwelt/netzpolitik/sascha-lobo-ueber-is-terror-ueberwachung-ist-die-falsche-antwort-a-1084629.html -spRedirectedFrom=www&referrrer=https://t.co/pgb5sEY4vm.

Umso wichtiger ist eine Evaluierung der bestehenden Befugnisse und Möglichkeiten zur Terrorbekämpfung, bevor man neue Überwachungsmethoden gesetzlich normiert. Nicht vergessen werden darf dabei, dass sich die geplante neue Ermittlungsmethode zu einem "Sicherheitsbumerang" entwickeln könnte. Einerseits können erhebliche Gefahren für die öffentliche Sicherheit entstehen, wenn Überwachte den Einsatz der Überwachungssoftware erkennen und die Ermittler auf falsche Fährten locken, um vom tatsächlich geplanten Vorhaben abzulenken, andererseits wird durch die Nichtschließung von kritischen Sicherheitslücken in Computersystemen die gesamte IT-Sicherheit in Österreich gefährdet.

II. Bei jeder Regelung von Online-Durchsuchung bzw. -Überwachung ist zu bedenken, dass die geheime Überwachung von Computersystemen ein besonders schwerwiegender Eingriff in die Privatsphäre ist. Denn diese Zwangsmaßnahme betrifft nicht nur jene Gedanken von Menschen, die diese nach außen hin mitteilen und insofern (willentlich) preisgeben, sondern sie erfasst auch die innere Gedankenwelt der überwachten Person, die bloß auf einem privaten Gerät aufgezeichnet ist – nur persönlich zugänglich, eventuell passwortgesichert und damit in der Vorstellung besonders geschützter Intimität. Oft wird eine verfasste Nachricht, deren Inhalt überwacht (z.B.: durch den Einsatz eines Software-Keyloggers) und an das Kontrollsystem übermittelt wird, aber vielleicht gar nicht vom Betroffenen abgesendet. Andererseits werden sehr private Gedanken häufig unversehens zu übermittelter Kommunikation, wenn E-Mails zu Notizzwecken an die eigene Adresse geschickt oder als Entwurf gespeichert werden (bei Verwendung des IMAP-Services oder bei Webmail-Anwendungen erfolgt auch dann eine Übermittlung durch Synchronisation an den Mail-Server). In diesem Fall befindet man sich im problematischen Bereich der "Gedankenpolizei", also der Kontrolle von Gedanken des höchstpersönlichen Bereichs, die nie für die Außenwelt bestimmt waren.

Der bloße Hinweis[43], dass der Einsatz von Überwachungssoftware wegen des derzeit damit verbundenen hohen technischen Aufwandes faktisch nur in seltenen Ausnahmefällen und ebenso wie die optische und akustische Überwachung von Personen (sogenannter "Lauschangriff") nur sehr maßvoll angewendet werden wird, kann rechtsstaatlichen Grundsätzen nicht genügen.

Zu überlegen ist die Schaffung eines rechtlichen Rahmens für die Nutzung von „Lawful Intercept“ Schnittstellen mit den entsprechenden Kontrollmechanismen auch für Anbieter von Kommunikationssoftware, um die Möglichkeit zu haben, Verdächtige gezielt zu überwachen und so schwerwiegende und unverhältnismäßige Grundrechtseingriffe zu vermeiden. Für den in den Materialien oft zitierten Kommunikationsdienst Skype wird die Existenz einer solchen Schnittstelle nicht nur vermutet[44], belegt sind für Österreich 109 Anfragen von Sicherheitsbehörden im Jahr 2015 (Micosoft Transparency Hub – Law Enforcement Requests Report)[45]. Dabei soll der Client eines bestimmten Nutzers von der Client-seitigen Verschlüsselung ohne Kenntnis des Betroffenen auf die Server-seitige Verschlüsselung umgestellt werden, um die Erfassung eines unverschlüsselten Datenstroms zu ermöglichen. Dass ein solcher Rechtsrahmen eine Herausforderung, vor allem im Hinblick auf die Existenz verschiedenster Unternehmen mit Sitz in unterschiedlichen Ländern, darstellt, liegt auf der Hand. Andererseits eröffnen sich für Kriminelle zahlreiche Möglichkeiten, der Überwachung von Nachrichten, die im Wege eines Computersystems übertragen werden, zu entgehen, sodass man diesen Weg trotzdem in Betracht ziehen muss. Eine echte "end-to-end-encrypted" Kommunikation soll aber auch gar nicht verhindert werden. Eine funktionierende rechtsstaatliche Demokratie wird damit umgehen können, vor allem, weil solche Technologien zum überwiegenden Teil für nicht kriminelle Zwecke verwendet[46] werden und nicht nur für das Funktionieren des Wirtschaftsstandorts Österreich, sondern auch für die Wahrnehmung von Grundrechten unerlässlich sind

[43] 192/ME XXV. GP Erläuterungen, S 3.
[44] http://news.softpedia.com/news/Skype-Provided-Backdoor-Access-to-the-NSA-Before-Microsoft-Takeover-NYT-362384.shtml oder http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html.
[45] https://www.microsoft.com/about/csr/transparencyhub/lerr/.
[46] Die Möglichkeit vertraulich zu kommunizieren, ist elementar unter anderem für Journalisten, Rechtsanwälte und Unternehmer.

(Ausübung des Rechts auf freie Meinungsäußerung, Fernmeldegeheimnis, Kommunikationsgeheimnis).

III. Auch wenn das vorgeschlagene Gesetz in seiner Gesamtheit abzulehnen ist, soll darauf hingewiesen werden, dass es unerlässlich ist, die materiellen Eingriffsvoraussetzungen im Gesetz möglichst präzise zu formulieren.

Dieses Bemühen stößt jedoch an Grenzen, wenn man die Überwachung – wie etwa die Überwachung von Nachrichten (vgl. § 135 Abs. 3 Z 3 StPO) – auch bei bloßem Verdacht einer kriminellen Organisation (§ 278a StGB) oder zur Verhinderung von im Rahmen einer solchen Organisation geplanten Straftaten zulassen will. Denn dann lässt man den Verdacht der Planung eines Delikts oder den Verdacht einer Vorbereitungshandlung genügen, also den bloßen Verdacht eines Geschehens (wenn überhaupt ein konkretes „Geschehen“ ausgemacht werden kann), das weit ins Vorfeld der eigentlichen Rechtsgutsschädigung vorverlagert ist. Außer (vermutete) Absichten des „Verdächtigen“ und seinen Gedanken hat man kaum ein reales Substrat zur Hand, an das man die Verdachtsprüfung anknüpfen könnte. Es ist daher unabdingbar, besonders wirksame Sicherungs- und Rechtsschutzmaßnahmen vorzusehen. Diese sollten zumindest umfassen:

1. Die geheime Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, sollte von einem Richtersenat angeordnet werden. Die Genehmigung durch den (bisweilen jungen und unerfahrenen) Haft- und Rechtsschutzrichter kann nicht genügen. Zu denken ist hier an das "Ratskammer-Modell" der alten StPO. Besagte Ratskammer war als Kontroll- und Überwachungsorgan eingerichtet, dem die Gewährleistung der gesetzmäßigen Vorgangsweise im Rahmen des früheren strafgerichtlichen Strafverfahrens zukam und das die Gefahren, die für die Betroffenen in einem geheim geführten Verfahren eintreten konnten, beherrschen sollte. Der Ratskammer oblag unter anderem die Anordnung sowohl der Telekommunikationsüberwachung, der optischen und akustischen Überwachung von Personen unter Verwendung technischer Mittel (sogenannter "Lausch- und Spähangriff")

als auch des automationsunterstützten Datenabgleichs. Gerade in so sensiblen Bereichen, wo sehr eingriffsintensive Ermittlungsmaßnahmen angeordnet werden sollen, wäre eine Senatsentscheidung wünschenswert um die Qualität und Maßhaltigkeit der Entscheidung zu sichern.

2. Die Kontrolle durch den Rechtsschutzbeauftragten sollte ausgebaut und verbessert werden. Dieser sollte im aktiven Berufsleben stehen und auch nach Maßgabe seiner bisherigen Berufslaufbahn unabhängig sein, vorzugsweise ein Rechtsanwalt oder ein Universitätslehrer im aktiven Dienst. Er sollte – selbstverständlich bei strikter Pflicht zur Geheimhaltung – den gesetzlichen Auftrag erhalten, vor allem die Rechte der Betroffenen zu wahren, die von den geheimen Maßnahmen nichts wissen und darum ihre Rechte nicht geltend machen können. Hegt man Bedenken, dass ein solcher Rechtsschutzbeauftragter zu viel Macht haben könnte, so ist darauf hinzuweisen, dass er allein keine Entscheidungen treffen soll, sondern – gleichsam als ein Abwesenheitskurator im Auftrag der Öffentlichkeit – die Kontradiktorietät im geheimen Ermittlungsverfahren wahrt (audiatur et altera pars).

3. Die Entscheidungen zu den geheimen Überwachungen (Beschlüsse, Anordnungen, Rechtsmittelentscheidungen) sind nach Beendigung der Maßnahme, jedenfalls aber nach Ablauf eines bestimmten fixen Zeitraumes ab ihrer Erlassung, anonymisiert zu veröffentlichen. Sie wären damit insbesondere der wissenschaftlichen Öffentlichkeit zugänglich, die sie diskutieren und evaluieren könnte."[47]

4. Obligatorische nachträgliche Überprüfung der Ermittlungsmaßnahme nach einem Jahr.

[47] Interministerielle Arbeitsgruppe BMJ/BMI, Online-Durchsuchung (2008) 34ff.

B. Fehlende Wirkungsfolgenabschätzung

Auf den ersten Blick erscheint es erfreulich, dass dem Gesetzesvorschlag eine „wirkungsorientierte Folgenabschätzung“ (WFA) zugrunde liegt. Bei Betrachtung des Inhalts der WFA zeigt sich jedoch, dass sich diese wieder einmal darauf beschränkt, die Folgen für den Bundeshaushalt zu beschreiben (Kosten der Software-Lizenzen und Anschaffung von Hardware). Eine Folgenabschätzung im Hinblick auf die erwarteten Auswirkungen auf die Sicherheitslage und die Aufklärungsarbeit im Rahmen gerichtlicher Strafverfahren nach der Strafprozessordnung, auf die Kriminalitätsentwicklung und die Aufklärungs- sowie die Präventionsstatistik fehlt ebenso wie eine Einschätzung der Auswirkungen auf die Grundrechte der in Österreich lebenden Menschen und auf die Gesellschaft insgesamt.

Der einzige Grundrechtsbezug findet sich in der Aussage, dass die optische und akustische Überwachung - im Gegensatz zu der geplanten Ermittlungsmethode - einen weitaus schwereren Grundrechtseingriff für den Betroffenen darstellt.[48] Darüber hinaus ist diese Aussage schlichtweg falsch, nachdem die Überwachung von Nachrichten, die im Wege eines Computersystems übertragen werden, einen der intimsten Bereiche der Privatsphäre (höchstpersönliche Gedanken) betrifft und somit mindestens einen ebenso schweren Grundrechtseingriff bedeutet. Die neue Ermittlungsmaßnahme soll den gleichen Anwendungsbereich haben wie die optische und akustische Überwachung, wobei nicht vergessen werden darf, dass eine Ausweitung der Ermittlungsmaßnahmen mit rechtsstaatlichen Grundsätzen nur vereinbar ist, wenn sie behutsam erfolgt und gleichzeitig den mit den Maßnahmen verbundenen Gefahren ausreichend gegengesteuert wird. Die Kritik, dass die optische und akustische Überwachung von Personen weder von einem Richtergremium genehmigt werden muss, noch, dass eine zeitliche Höchstdauer gesetzlich vorgegeben ist, gilt auch hier.

Die Bezeichnung als „wirkungsorientierte Folgenabschätzung“ ist im Hinblick auf das vorliegende Dokument geradezu irreführend. Die Problemanalyse verzichtet auf jegliche Art von Statistik, Fallzahlen, konkrete Fallbeispiele oder dokumentierte konkrete

[48] Vorblatt zum Begutachtungsentwurf, WFA S 3.

Erfahrungen, welche die Notwendigkeit von Änderungen und die Einführung neuer und erweiterter Befugnisse objektiv nachvollziehbar werden lassen. Die Notwendigkeit der Änderungen bzw. Neuerungen wird postuliert aber nicht begründet. An dieser Stelle sei daran erinnert, dass sowohl der Europäische Gerichtshof als auch der Österreichische Verfassungsgerichtshof in der Verhandlung zur Aufhebung der Vorratsdatenspeicherung durch die Fragen der Richterinnen und Richter besonders hervorgehoben haben, dass den rechtspolitischen Entscheidungen zur rechtlichen Ausführung der Vorratsdatenspeicherung kein objektiviertes Datenmaterial zugrunde gelegt worden sei und, dass auch die Evaluierung keine Einschätzung des Nutzens im Hinblick auf die vorgegebenen Ziele der Bekämpfung von Terrorismus und schwerer (organisierter) Kriminalität zulasse. In den Grundrechten, insbesondere der Europäischen Menschenrechtskonvention, die einen wichtigen Teil unseres Grundrechtekatalogs ausmacht, zieht sich ein Prinzip klar durch: Die Rechtfertigungslast für Grundrechtseingriffe liegt beim Staat und nicht auf Seiten der Menschen, die den Eingriff in ihre Grundrechte für ungerechtfertigt halten. Die „Wer nichts zu verbergen hat, hat auch nichts zu befürchten"-Doktrin pervertiert diesen liberalen Abwehrcharakter unserer Grundrechte ins Gegenteil und verdächtigt alle, die eine Sphäre ohne staatlichen Einblick als verfassungsrechtlich geschützten Grundzustand reklamieren.

Das deutsche Bundesverfassungsgericht hat in dessen Urteil zur Aufhebung der deutschen nationalen Umsetzung der Vorratsdatenspeicherung den Gedanken ausgeführt, dass eine staatliche Überwachungsmaßnahme bzw. deren Verhältnismäßigkeit nur beurteilt werden kann, wenn man diese in Zusammenschau mit anderen, bereits bestehenden Befugnissen betrachtet. Durch die Summe aller Eingriffe könne sich ergeben, dass der Spielraum des Gesetzgebers zur Normierung neuer Befugnisse enger wird. Damit beschreibt das deutsche Bundesverfassungsgericht im Prinzip die Notwendigkeit einer „Überwachungs-Gesamtrechnung". In eben diesem Geiste steht das AKVorrat Projekt HEAT (Handlungskatalog zur Evaluierung der Anti-Terror Gesetze in Österreich), welches zur Hälfte von der Internet Privatstiftung Austria (IPA) im Rahmen der „NetIdee"-Förderung finanziert wird und in diesem Zusammenhang

Ende 2014 auch den „Privacy Award“ gewonnen hat. Das Ergebnis des Projekts ist eine Handlungsanleitung, gewissermaßen ein „Pflichtenheft“ zur Evaluierung bestehender wie auch neu vorgeschlagener Gesetze, die Überwachungsbefugnisse mit dem Ziel der Bekämpfung organisierter Kriminalität oder von Terrorismus normieren. Das Projekt HEAT enthält einen Vorschlag für die Objekte einer notwendigen Evaluierung im Sinne der „Überwachungsgesamtrechnung“, Vorschläge zu den Methoden, Zielsetzungen, Handlungsalternativen der Politik und vor allem Vorschläge für die Kriterien, nach denen eine Evaluierung vorzunehmen ist. Gefolgt wird dabei im Wesentlichen den *Leitlinien zur Folgenabschätzung*, Europäische Kommission, SEK(2009) 92, ergänzt durch die Vorgaben des Bundeskanzleramts für alle legistischen Projekte als Österreichisches Handbuch „Bessere Rechtsetzung“, *Hable, Kunnert, Pürgy,* Bundeskanzleramt (Hrsg)*,* Wien 2008. Die dort praxisbezogen und einfach beschriebene Systematik und die Kriterien sollten schon längst die Standardprozedur für jedes konkrete legistische Vorhaben sein, insbesondere wenn dieses mit schwerwiegenden und breit gestreuten Grundrechtseingriffen verbunden ist, also bei "eingriffsnahen Gesetzen". Die vorliegende „wirkungsorientierte Folgenabschätzung“ ist ohne jeden Zweifel nicht auf Basis der systematischen Vorgaben von EU Kommission und Bundeskanzleramt entstanden.

Unumgänglich ist jedenfalls eine echte öffentliche und parlamentarische Debatte im Begutachtungsprozess über die Notwendigkeit der vorgeschlagenen neuen Ermittlungsmaßnahme. Im Gesetzgebungsverfahren zum Polizeilichen Staatsschutzgesetz (das auch neue Überwachungsbefugnisse normiert) konnte man sich des Eindrucks nicht verwehren, dass der erste Entwurf schon in Stein gemeißelt war und auf die berechtigte und sachlich begründete Kritik aus der Zivilgesellschaft nicht oder nur mit kosmetischen Änderungen reagiert wurde. Insbesondere bei so heiklen Gesetzesvorstößen muss das Parlament seine Rolle als Gesetzgeber und Vertretung der Bevölkerung und ihrer Grundrechte auch gegenüber der Regierung wahrnehmen.