DIE ÖSTERREICHISCHEN RECHTSANWÄLTE

Bundesministerium für Justiz
Museumstraße 7
1070 Wien

per E-Mail: team.s@bmj.gv.at

Zl. 13/1 16/55

BMJ-S430.010/0001-IV 3/2016
BG, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden

Referent: VP Dr. Elisabeth Rech, Rechtsanwalt in Wien

Sehr geehrte Damen und Herren!

Der Österreichische Rechtsanwaltskammertag (ÖRAK) dankt für die Übersendung des Entwurfes und erstattet dazu folgende

S t e l l u n g n a h m e :

I. Vorwort

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 in die StPO einzuführen.

In den Erläuterungen heißt es dazu: *Zur Ermöglichung einer wirksamen Strafverfolgung unter größtmöglicher Wahrung der Grundrechte und der Verhältnismäßigkeit ist daher die Einführung einer neuen Ermittlungsmaßnahme zur Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, notwendig. Sie soll jedoch auf den Bereich schwerste Kriminalität (organisierte Kriminalität und Terrorismus) beschränkt werden.*

Durch die vorgeschlagenen Ermächtigungen zu Ermittlungsmaßnahmen wird ganz wesentlich in das verfassungsrechtlich geschützte Recht des Telekommunikationsgeheimnisses eingegriffen (Art 8 EMRK, vgl *Grabenwarter,* Europäische Menschenrechtskonvention § 22 Rz 10). Umso wichtiger ist es, dass diese Eingriffsermächtigungen dem – gerade in der Strafrechtspflege zentralen – Grundsatz der Bestimmtheit und der Verhältnismäßigkeit entsprechen (*Wiederin* in *Fuchs/Ratz*, WK StPO § 5 Rz 18ff).

Für die österreichische Rechtsanwaltschaft sprechen zahlreiche Kritikpunkte gegen die geplante neue Ermittlungsmethode in Form der Online-Überwachung.

II. Einzelne Kritikpunkte

1.) Wirkungsfolgenabschätzung und Evaluierung

Außer Zweifel steht, dass die geplanten Normen gravierende Grundrechtseingriffe bedingen. Dennoch erfolgte weder eine grundrechtliche Wirkungsfolgenabschätzung noch eine Evaluierung schon bestehender Maßnahmen.

Zwar findet sich ab Seite 2 des Vorblattes ein Kapitel mit der Überschrift „wirkungsorientierte Folgenabschätzung“ - tatsächlich abgeschätzt wurden jedoch lediglich die finanziellen Auswirkungen durch Anschaffung von Software und Lizenzgebühren. Eine sicherheitspolitische und grundrechtliche Abschätzung erfolgte ebenso wenig wie eine solche in Richtung von Prävention und Aufklärung.

Eine Evaluierung sämtlicher Überwachungsmaßnahmen seit 2002 wird seit Jahren von der Rechtsanwaltschaft gefordert. Sie wurde jedoch bis dato nicht durchgeführt, obwohl man annehmen sollte, dass das in einem Rechtsstaat bei Normen, die derart in die Privatsphäre und die Grundrechte der Bevölkerung eingreifen, selbstverständlich ist. Stattdessen wird Jahr für Jahr die Überwachung der Bürger verschärft.

2.) Zeitpunkt

Kritikwürdig ist auch der Zeitpunkt, an dem der Gesetzesentwurf in Begutachtung geht. Es ist nicht das erste Mal, dass ein Zeitpunkt gewählt wird, der unmittelbar nach einem Terroranschlag liegt. In diesem Fall nur wenige Tage nach den Attentaten von Brüssel Ende März 2016. Dadurch entsteht der Anschein, die Regierung würde die Angst der Bevölkerung dazu nutzen, missliebige Maßnahmen, die anderenfalls keine Mehrheit bekämen, durchzusetzen und, dass diese Maßnahmen nicht auf objektiv fundierten Überlegungen, die überzeugend kommuniziert werden können, beruhen. Das macht misstrauisch gegenüber der geplanten Maßnahme und auch gegenüber jenen, die sie propagieren und für unbedingt notwendig erklären.

3.) Verhältnismäßigkeit

Im Fall von grundrechtsintensiven Eingriffen ist die Verhältnismäßigkeit der Maßnahme zu prüfen. Jede staatliche Maßnahme, die in Grundrechte eingreift, muss geeignet, erforderlich und angemessen sein.

Zur Eignung wird auf die Ausführungen im nächsten Punkt „Meinung technischer Experten“ verwiesen. Nach dieser Meinung lässt der aktuelle Stand der Technik eine treffsichere, schadlose und zuverlässige Anwendung nicht zu. Außerdem könne trotz Überwachungssoftware dennoch verschlüsselt kommuniziert werden. Die Geeignetheit ist somit sehr zweifelhaft.

Zur Erforderlichkeit sei aus dem Schlussbericht der Arbeitsgruppe zur Online-Durchsuchung zitiert: *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 oder ähnliche Möglichkeiten, die die Rechtsordnung schon jetzt bieten, nicht ausreichen, um das Ziel der Strafverfolgung und der Beweissicherung zu erreichen.*

Eine vergleichbare Möglichkeit wie die jetzt geplante existiert bereits, nämlich die optische und akustische Überwachung gemäß § 136 Abs 1 Z 3 StPO. Sie ist an dieselben Voraussetzungen gebunden, setzt damit unter anderem auch einen dringenden Tatverdacht voraus. Die Erläuterungen erachten den schweren Lauschangriff als den weitaus schwereren im Vergleich zu der jetzt geplanten Maßnahme. Dies entspricht nicht der Meinung der Rechtsanwaltschaft. Die Online-Überwachung dringt zumindest gleich weit in die Privatsphäre des Betroffenen und allfälliger Dritter ein.

Nach den Erläuterungen kam es 2012 in zwei und 2013 in drei Verfahren zu einem großen Späh- und Lauschangriff. Eine Evaluierung oder zumindest entsprechende Ausführungen, inwieweit der Einsatz tatsächlich erforderlich war und welches Ergebnis er brachte (losgelöst von einem allfälligen Ausgang des Verfahrens) liegt nicht vor. Eine objektive Beurteilung, ob diese insgesamt fünf Mal in zwei Jahren überhaupt die Norm im Verhältnis zu dem dadurch verursachten Grundrechtseingriff rechtfertigen, kann daher nicht erfolgen.

Die Schätzung für die geplante Maßnahme beträgt sechs Fälle pro Jahr. Als Begründung für die Notwendigkeit wird das neue internetbasierte Kommunikationsverhalten angeführt. Konkret die Kommunikation zwischen den Paris Attentätern über Spielekonsolen. Zumindest wenn man den Informationen aus den Medien Glauben schenkt, gab es gar keine Kommunikation über Spielekonsolen. Es besteht zumindest nach Information der Rechtsanwaltschaft kein Beweis dafür, dass die Kommunikation dieser Personen internetbasiert erfolgte bzw. die Tat durch eine Online-Überwachung hätte verhindert werden können. Es ist dies daher kein Argument für die geplante Maßnahme.

Je intensiver der Grundrechtseingriff ist, umso höher muss der Maßstab für die Nachvollziehbarkeit der Argumente bei der Abwägung gegen das öffentliche Interesse sein. Unter Berücksichtigung der hohen Intensität des Grundrechtseingriffs im gegenständlichen Fall überzeugt die Abwägung nicht, weshalb auch die Angemessenheit verneint werden muss.

4.) Meinung technischer Experten

Laut Meinung technischer Experten *benötigen die Installation, der Betrieb und das Verstecken einer Überwachungssoftware solche Zugriffsrechte auf dem Zielsystem, welche dem Trojaner jede beliebige Funktionalität erlauben, inklusive das Durchsuchen, Manipulieren und Erstellen von Dateien. Es sei eine Trennung von Online- Überwachung und „Online-Durchsuchung“ nicht möglich (Verein Arbeitskreis Vorratsdaten Österreich).*

Dies widerspricht klar der Meinung des Bundesministeriums für Justiz in den Erläuterungen Seite 1, wonach sich der gegenständliche Entwurf auf eine Überwachung von im Wege des Computersystems übermittelter Nachrichten beschränke und der Annahme, es handle sich nicht um eine nach geltendem Recht unzulässige Maßnahme.

Laut Meinung technischer Experten *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. Dazu komme noch, dass die Zielgruppe sich vor diesen Maßnahmen schützen könne und es möglich sei, die Software durch ein Anti-Virus-Programm zu blockieren. Bei Erkennen könne der Betroffene außerdem die Software manipulieren. (Verein Arbeitskreis Vorratsdaten Österreich).*

5.) Divergenzen zwischen Erläuterungen und Gesetzesvorschlag

In folgenden Punkten bestehen wesentliche Divergenzen zwischen den Erläuterungen und dem Gesetzesvorschlag:

- Ziel der Überwachung sollen zunächst laut Erläuterungen Endgeräte von Benutzern internetbasierter Kommunikationsprogramme, nämlich Verdächtigen und deren Kommunikationspartner sein („*Kommunikationsinhalte auf dem von der Maßnahme betroffenen Gerät noch vor einer eventuellen Verschlüsselung*“, Erläuterungen Seite 2, 3. Absatz „*Person, gegen die sich die Überwachung richtet“,* Erläuterungen Seite 5, 5. Absatz)

Der Gesetzesvorschlag ist insoweit aber völlig offen formuliert. Dem Wortlaut folgend ist nicht ausgeschlossen, dass auch Geräte von unbeteiligten Dritten oder gar von betroffenen Kommunikationsanbietern und somit Daten, die keinesfalls für den konkreten Ermittlungszweck erforderlich sind, Ziel der Überwachung werden. Dadurch würde ein unverhältnismäßiger Eingriff in Grundrechte verwirklicht, der gemäß § 5 StPO vom Gesetzgeber ausdrücklich abgelehnt wird.

- Ausschließlich die physische Installation eines Überwachungsprogramms im Wege der unmittelbaren Bedienung eines Zielgerätes durch Ermittlungsbeamte soll zulässig sein, um die richtige Zuordnung des von der Maßnahme betroffenen Geräts zur richtigen Zielperson sicherzustellen. Die remote-Installation, damit gemeint ein Fernzugriff, soll nicht zulässig sein (Erläuterungen Seite 5, 4. Absatz).

Durch den Gesetzeswortlaut in § 134 Z 4a, wonach die Installation eines Überwachungsprogramms im Computersystem ohne Kenntnis des Inhabers zulässig sein soll, wird keineswegs die ausschließlich physische Installation sichergestellt. Auch der Fernzugriff wäre davon zweifellos umfasst, in welchem Fall eben gerade nicht sichergestellt wäre, ausschließlich das richtige Gerät zu überwachen. Das Gesetz sieht auch keine im Antrag der Ermittlungsbehörden auf gerichtliche Bewilligung vorzunehmende exakte Spezifikation der jeweiligen Ziel-Computersysteme vor, der jedoch im Sinne des § 5 Abs 2 StPO zwingend erforderlich wäre. Durch Ermittlungsermächtigungen gemäß dem aktuellen Vorschlag

wäre somit ein gemäß § 5 StPO abzulehnender, unverhältnismäßiger Eingriff in Grundrechte gemäß Art 8 EMRK verwirklicht.

- Folgt man den Erläuterungen, soll das vorgeschlagene Gesetz lediglich die Überwachung von Nachrichteninhalten sowie den damit unmittelbar verbundenen Daten wie insbesondere jene zur Identifikation der Personen der Kommunikationspartner, ermöglichen. Dies sei durch den Gesetzeswortlaut des § 136a Abs 3 sichergestellt (Erläuterungen Seite 5, 5. Absatz).

Der diesbezügliche Gesetzesvorschlag lautet, dass eine Überwachung von Nachrichten nur unter der Voraussetzung zulässig sei, dass ausschließlich jene Daten erfasst werden, die im Wege eines Computersystems übermittelt und empfangen werden, sowie jene Daten, die Rückschlüsse auf die Namen oder die sonstigen Identifizierungsmerkmale der Inhaber oder Verfügungsbefugten der ab der Nachrichtenübermittlung beteiligten Computersysteme erlauben.

Dieser Wortlaut eröffnet den Ermittlungsbehörden über die in den Erläuterungen beschriebenen Intentionen weit darüber hinausgehende Datenüberwachungsmöglichkeiten:

- Abhängig von den jeweils verwendeten Computersystemen werden Benutzerdaten mitunter in Cloudsysteme wie *dropbox, iCloud, google drive* oder *Microsoft Cloud* transferiert und dort zentral gespeichert. „*Jene Daten, die im Wege des Computersystems übermittelt werden“* im Sinne des § 136a Abs 3 Z 1 erster Satz sind daher im Ergebnis (mit Ausnahme von Anwendungsprogrammen) potentiell sämtliche auf den überwachten Computersystemen gespeicherte Daten.

- Die von § 136 Abs 3 Z 1 zweiter Satz erfassten „*Daten, die Rückschlüsse auf Namen oder Identifizierungsmerkmale der Inhaber oder Verfügungsberechtigten“* erlauben, sind (sofern diese nicht ohnehin auf Cloudspeicher transferiert und damit von § 136 Abs 3 Z 1 erster Satz erfasst sind) potentiell sämtliche auf Computersystemen gespeicherte Daten, wie zB Fotos, Videos, Steuerdokumente, private Briefe, etc. Diese Aufzählung ließe sich nach Belieben fortsetzen, den Ermittlungsbeamten stünde praktisch die „Durchforstung“ des gesamten Dateninhalts betroffener Computersysteme offen.

6.) Überwachung von Computersystemen bei Berufsgeheimnisträgern

RZ 15 sieht eine Änderung des § 147 Abs. 2 StPO vor. Demnach darf künftig die Überwachung des Computersystems bei den im § 157 Abs. 1 Z 2-4 erwähnten Personen, somit auch bei Rechtsanwälten, „nur“ dann vom Rechtsschutzbeauftragten genehmigt werden, wenn „besonders schwerwiegende Gründe vorliegen, die diesen Eingriff verhältnismäßig erscheinen lassen“.

In den Erläuterungen wird nicht näher dargelegt, was darunter zu verstehen ist und wann diese Voraussetzungen erfüllt sind. Auffallend ist jedoch, dass die im Gesetzesentwurf enthaltene Bezeichnung „besonders schwerwiegende Gründe“ in den Erläuterungen lediglich als „besondere Gründe“ formuliert ist.

Die Rechtsanwaltschaft sieht darin die Gefahr, dass in Zukunft auch Rechtsanwälte zum „Objekt der Begierde“ der Strafverfolgungsbehörden werden. Ein „besonders schwerwiegender Grund“ (RV) bzw. „besonderer Grund“ (Erläuterungen) kann wohl schon darin liegen, dass einem Tatverdächtigen schwerwiegende Tathandlungen vorgeworfen werden und die Durchführung einer Online-Durchsuchung bei seinem Rechtsanwalt aus Sicht der Strafverfolgungsbehörden ermittlungstaktisch der Erfolg versprechendste Ansatz ist, zu den angestrebten Informationen zu gelangen.

Der ÖRAK sieht in einer solchen Regelung einen ernsten Angriff auf die anwaltliche Verschwiegenheit und den Nemo-Tenetur-Grundsatz, im Ergebnis eine Umgehung des § 157 Abs. 1 Z 2 StPO.

Der ÖRAK fordert daher, die in § 157 Abs. 1 Z 2-5 genannten Berufsgeheimnisträger vom Anwendungsbereich der neuen Ermittlungsmaßnahme grundsätzlich auszunehmen.

Zudem besteht ein Widerspruch zwischen den Ausführungen in Z 12 und Z 15 des Entwurfs:

Gemäß § 144 Abs. 3 StPO neu sind Ermittlungsmaßnahmen nach §136a StPO, die sich gegen einen Rechtsanwalt richten, nur dann zulässig, wenn dieser selbst der Tat dringend verdächtig ist, da das Umgehungsverbot nach § 144 Abs. 1 StPO nur in diesem Fall nicht besteht. Nun soll § 144 Abs. 3 StPO um die Beifügung des § 136a StPO ergänzt werden, die Erteilung der Zustimmung durch den Rechtschutzbeauftragten nach § 147 Abs. 2 StPO verweist jedoch ausschließlich auf „besonders schwerwiegende Gründe“, die diesen Eingriff verhältnismäßig erscheinen lassen. Zur Klarstellung sollte daher auch in § 147 Abs. 2 StPO angeführt werden, dass die neue Ermittlungsmaßnahme nur dann zulässig ist, wenn der Berufsgeheimnisträger selbst der Tat dringend verdächtig ist und darüber hinaus besonders schwerwiegende Gründe vorliegen, die die Verhältnismäßigkeit dieser Maßnahme begründen.
Nach dem Wortlaut des Entwurfs könnte man nämlich annehmen, dass bereits die besonders schwerwiegenden Gründe alleine (ohne dringenden Tatverdacht gegen einen Rechtsanwalt) ausreichen, um bei einem Rechtsanwalt eine Online-Durchsuchung vorzunehmen.

Dies ist jedoch entschieden abzulehnen, denn eine solche Interpretation würde im Ergebnis bedeuten, dass etwa eine Hausdurchsuchung bei einem Rechtsanwalt auf Grund des § 144 Abs. 3 StPO auch den dringenden Tatverdacht voraussetzt und daher an strengere Voraussetzungen gebunden ist, als die geplante Online-Durchsuchung.

Dazu bedarf es einer Klarstellung in den Gesetzesmaterialien in diesem Punkt, welche durch folgende Ergänzung des § 147 Abs. 2, 4. Satz erfolgen könnte: „*Eine Ermächtigung zu einem Antrag auf Bewilligung […] einer Ermittlungsmaßnahme nach § 136a darf der Rechtsschutzbeauftragte nur erteilen, wenn* ***neben den Voraussetzungen des § 144 Abs. 3*** *besonders schwerwiegende Gründe vorliegen, die diesen Eingriff verhältnismäßig erscheinen lassen.“*

Anknüpfungspunkt für diese Klarstellung ist nicht die Privilegierung eines selbst dringend tatverdächtigen Rechtsanwaltes, sondern die Notwendigkeit, von ihm verwaltete Daten und an ihn erteilte Informationen zu schützen. Während nämlich bei einer Hausdurchsuchung durch § 112 StPO sichergestellt ist, dass bei einem auch selbst dringend tatverdächtigen Rechtsanwalt eine gerichtliche Entscheidung darüber ergeht, welche Unterlagen dem Berufsgeheimnis unterliegen und welche für die Ermittlungen verwendet werden dürfen, fehlt diese Rechtschutzmöglichkeit bei einer Online-Durchsuchung völlig, da den Strafverfolgungsbehörden uneingeschränkt Zugriff auf alle in der Kanzlei verwalteten Daten und Informationen eingeräumt wird. **Eine solche Vorgehensweise ist im Rechtsstaat unvorstellbar.** Die bloße Gefahr eines solchen Missbrauchs dieser Ermittlungsmaßnahmen verlangt daher die **uneingeschränkte Ausnahme des Rechtsanwaltes vom Anwendungsbereich des**
§ 136a StPO.

Denkbar wäre auch der Fall, dass sich die Ermittlungsmaßnahmen nach § 136a StPO nicht gegen den Rechtsanwalt selbst, sondern gegen einen in seiner Kanzlei tätigen Mitarbeiter richten, der über die EDV der Kanzlei (private) Kommunikation durchführt. Da die StPO in diesem Fall keine Sonderregelung enthält, könnten die Strafverfolgungsbehörden unter den im § 136a StPO normierten Voraussetzungen Nachrichten, die im Wege des Computersystems der Anwaltskanzlei übermittelt werden, überwachen. Sie hätten auf diese Weise wiederum vollständigen Zugriff auf den Datenbestand der Anwaltskanzlei, ohne dass der Rechtsanwalt selbst in den Sachverhalt involviert, geschweige denn dringend tatverdächtig ist.

Auch aus diesem Grund ist die Durchführung einer Untersuchung von Computersystemen, die der Berufsausübung dienen bzw. dieser gewidmet sind, strikt abzulehnen.

Obwohl eine Online-Durchsuchung wesentlich weiter als andere Ermittlungsmaßnahmen in die Rechtssphäre eingreift und daher auch eine erhebliche Gefahr für einen Eingriff in das anwaltliche Berufsgeheimnis darstellt, unterscheiden sich die Anforderungen betreffend dringenden Tatverdacht und Bewilligung durch den Rechtschutzbeauftragten nicht von der bloßen Überwachung der Telekommunikation, dies abgesehen von den für § 136a StPO vorausgesetzten Anlassfällen. Diese Situation ist unbefriedigend und bedeutet im Ergebnis eine Geringschätzung der anwaltlichen Verschwiegenheit.

Hinzuweisen ist auch auf die im ähnlichen Zusammenhang jüngst ergangene Entscheidung des deutschen Bundesverfassungsgerichtes (1 Bv R966/09, 1140/09) vom 20. April 2016, in welcher das Gericht über Verfassungsbeschwerden gegen vergleichbare deutsche Bestimmungen zu entscheiden hatte. Das Bundesverfassungsgericht führt ausdrücklich aus, dass die Ausgestaltung der in Rede stehenden Befugnisse dem Verhältnismäßigkeitsgrundsatz genügen muss und dass insbesondere besondere Regelungen zum Schutz von Berufsgeheimnisträgern erforderlich sind. Diese besonderen Regelungen sind in der StPO nicht auf die im Rechtsstaat erforderliche Weise enthalten.

In den Erläuterungen werden „strenge Vernichtungsregelungen“ von unzulässig ermittelten oder für die Untersuchung nicht bedeutsamen Daten erwähnt, welche im

vorgeschlagenen Gesetzestext jedoch nicht umgesetzt sind. Vielmehr werden auf der Grundlage des § 136a StPO erzielte Ergebnisse gleich behandelt wie andere Ergebnisse nach dem 5. und 6. Abschnitt des 10. Hauptstücks (§ 89 Abs. 4 StPO). Von „strengeren“ Vernichtungsregelungen kann daher keine Rede sein.

III. Conclusio

Die Österreichische Rechtsanwaltschaft spricht sich entschieden gegen die geplante Maßnahme aus.

- Der vorliegende Gesetzesentwurf ermöglicht den Ermittlungsbehörden umfangreichste Überwachungsmaßnahmen, die weit über die in den Erläuterungen dargelegten Intentionen hinausgehen. Es ist daher zu befürchten, dass die vorgeschlagene Gesetzesänderung zu unverhältnismäßigen Eingriffen in Grundrechte, insbesondere das gemäß Art 8 EMRK im Verfassungsrang geschützte Telekommunikationsgeheimnis, führen wird. **Die im vorgeschlagenen § 136a StPO enthaltene gesetzliche Ermächtigung ist aufgrund ihrer überschießenden Formulierung nicht hinreichend bestimmt und würde deshalb gegen das Verhältnismäßigkeits- und Bestimmtheitsgebot des § 5 StPO verstoßen.**

- Je Eingriff-sensibler Ermittlungsmaßnahmen sind, desto exakter müssen sie bestimmt sein, um nicht gegen Art 18 B-VG und Art 8 EMRK zu verstoßen. Im vorliegenden Gesetzesentwurf sind – in den Erläuterungen auch zugestandenermaßen – sensibelste Eingriffsmöglichkeiten vorgesehen, die vorgeschlagenen **Bestimmungen hingegen überaus unbestimmt.** Potentielle Grundrechtsverstöße sind daher evident.

  Das betrifft die Einschränkung bzw. Klarstellung im Gesetzeswortlaut, wonach expressis verbis zumindest
  - der Zugriff auf Geräte unbeteiligter Dritter und Kommunikationsanbieter,
  - der Fernzugriff, sowie
  - die Überwachung von Daten, die über die konkreten, von einem Benutzer zu einem anderen übermittelten Nachrichteninhalte hinausgehen,

  ausgeschlossen werden muss.

- Im Sinne der Bestimmung des § 5 Abs 2 StPO, die verfassungsmäßig garantierte Rechte näher konkretisiert, wäre es notwendig, die Ermittlungsbehörden zu verpflichten, die zur Überwachung beantragten Personen und Computersysteme bereits im entsprechenden Antrag an das Gericht exakt zu spezifizieren.

- Die österreichische Rechtsanwaltschaft erwartet, dass **vor einer Entscheidung über derart intensive Grundrechtseingriffe eine umfassende Wirkungsfolgenabschätzung und Evaluierung schon bestehender Maßnahmen erfolgt.**

- Ebenso erwartet die Rechtsanwaltschaft eine **klare Analyse der technischen Auswirkungen und Möglichkeiten der Online-Überwachungssoftware auch auf ihre Eignung für den beabsichtigten Zweck durch unabhängige Experten.**

- **Die Antwort zur Verhältnismäßigkeit fällt nach Meinung des ÖRAK negativ aus.** Die geplante Maßnahme scheint weder geeignet, noch erforderlich und angemessen, berücksichtigt man die hohe Eingriffsintensität in die Grundrechte der Bürger.

- **Berufsgeheimnisträger sind vom Anwendungsbereich der neuen Ermittlungsmaßnahme grundsätzlich auszunehmen.**

Und zuletzt möchte die Rechtsanwaltschaft ihr Unverständnis nicht verhehlen, dass sie der interministeriellen Arbeitsgruppe „Online-Durchsuchung“ nicht beigezogen war. Die Sorge, die Rechtsanwaltschaft sei besonders kritisch, ist berechtigt. Umso mehr schadet es dem Rechtsstaat und damit auch dem Bürger, auf diese kritische Stimme zu verzichten.

Wien, am 12. Mai 2016

DER ÖSTERREICHISCHE RECHTSANWALTSKAMMERTAG

Dr. Rupert Wolff
Präsident