Amt der Wiener Landesregierung

Magistratsdirektion der Stadt Wien
Geschäftsbereich Recht
Rathaus, Stiege 8, 2. Stock, Tür 428
1082 Wien
Tel.: +43 1 4000 82377
Fax: +43 1 4000 99 82310
E-Mail: post@md-r.wien.gv.at
www.wien.at

Bundesministerium für Justiz

Wien, 26. April 2016

MDR - 268441-2016-6
Entwurf eines Bundesgesetzes,
mit dem die Strafprozessordnung 1975
und das Staatsanwaltschaftsgesetz
geändert werden;
Begutachtung;
Stellungnahme

zu BMJ-S430.010/0001-IV-3/2016

Zu dem mit Schreiben vom 31.März 2016 übermittelten Entwurf eines Bundesgesetzes wird wie folgt Stellung genommen:

Obgleich es aus Sicht der Strafverfolgung (insbesondere angesichts der jüngsten Terrorereignisse) als nachvollziehbar erachtet wird neue Ermittlungsmethoden in Betracht zu ziehen, wird der vorliegende Entwurf weitestgehend als nicht ausreichend zielgerichtet erachtet und es wird die Verhältnismäßigkeit der Methoden in Frage gestellt.

Die Zielgerichtetheit und Verhältnismäßigkeit wird wie folgt beurteilt:

Allgemeine Bedenken:

Der Entwurf zielt im Kern vor allem darauf ab, internetbasierte Kommunikationsmöglichkeiten wie WhatsApp oder Skype im Rahmen der Strafverfolgung zu überwachen, indem entsprechende Überwachungssoftware auf dem Computersystem des Überwachten installiert werden soll und sich hierfür im Bedarfsfall Zutritt zu den Wohnungen der Verdächtigen verschaffen zu können.

Die Software WhatsApp wird grundsätzlich auf Mobiltelefonen installiert und genutzt. Obgleich es sich bei Mobiltelefonen im weitesten Sinne um Computersysteme im Sinne des § 74 Abs. 1 Z 8 StGB handeln mag, ist nicht erkennbar wie in der Praxis eine derartige Installation ohne Kenntnis des Überwachten erfolgen kann, da Mobiltelefone in aller Regel

von den Besitzern mitgeführt werden und nur in Ausnahmefällen (z. B. Vergessen) unbeaufsichtigt zurückgelassen werden. Die Überwachung von WhatsApp-Internetkommunikation erscheint durch die geplante Maßnahme nicht realisierbar.

Ähnliches gilt für die Überwachung von Kommunikation via Skype, obwohl diese Software, welche deutlich weniger genutzt wird als WhatsApp, auch auf Desktop-PCs und Laptops installiert und betrieben wird.

Zu § 136a StPO:

Es ist festzustellen, dass sich der Grundrechtseingriff nicht nur auf eine Beschränkung des Fernmelde- bzw. Kommunikationsgeheimnis, sondern auch auf die Verletzung des Hausrechts bezieht, wobei dieser Eingriff ohne Wissen des Überwachten erfolgen muss, da ansonsten der Zweck der Überwachung vereitelt würde. Die Eingriffsintensität ist nicht ohne weiteres mit der optischen und akustischen Überwachung von Personen unter Verwendung technischer Mittel gemäß § 136 Abs. 1 Z 3 StPO vergleichbar, da durch die Verletzung des Hausrechts noch unmittelbarer in die Privatsphäre der betroffenen Person eingedrungen wird. Dies vor allem dann, wenn die Überwachungsmaßnahme nicht gegenüber dem unmittelbaren Täter, sondern gegenüber einer Person angewendet wird, die mit dem Täter zwar in Kontakt steht, aber weder an der Tat beteiligt ist noch von den verbrecherischen Absichten oder Taten wusste (siehe § 136a Abs. 1 iVm § 136 Abs. 1 Z 3 und Abs. 4 des geltenden Rechts).

Die Verhältnismäßigkeit des Grundrechtseingriffs ist aber auch daran zu messen, wie zielführend die Maßnahme zur Erreichung eines den Eingriff rechtfertigenden Zwecks ist.

Diesbezüglich bestehen allerdings mehrfach Bedenken:

In den Erläuterungen wird ausgeführt, dass „ausschließlich eine Installation durch physischen Zugriff auf das Computersystem, nicht jedoch eine remote-Installation der Überwachungssoftware zulässig sein soll.“ In diesem Zusammenhang stellt sich die Frage, wie der physische Zugriff bewerkstelligt werden soll, ohne dass der Inhaber des Computersystems etwas davon bemerkt. Für darauf sensibilisierte Personen ist es ein leichtes (durch entsprechende Maßnahmen) festzustellen, ob in eine Wohnung eingedrungen wurde bzw. ein physischer Zugriff auf das Computersystem erfolgte, wodurch der Betroffene Kenntnis von der beabsichtigten Überwachung erlangt und dadurch deren Zweck vereitelt.

Da sich die Ermittlungsmaßnahme auf „eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden" beschränkt, kann ein mutmaßlicher Täter den Inhalt einer Nachricht bereits vor der Einleitung eines Übermittlungsvorgangs als Datei verschlüsseln. Die Überwachungsmaßnahme ist aber gerade darauf gerichtet, den Inhalt einer Nachricht zu ermitteln, bevor sie während eines Übermittlungsvorgangs verschlüsselt wird (sogenannte Kanalverschlüsselung).

Zum anderen könnte er die Methoden der Zwei-Faktor basierenden Ver- und Entschlüsselung, Festplattenverschlüsselung, Pre Boot Authentification, Dual Boot oder den Betrieb einer weiteren, virtuellen Maschine nutzen, um den Einsatz der Überwachungssoftware zu vereiteln.

Weiters kann ein mutmaßlicher Täter ein Endgerät verwenden, das selbst keine Daten verarbeitet, sondern die Verarbeitung auf einem zentralen Server durchführt (z. B.: Thin Client). Das Überwachungsprogramm müsste dann auf diesem Server installiert werden, auf welchem aber auch die Daten unbeteiligter Personen verarbeitet werden, gegen die sich die Überwachungsmaßnahme gar nicht richten soll. Außerdem müssten die Ermittler an den Server physisch heran kommen, welcher sich nicht zwangsläufig in Österreich oder in Europa befindet.

Schließlich könnte ein mutmaßlicher Täter auch ein öffentlich zugängliches Endgerät benützen wie beispielsweise in einer öffentlichen Bibliothek oder einem Internetcafé. Hier würde die Überwachungsmaßnahme wiederum in die Rechte unbeteiligter Personen massiv in das Grundrecht auf Eigentum eingreifen. Die Installation der Überwachungssoftware an einem derartigen Gerät widerspräche auch den Erläuterungen, welche „der eindeutigen Zuordnung des Zielsystems zur Zielperson vor und während der Maßnahme besondere Bedeutung" zumessen.

Ein weiterer Widerspruch der Erläuterungen besteht darin, dass einerseits behauptet wird, der Eingriff beschränke sich im Gegensatz zur sogenannten „Online Durchsuchung" auf „eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden", andererseits aber ein „Zugriff auf Adressbücher und Kontaktverzeichnisse" zwecks „Identifizierung des Benutzers" ermöglicht werden müsse.

Insgesamt ergeben sich viele Möglichkeiten, die angestrebte Ermittlungsmaßnahme zu vereiteln. Aufgrund der angeführten Argumente wird daher empfohlen, noch einmal abzuwägen, ob im Hinblick auf den Erfolg der geplanten gesetzlichen Maßnahmen die Eingriffe in die Grundrechte verhältnismäßig sind.

Im Zusammenhang mit den durch Berufsgeheimnis privilegierten Personen (beabsichtigter § 147 Abs. 2 vierter Satz iVm § 157 Abs. 1 Z 2 bis 4 geltendem Recht) ist anzumerken, dass die Ermittlungsmaßnahme an einem Computersystem einer öffentlichen Gebietskörperschaft nur mit vorheriger Zustimmung des zuständigen Organwalters erfolgen sollte.

Zu § 148 StPO:

Es liegt sowohl ein Widerspruch zwischen Teil I und II der Erläuterungen, als auch ein Widerspruch zwischen Gesetzestext und den Erläuterungen vor.

In den Erläuterungen ist im Teil I. Seite 2, 7. Zeile von unten wie folgt vorgesehen:
*„eine verschuldens**un**abhängige Haftung des Bundes für Schäden, die durch eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, verursacht wurd**e** (§ 148 StPO)".*

Diese Stelle der Erläuterungen ist hinsichtlich der (sinngebenden) Silbe „un" im Adjektiv „verschuldensunabhängig", bedenklich, wie im Folgenden abgeleitet wird. Eine Haftung für Schadenersatz ist im Österreichischen Recht mit ganz wenigen gesetzlichen Ausnahmen immer auch an die Prüfung der Haftungsvoraussetzung gebunden, ob nicht bloß Verursachung, sondern auch Verschulden vorlag.

Widersprüchlich dazu ist der Gesetzestext zu § 148 StPO insofern, dass in dieser Bestimmung der erste Satz wie folgt lautet: *Der Bund haftet für vermögensrechtliche Nachteile, die durch die Durchführung einer Überwachung von … etc.…entstanden sind".*

Diese Formulierung gibt keinen Anlass zu Bedenken. Gäbe es o.a. bedenkliches Adjektiv (in den Erläuterungen) nicht, bestünde auch nicht der geringste Zweifel, dass auch diese Haftung den allgemeinen Haftungsregeln des ABGB unterliegt. Die Bestimmungen des ABGB (§§ 1295 ff ABGB) sehen aber die Haftung anderer Personen für erlittene Schäden nur bei deren Verschulden vor. Ansprüche Geschädigter würden beim entwurfsgegenständlichen Szenario stets als „Amtshaftungsansprüche" gemäß AHG gelten.

Nun ist aber das ABGB auch im Bereiche des AHG unbedingt anzuwenden, wobei der Gesetzgeber in § 1 AHG auf das „bürgerliche Recht" nicht bloß „verweist", sondern extra dazu betont, dass für ein Entstehen der Haftung, die „Zufügung des Schadens schuldhaft" gewesen sein musste. Kein Wort von einer verschuldensunabhängigen Haftung findet sich auch in den

Erläuterungen Teil II. Seite 7:

Die fundamentale Polarisierung bzw. Spannung zwischen Erfolgshaftung und Verschuldenshaftung wird auch hier nicht thematisiert.

A. Gegen die verschuldensunabhängige Haftung bestehen gravierende Bedenken:

a. Die verschuldensunabhängige Schadenshaftung (Erfolgshaftung) ist im Österreichischen Recht eine absolute Randerscheinung. Erfolgshaftung ist rechtshistorisch aus Zeiten vor der „Aufklärung". Sie ist nur noch in Extrembereichen, in denen z.B. physikalische erhöhte Betriebsgefahren auftreten können (z.B. Atom, EKHG etc.) tolerierbar. Das gilt auch für Fehler auf Seiten der Rechtsträger, hinter denen ja Organwalter (natürliche Personen/Menschen), stehen.

   Bei Implantierung und Entfernung von Programmen handelt es sich ja nicht (wie bei den wenigen noch existierenden Erfolgshaftungen) um unberechenbare, erhöhte Betriebsgefahren bzw. "Naturgewalten", sondern um menschliche Programmierung, Installierung und Löschung/Unlesbarmachung von Dateien. Das sind berechenbare mathematische Prozesse und deren Bearbeitung. Dabei sind menschliche Fehler auch auf Seiten der MitarbeiterInnen (bzw. auf Seiten von MitarbeiterInnen von Polizei, Staatsanwaltschaft und Gericht beauftragter Computerunternehmen), leicht denkbar und erschienen in Ansehung eines vitalen Überwachungsanlasses, der das Potenzial hat, viele Menschenleben zu retten und die Funktionsfähigkeit demokratischer bzw. organisatorischer Strukturen zu schützen (z. B. gegen Terror), sogar um den Preis von Begleitschäden sozialverträglich.

   Für menschliche Fehler in hohen Stresssituationen wie beim Eindringen in fremde Räumlichkeiten bzw. Computersysteme, existiert im Gesetz ohnehin bereits ein extrem strenger Sorgfaltsmaßstab, eine „hohe Latte" - jene/r gemäß § 1299 ABGB.

b. Wenn im Anwendungsfall zu allen anderen Schwierigkeiten (unbemerktes Eindringen, Überwachen, unbemerktes Abbauen, Löschen, etc., dann noch (insbesondere bei älte-

ren Computersystemen) ständige Sorge vor „verschuldensunabhängiger“ Haftung dazukäme, könnten enorm wichtige Überwachungsschritte a priori unterbleiben - aus reiner Furcht vor dem Risiko der Amtshaftung, der bei Schädigung größerer Einheiten (Anzapfen einer verdächtigen kriminellen „Kommandozentrale“ in großen Bürogebäuden) ungeahnte finanzielle Ausmaße annehmen könnte. Dazu käme noch ein Ausufern des Schadens in andere Netzwerke (Problem der Eingrenzung und Identifikation des „überwachten Computersystems“).

c. Kontraproduktivität der Erfolgshaftung in Anbetracht höchstrangiger Schutzziele: Man bedenke, dass die beauftragten technischen Privatunternehmen und/oder Detekteien, dem Rechtsträger im Innenverhältnis haften und unter dem für ihren Auftraggeber verschärften Haftungsdruck wohl schon recht früh dahin tendierten, diesem von jedem tragbaren Risiko technisch abzuraten, woraufhin in der Praxis die Verantwortlichen aus Angst vor finanziellem Schaden wohl geneigt wären, in bestimmten Fällen auf die Überwachung a priori zu verzichten. Bei der Terror - bzw. Kriminalitätsbekämpfung aber sollten derlei unnötige Demotivationen wie z. B. übertriebene Furcht vor Fehlentscheidungen möglichst nicht gefördert werden.

Abschließend ist daher festzuhalten, da der Entwurf jedoch eine verschuldensabhängige Haftung vorsieht, der Entwurf durch seine Erläuterungen eine juristische Unvereinbarkeit zwischen StPO und den Bestimmungen des Amtshaftungsgesetzes provoziert. Das Adjektiv „verschuldensunabhängig“ auf Seite 2, 7. Zeile von unten der Erläuterungen kann und sollte aus den angeführten Gründen ersatzlos entfallen.

Für den Landesamtsdirektor:

Dr. Ulrich Hejsek

Mag.[a] Regina Mertz-Koller
Senatsrätin

Ergeht an:
1. Präsidium des Nationalrates

2. alle Ämter der Landesregierungen

3. Verbindungsstelle der Bundesländer

4. MA 26
mit dem Ersuchen um Weiterleitung an die einbezogenen Dienststellen