Amt der Wiener Landesregierung

Magistratsdirektion der Stadt Wien
Geschäftsbereich Recht
Rathaus, Stiege 8, 2. Stock, Tür 428
1082 Wien
Tel.: +43 1 4000 82375
Fax: +43 1 4000 99 82310
E-Mail: post@md-r.wien.gv.at
www.wien.at

Bundesministerium für Justiz

Wien, 21. August 2017

MDR - 579044-2017-9
Entwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 geändert wird (Strafgesetznovelle 2017);
Begutachtung;
Stellungnahme

zu BMJ-S578.031/0008-IV 3/2017

Zu dem mit Schreiben vom 10. Juli 2017 übermittelten Entwurf eines Bundesgesetzes wird wie folgt Stellung genommen:

Änderung der Strafprozessordnung 1975

Zu Z 4 (§ 76a Abs. 1):

Beim Amt der Wiener Landesregierung bestehen erhebliche Bedenken dagegen, dass der PUK ohne Weiteres insbesondere auch an kriminalpolizeiliche Behörden übermittelt werden soll. Der PUK ist keinesfalls mit den sonst in § 76a Abs. 1 StPO angeführten „Stammdaten“ gleichzusetzen, sondern ermöglicht dieser den Zugang zu zahlreichen und auch inhaltlichen Kommunikationsdaten der BesitzerInnen eines Endgerätes. Insoweit besteht auch ein massiver Wertungswiderspruch zur bestehenden Regelung des § 76a Abs. 2 StPO, welcher für die dort genannten Daten – die aber wesentlich weniger massive Eingriffe in die Privatsphäre einer Person als die Bekanntgabe des PUK darstellen – bereits eine staatsanwaltschaftliche Anordnung erfordern. Die Regelung ist daher weder systemkonform noch sachgerecht. Vielmehr wäre zu erwägen, ob aufgrund des möglichen massiven Eingriffes in Grundrechte der betroffenen Person nicht sogar eine richterliche Anordnung für die Herausgabe des PUK durch einen Anbieter von Kommunikationsdiensten vorzusehen wäre.

Zu Z 15 (§ 135a):

Mit dem vorliegenden Entwurf soll insbesondere erreicht werden, dass künftig auch unter Verwendung von – aufgrund deren Programmierung – speziell verschlüsselten Applikationen (wie etwa Skype oder WhatsApp) übermittelte Nachrichten von den Strafverfolgungsbehörden überwacht werden können. Vor dem Hintergrund der heutzutage üblichen standardmäßigen Verwendung solcher Applikationen im Kommunikationsverkehr ist diese Intention im Sinne einer wirksamen Strafverfolgung nachvollziehbar und daher grundsätzlich sinnvoll.

Allerdings soll dieses Ziel technologisch dadurch erreicht werden, dass auf einem Endgerät einer verdächtigen Person (remote oder durch physische Manipulation am Gerät) eine spezielle Software installiert wird, die sämtliche durch dieses Gerät übermittelten und von diesem Gerät erhaltenen Informationen (bei Datenausgang noch vor einer allfälligen Verschlüsselung und bei Dateneingang nach erfolgter Entschlüsselung) ausliest und diese den Strafverfolgungsbehörden elektronisch übermittelt. Wie auch in den Erläuterungen ausdrücklich dargelegt wird, umfasst die Überwachung daher nicht nur „Nachrichten“ im üblichen Sinn, sondern die gesamte Kommunikation des Gerätes (vgl. die entsprechenden Ausführungen zu § 134 Z 3 des Entwurfs in den Erläuterungen und den hier verwendeten Begriff der „Ausleitung des Internetdatenverkehrs“).

Es besteht jedoch ein erheblicher Unterschied, ob lediglich die konkrete verschlüsselte Nachrichtenübermittlung oder der gesamte Internet-Datenverkehr einer Person überwacht wird. Letzterer kann nämlich sehr wohl höchstpersönliche Daten umfassen (etwa Gesundheitsdaten, Bankdaten bei Online-Banking, Zugangscodes zu Websites), welche nach der vorgesehenen Regelung „lediglich“ als Nebenprodukt erhoben werden. Zu der zur Rechtfertigung dieser Regelung in den Erläuterungen unter anderem angeführten Entscheidung des deutschen Bundesverfassungsgerichtes (vgl. Seite 5, 2. Absatz) ist festzuhalten, dass heutzutage die vollumfängliche Kommunikation via elektronischer Geräte bei vielen Personen üblich ist. Oftmals werden sensible Daten nur über diese Geräte ausgetauscht und auch nur auf diesen gespeichert, weshalb bei einer in den Erläuterungen angesprochenen physischen Hausdurchsuchung oftmals weniger Informationen erhoben werden können als bei einer Überwachung des Internet-Verkehrs einer Person. Der Rückschluss, es würde sich daher bei einer Online-Überwachung um einen weniger grundrechtsrelevanten Eingriff als bei einer Hausdurchsuchung handeln, erscheint daher nur bedingt schlüssig und ist keineswegs sicher, dass die österreichischen Höchstgerichte diese Auffassung im Lichte der fortschreitenden technologischen Entwicklung teilen.

In den Erläuterungen nicht gänzlich zutreffend dargestellt wird auch das Verhältnis der mit der gegenständlichen Bestimmung beabsichtigten Überwachungsmaßnahme zu der als weithin unzulässig erachteten Online-Durchsuchung von Computersystemen. Nahezu jedes moderne Kommunikationsgerät erstellt nämlich – allenfalls sogar automatisiert – Backups des gesamten Systems (samt aller enthaltenen privaten Daten) und werden diese Backups aufgrund deren Größe regelmäßig in cloud-basierten Systemen extern abgespeichert. Ein Auslesen des gesamten Internet-Verkehrs führt daher in der Praxis sehr wohl dazu, dass somit alle auf einem Gerät gespeicherten Daten ausgelesen werden können und ist dies im Ergebnis einer Online-Durchsuchung gleichzuhalten.

Nicht nachvollziehbar sind auch die Ausführungen auf Seite 10 im zweiten Absatz der Erläuterungen, wonach hinsichtlich der vorgesehenen Bestimmung des § 135a des Entwurfs deshalb höhere Zulässigkeitsvoraussetzungen erforderlich seien, weil diese bei der Umsetzung technisch und quantitativ ressourcenaufwändiger wären. Dies erscheint schon deshalb als Zirkelschluss, weil in den Erläuterungen umfassend dargelegt wird, dass die unverschlüsselte Übermittlung von Nachrichten der verschlüsselten Übermittlung von Nachrichten gleichzusetzen ist und gerade vor diesem Hintergrund – auch von der zitierten Expertengruppe – die Zulässigkeit der Überwachung von verschlüsselten Nachrichten überhaupt erst für zulässig erachtet wird. In der Anwendung müsste die letztgenannte Argumentation dazu führen, dass die Überwachung verschlüsselter und unverschlüsselter Nachrichten unter denselben Voraussetzungen zulässig sein muss. Bei dem im Entwurf gewählten Zugang wären im Ergebnis jene kriminellen Personen besser gestellt, welche sich verschlüsselter Nachrichtendienste bedienen und ist dies wohl kaum sachgerecht. Die Regelung sollte schon aus diesem Grund dringend überdacht werden. Eine erhöhte Zulässigkeitsvoraussetzung für die Überwachung von verschlüsselten Nachrichten könnte sich allenfalls nur daraus ergeben, dass nach der vorgesehenen Regelung neben den verschlüsselten Nachrichten umfassend auch weitere – wie dargelegt äußerst sensible – Daten erhoben werden.

Schließlich ist festzuhalten, dass sich die in den Erläuterungen angesprochene Expertengruppe offenbar im Wesentlichen mit der Frage der Zulässigkeit der Überwachung auch verschlüsselter Nachrichten auseinandergesetzt und diese – nachvollziehbar – als zulässig erachtet hat. Eine klare Aussage der Expertengruppe, wonach eine umfassende Erhebung des gesamten Datenverkehrs für zulässig erachtet wird, ist den Erläuterungen nicht zu entnehmen, sondern sprechen hier einige Ausführungen (vgl. etwa Seite 8, 3. Absatz „[…] sei dieser Vorgang daher durchaus als eine Art Nachrichtenüberwachung zu werten, die sich von einer (umfassenden) Online-Überwachung abgrenzen lasse […]) sogar für die gegenteilige Annahme.

Nach dem Dafürhalten des Amtes der Wiener Landesregierung wären die einzelnen Überwachungstatbestände „Nachrichtenübermittlung mittels verschlüsselter Dienste“ und „Online-Datenverkehrsüberwachung“ zur Einhaltung des konkreten Überwachungsbedürfnisses klar zu trennen. Es wäre daher sowohl technisch als auch legistisch Vorsorge dafür zu treffen, dass ausschließlich eine Überwachung des verschlüsselten Nachrichtenverkehrs stattfindet, sofern damit im konkreten Fall das Auslangen gefunden werden kann. Damit könnte auch verhindert werden, dass Verdächtige – bei grundsätzlich gleicher Sachlage hinsichtlich eines begangenen Deliktes – je nach verwendeter Technologie überwacht werden dürfen oder nicht (vgl. dazu auch die Ausführungen im vorletzten Absatz). Wenn darüber hinaus bei verdächtigen Personen nach der Sachlage tatsächlich der gesamte Online-Datenverkehr überwacht werden soll, wäre dies gesetzlich gesondert vorzusehen und sollte eine derart weitreichende Überwachung auch weitergehende – derzeit nicht vorgesehene – Genehmigungsvoraussetzungen erfordern.

Zu Z 19 und 24 (§§ 137 Abs. 2 und § 138 Abs. 5):

Die in den Erläuterungen zu diesen Bestimmungen enthaltenen Ausführungen erscheinen grundsätzlich nachvollziehbar. Allerdings regt das Amt der Wiener Landesregierung an, hinsichtlich des Entfalls der Verständigungspflicht nach dem Inhalt der beschlagnahmten Sendung zu differenzieren. Sofern es sich, in Anlehnung an die bisherige Regelung, um

klassische Briefe handelt und sich die Person in Haft befindet, wird die Beibehaltung der bisherigen Regelung angeregt. Bei Briefsendungen anderer Personen und Paketsendungen „strafrechtsrelevanten“ Inhaltes – auf welche die Novelle erkennbar abzielt – könnte bzw. sollte nach der vorgeschlagenen Regelung vorgegangen werden.

Zu Z 34 (§ 147 Abs. 3a):

Nach der vorgesehenen Formulierung kann der oder die Rechtsschutzbeauftragte auch die Beiziehung von Sachverständigen „nach Maßgabe der §§ 126 und 127“ StPO verlangen. Laut dem geltenden § 126 Abs. 3 StPO sind für gerichtliche Ermittlungen Sachverständige von der Staatsanwaltschaft zu bestellen. Im Sinne des Rechtsschutzes erscheint es aber nicht zweckmäßig, den herangezogenen Sachverständigen von jenem Organ bestellen zu lassen, dessen Verfügungen allenfalls kontrolliert werden sollen. Es wird daher angeregt, diese Bestimmung zu überdenken.

Zu Z 39 (§ 516 Abs. 36):

Es erscheint nicht nachvollziehbar, § 135a des Entwurfs – somit die Kernbestimmung der vorliegenden Novelle – erst mit 1. August 2019 in Kraft zu setzen und dies im Wesentlichen mit dem Erfordernis der Schaffung der technischen Voraussetzungen zu begründen. Sofern ein unmittelbares Bedürfnis der Justizbehörden zur Schaffung der mit dieser Bestimmung verbundenen Überwachungsmöglichkeiten besteht, wäre diese im Interesse einer effizienten Strafverfolgung wohl auch so schnell wie möglich in Kraft zu setzen und sodann unverzüglich für die technische Umsetzung zu sorgen. Dies insbesondere auch vor dem Hintergrund, dass in den Erläuterungen (vgl. Seite 7 Abs. 4) ausdrücklich darauf hingewiesen wird, in welchen Ländern eine derartige Überwachung bereits gesetzlich zulässig (und damit offenbar auch technisch bereits umgesetzt) ist und daher die technische Umsetzung auch kurzfristig möglich sein müsste.

Für den Landesamtsdirektor:

Mag.ª Eva Tiefenbrunner

Mag.ª Regina Mertz-Koller

Ergeht an:

1. Präsidium des Nationalrates
2. alle Ämter der Landesregierungen
3. Verbindungsstelle der Bundesländer
4. MA 62
   (z. Zl. MA 62 - I/587396/2017)
   mit dem Ersuchen um Weiterleitung an die einbezogenen Dienststellen