BUNDESARBEITSKAMMER
PRINZ EUGEN STRASSE 20-22
1040 WIEN
T 01 501 65
www.arbeiterkammer.at
DVR 1048384

Bundesministerium für Justiz
Museumstraße 7
1070 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel **501 65**	Fax **501 65**	Datum
BMJ-S430.010/0001-IV 3/2016	AR-GStBAK/Ap	Ludwig Dvorak	DW 2221	DW 2471	12.05.2016

Entwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden

Die Bundesarbeitskammer dankt für die Übermittlung des Entwurfs und nimmt dazu wie folgt Stellung:

Allgemeine Vorbemerkungen:

Der vorliegende Gesetzesentwurf regelt die Zulässigkeit neuer Überwachungsmaßnahmen für Nachrichten, die im Wege eines Computersystems übermittelt werden. Die Bundesarbeitskammer begrüßt, dass der vorliegende Gesetzesentwurf strikt einzelfallbezogene Maßnahmen mit Rechtsschutzgarantien vorsieht.

Wie in den Erläuterungen angesprochen, handelt es sich um einen grundrechtlich sensiblen Bereich, in dem Eingriffe verhältnismäßig sein müssen. Mit der neuen gesetzlichen Regelung sollen die Voraussetzungen geschaffen werden, um bei dringendem Tatverdacht wegen schwerster Delikte, vor bzw nach der Ver- bzw Entschlüsselung von mit Computersystemen übertragene Nachrichten überwachen zu können. Nach den Erläuterungen soll damit der Umgehung der Überwachungsmöglichkeiten durch Beschuldigte begegnet werden. Ganz grundsätzlich ist dazu anzumerken, dass die Verschlüsselung von Nachrichten in der privaten Kommunikation per se keinesfalls unstatthaft und schon gar kein Hinweis auf kriminelles Verhalten darstellt, sondern eine in Fachkreisen durchaus empfohlene Form der Kommunikation ist, um dem Abfangen von Nachrichten und der Nachvollziehbarkeit von Online-Kommunikation durch Dritte vorzubeugen.

Wie in weiterer Folge dargelegt wird, reicht der gegenständliche Entwurf auch abseits der für die Installation von Überwachungsprogrammen idR notwendigen Verletzung des Hausrechts über die Überwachung von Nachrichten iSd § 135 StPO hinaus und ergibt sich daraus ein besonderer Bedarf an Rechtsschutzmaßnahmen. Aus Sicht der Bundesarbeitskammer wären in diesem Zusammenhang einige Klarstellungen im Gesetzestext bzw in den Erläuterungen wünschenswert und wird dazu im Einzelnen wie folgt Stellung genommen:

Zu § 134 Z 4a StPO:

Während die Erläuterungen davon ausgehen, dass der wesentliche Unterschied in der Eingriffsintensität in Grundrechte zwischen der bisherigen Nachrichtenüberwachung und der neu geplanten Maßnahmen in der für die Installation von Software häufig erforderlichen Verletzung des Hausrechts liegt, deutet die Begriffsdefinition des § 134 Z 4a auch auf eine inhaltlich weitergehende Befugnis hin: Die Überwachung und Speicherung aller im Wege von Computersystemen übermittelten und empfangenen „Nachrichten und sonstigen Daten" soll, wie auch in den Erläuterungen ausgeführt, zB auch Cloud-Speicher erfassen. Es werden somit nicht nur Nachrichten vor oder nach ihrer Ver- und Entschlüsselung erfasst, sondern auch generell Daten, die in Clouds oder einem internen Netzwerk gespeichert werden, besuchte Websites überwacht, etc, also wesentlich mehr als „nur" übersandte und empfangene Nachrichten. Sofern der Gesetzgeber solche Eingriffe tatsächlich für notwendig erachtet, ist jedenfalls von einer erhöhten Eingriffsintensität dieser Maßnahme auszugehen und sind entsprechend grundrechtliche Absicherungen vorzunehmen.

Zu § 136a StPO:

Das Problem der weitgehenden und nicht näher spezifizierten Definition „sonstiger Daten" tritt insbesondere in § 136a Abs 3 zu Tage. Die Erläuterungen führen zu Z 1 leg cit aus, dass zwar auch Daten aus Adressbüchern und Kontaktverzeichnissen zur Ermittlung von Kommunikationspartnern überwacht werden können sollen, dies aber keine Durchsuchung sonstiger im Computersystem gespeicherter Daten im Sinne einer Online-Durchsuchung impliziere. Es ist jedoch nicht nachvollziehbar, wie Adressbücher uä erkannt und überwacht werden können sollen, ohne das gesamte System danach zu durchsuchen. Die vorgeschlagene Bestimmung erscheint daher in sich widersprüchlich und faktisch unanwendbar, wenn sie es einerseits ausdrücklich zur Bedingung der Überwachung macht, ausschließlich jene Daten zu erfassen, die der Identifizierung dienen, andererseits aber das Auffinden dieser Daten eine Durchsuchung des gesamten Computersystems logisch voraussetzt. Es wird daher angeregt, diesbezüglich eine Klarstellung vorzunehmen, die eine Online-Durchsuchung auch im Gesetzestext und nicht nur in den Erläuterungen tatsächlich ausschließt.

Die Erläuterungen zu § 136a StPO verweisen zudem darauf, dass eine Installation von Überwachungssoftware nur durch physischen Zugriff und nicht durch eine „remote-Installation" erfolgen soll. Dieser Gedanke ist grundsätzlich sehr zu begrüßen. Ganz generell hegt die Bundesarbeitskammer konsumentenpolitische Bedenken gegen den Einsatz von Software, die unbemerkt Daten überwachen kann. Solche Programme setzen letztlich

Sicherheitslücken voraus, die aus Sicht des Konsumentenschutzes dringend zu schließen wären, an die nun aber der Staat Überwachungsmaßnahmen anknüpft. Diese Bedenken sind umso größer, wenn die Software nicht nur Daten erfasst und übermittelt, sondern auch ferngesteuert werden könnte. Dies würde nämlich zusätzliche technische Gefahren des Missbrauchs durch Dritte schaffen.

Die in den Erläuterungen gemachte Einschränkung, dass nur eine physische und keine ferngesteuerte Installation in Frage komme, findet im aktuellen Gesetzestext keine Deckung und bedarf daher dringend auch einer Klarstellung im Gesetzestext.

Zu § 137 Abs 1 StPO:

Es ist grundsätzlich zu begrüßen, dass Überwachungsmaßnahmen nur aufgrund einer richterlichen Bewilligung erfolgen sollen. In Hinblick auf die grundrechtliche Bedeutung wird jedoch angeregt, die Bewilligung nicht von EinzelrichterInnen, sondern durch einen Senat vornehmen zu lassen.

Zu § 137 Abs 3 StPO:

Auch aufgrund der Erläuterungen ist wohl klargestellt, dass Überwachungsmaßnahmen für einen vergangenen Zeitraum nur bei Einhaltung der erforderlichen richterlichen Genehmigungen erfolgen dürfen. Auch hier erscheint jedoch nicht klar, wie sich die nachträgliche Sicherung von „Nachrichten und sonstigen Daten“ konkret von einer Online-Durchsuchung, die ja vom Gesetzgeber nach den Erläuterungen nicht gewünscht ist und nicht wünschenswert erscheint, unterscheiden soll. Es wäre daher in Erwägung zu ziehen, diese rückwirkende Durchsuchung aus dem Gesetzesprojekt auszunehmen. Wie die Erläuterungen zu Recht feststellen, stehen die neugeschaffenen Bestimmungen nicht im Widerspruch zur Möglichkeit der Beschlagnahmung von Datenträgern.

Zu § 145 Abs 4 StPO:

Diese Bestimmung soll nach Zusammenhang und Erläuterungen offenbar sicherstellen, dass Manipulationen durch Behörden auszuschließen sind und die Authentizität der gesammelten Daten garantiert werden kann. Der Wortlaut der gesetzlichen Bestimmung, dass jede Änderung und jeder Zugang zum Computersystem in Sicherungskopien zu speichern sind, kann jedoch auch so zu verstehen sein, dass sämtliche am Computersystem befindliche Daten – und nicht nur Nachrichten oder neu gespeicherte Daten – als „Sicherungskopien“ von den Behörden gespeichert werden. Damit würde aber ein wesentlich weitreichenderer Anwendungsbereich geschaffen, als die Erläuterungen nahelegen. Es wird daher dringend angeregt, diese Formulierung entsprechend abzuändern und sicherzustellen, dass nur das Handeln der Behörden entsprechend zu protokollieren ist.

Abschließend ist festzustellen, dass der Gesetzesentwurf zwar Vorsorge für die Entfernung der Software trifft, jedoch keine besondere Regelung über den Umgang mit gesammelten Nachrichten und Daten trifft. Es wird vorgeschlagen, eine Löschungsverpflichtung innerhalb eines angemessenen Zeitraums vorzusehen.

Rudi Kaske
Präsident
F.d.R.d.A.

Hans Trenner
iV des Direktors
F.d.R.d.A.