ÖKOBÜRO
ALLIANZ DER UMWELTBEWEGUNG

A-1070 Wien, Neustiftgasse 36/3a
T: +43 1 524 93 77
F: +43 1 524 93 77-20
E: office@oekobuero.at
www.oekobuero.at

ZVR 873642346

An das
Bundesministerium für Justiz
Museumstraße 7
1070 Wien

Per Mail an:
team.s@bmj.gv.at
begutachtungsverfahren@parlament.gv.at

Wien, 21.August 2017

GZ: BMJ-S578.031/0008-IV 3/2017

Stellungnahme zum Entwurf eines Bundesgesetzes, mit dem die Strafprozessordnung1975 geändert wird (Strafprozessrechtsänderungsgesetz 2017)

Sehr geehrte Damen und Herren,

mit diesem Schreiben nimmt ÖKOBÜRO – Allianz der Umweltbewegung Stellung zum Entwurf eines Bundesgesetzes, mit dem die Strafprozessordnung1975 geändert werden soll.

ÖKOBÜRO ist die Allianz der Umweltbewegung. Dazu gehören 16 österreichische Umwelt-, Natur- und Tierschutz-Organisationen wie GLOBAL 2000, Greenpeace, Naturschutzbund, VIER PFOTEN oder der WWF. ÖKOBÜRO arbeitet auf politischer und juristischer Ebene für die Interessen der Umweltbewegung.

1. Legalisierung des Einsatzes sog. „IMSI-Catchern" - § 134 Z 2a StPO

In § 134 soll folgende Z 2a eingefügt werden:

> *„2a. „Lokalisierung einer technischen Einrichtung" der Einsatz technischer Mittel zur Feststellung von geographischen Standorten und der zur internationalen Kennung des Benutzers dienenden Nummer (IMSI) ohne Mitwirkung eines Anbieters (§ 92 Abs. 3 Z 1 TKG) oder sonstigen Diensteanbieters (§§ 13, 16 und 18 Abs. 2 des E – Commerce – Gesetzes, BGBl. I Nr. 152/2001),"*

Anders als in den EB erwähnt, ist ein IMSI-Catcher, also ein Sender, der einen regulären Funkmasten simuliert, nicht nur geeignet um Mobilgeräte zu orten, sondern auch um den Inhalt der Kommunikation zu überwachen. Für diese Überwachung gibt es jedoch keine Rechtsgrundlage.

ÖKOBÜRO lehnt daher die Einführung des § 134 Z 2a StPO ab.

2. Einschränkung des Briefgeheimnisses - § 135 Abs 1 StPO

In § 135 Abs 1 StPO soll folgender Satz entfallen:

> *„und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde."*

Das Briefgeheimnis ist einer der wichtigsten Punkte des Staatsgrundgesetzes über die allgemeinen Rechte der Staatsbürger, das ursprünglich gerade dazu diente, den Metternichschen Überwachungsstaat einzuschränken. Die Änderung des § 135 Abs 1 StPO würde das Briefgeheimnis massiv einschränken, was zusammen mit der Streichung des § 137 Abs 2 StPO dazu führen würde, dass die Pflicht zur Information der/des Betroffenen binnen 24 Stunden entfällt. Somit wäre bei jeder Verzögerung oder verlorenen Sendung die Frage offen, ob diese Gegenstand einer Beschlagnahme wurde. Dieser Eingriff in das Grundrecht auf das Briefgeheimnis ist unverhältnismäßig.

ÖKOBÜRO lehnt daher die Einschränkung des Briefgeheimnisses durch die Änderung in § 135 Abs 1 StPO ab.

3. Einführung eines „Bundestrojaners" - § 135a StPO

Nach § 135 StPO soll folgender § 135a StPO eingeführt werden:

> *„Überwachung verschlüsselter Nachrichten*
>
> *§ 135a. (1) Überwachung verschlüsselter Nachrichten ist zulässig:*
> *1. in den Fällen des § 135 Abs. 2 Z 1,*
> *2. in den Fällen des § 135 Abs. 2 Z 2, sofern der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, der Überwachung zustimmt,*
> *3. wenn dies zur Aufklärung einer Straftat, die der Zuständigkeit des Landesgerichts als Schöffen- oder Geschworenengericht (§ 31 Abs. 2 und 3) unterliegt, erforderlich ist oder die Aufklärung oder Verhinderung einer im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten Straftat ansonsten wesentlich erschwert wäre und*
> *a. der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, einer Straftat, die der Zuständigkeit des Landesgerichts als Schöffen- oder Geschworenengericht (§ 31 Abs. 2 und 3) unterliegt, oder einer Straftat nach den §§ 278 bis 278b StGB dringend verdächtig ist, oder*
> *b. auf Grund bestimmter Tatsachen anzunehmen ist, dass eine einer solchen Tat dringend verdächtige Person das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, benützen oder mit ihm eine Verbindung herstellen werde.*
> *(2) Eine Überwachung verschlüsselter Nachrichten ist überdies nur dann zulässig, wenn das Programm*
> *1. nach Beendigung der Ermittlungsmaßnahme funktionsunfähig ist oder ohne dauerhafte Schädigung oder Beeinträchtigung des Computersystems, in dem es installiert wurde, und der in ihm gespeicherten Daten entfernt werden kann, und*

2. keine Schädigung oder dauerhafte Beeinträchtigung dritter Computersysteme, in denen kein Programm zur Überwachung verschlüsselter Nachrichten installiert wird, bewirkt.
(3) 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 die Installation des Programms zur Überwachung verschlüsselter Nachrichten in dem Computersystem zu ermöglichen. Die Eigentums- und Persönlichkeitsrechte sämtlicher Betroffener sind soweit wie möglich zu wahren."

Mit der Einführung staatlicher Spionagesoftware fördert der Staat absichtlich und gezielt die Unsicherheit von Betriebssystemen, da für die Installation eine Sicherheitslücke verwendet werden muss. Da der Staat so Sicherheitslücken geheim und damit offen halten muss, fördert er die Verletzlichkeit von Betriebssystemen und die Wahrscheinlichkeit von Angriffen auf EDV-Infrastruktur von unschuldigen Einzelpersonen, NGOs und Unternehmen. Wie gefährlich diese Lücken auch für überlebenswichtige Maschinen sein können zeigte sich in der Infektion von Krankenhausgeräten in London im Zuge des „WannaCry" Virus 2017. Durch den neuen § 135a StPO kreiert der Gesetzgeber ein Interesse des Staates an unsicheren Computersystemen. Von dieser Änderung ist daher jede Person in Österreich, die einen Computer, ein Smartphone, ein Tablet oder sogar eine Spielkonsole besitzt, direkt betroffen.

2008 stellte eine Kommission des BMI und BMJ fest, dass die „Online-Durchsuchung" von Computern und anderen Geräten der österreichischen Rechtsordnung (u.a. der StPO, dem SPG und dem MBG) widerspricht und unzulässig ist. [1] Eine Abgrenzung der „Online-Durchsuchung" zur „Online-Überwachung" ist jedoch technisch nicht durchführbar. Die Kontrolle der Software durch die Datenschutzbehörde erscheint darüber hinaus fraglich, da dieser keine Technikerin/Techniker angehört.

Schließlich ist auch die Wirksamkeit dieser Überwachung höchst umstritten, da selbst von technisch nicht versierten Benutzerinnen/Benutzern eine unerwünschte Überwachungssoftware etwa durch gängige Virenschutzprogramme leicht erkannt werden kann. Antivirensofware-Hersteller Kaspersky etwa entdeckte bereits mehrmals derartige Software und verhinderte ihre Aktivierung.[2]

Auch Umwelt-NGOs sind auf die Sicherheit ihrer Computersysteme und auf verlässlich vertrauliche Kommunikation in ihrer täglichen Arbeit angewiesen. Das Unterwandern dieser Sicherheit durch das Offen-Halten von Lücken gefährdet daher die Arbeit von Umweltorganisationen und die Sicherheit ihrer Mitarbeitenden sowohl beruflich als auch privat.

ÖKOBÜRO lehnt daher die Einführung des § 135a StPO ab.

[1] https://epicenter.works/sites/default/files/1pager-legalitaet_bundestrojaner.pdf .
[2] https://www.pcwelt.de/news/Sicherheit-Kaspersky-entdeckt-neue-Bundestrojaner-Version-3526766.html .

Die genannten Bestimmungen der StPO Novelle sind geeignet, die Gesamtbevölkerung stark zu gefährden und nehmen für zweifelhafte Ermittlungsvorteile massive Grundrechtsverletzungen und unwirtschaftliche Ausgaben in Kauf. Das mutwillige Gefährden der EDV-Systemsicherheit schadet der Arbeit von NGOs und der Sicherheit ihrer Mitarbeiterinnen und Mitarbeiter enorm. Auch die rechtgrundlose Verwendung von Überwachungshardware und das potentielle Kompromittieren von Kommunikation können zu starken Problemen in der Arbeit der Zivilgesellschaft führen. ÖKOBÜRO empfiehlt daher dringend, von der Einführung des „Bundes-Trojaners" abzusehen und die Regelung zum „IMSI-Catcher" von Grund auf zu überarbeiten.

Mit freundlichen Grüßen

Mag. Thomas ALGE
Geschäftsführer ÖKOBÜRO