Republik Österreich
Datenschutzbehörde

A-1010 Wien, Hohenstaufengasse 3
Tel.: ++43-1-53115 20
Fax: ++43-1-53109 202690
E-Mail: dsb@dsb.gv.at
DVR: 0000027

GZ: DSB-D054.539/0001-DSB/2016

Sachbearbeiterin: Mag. Stefanie PITSCH

Präsidium des Nationalrates

Dr. Karl Renner Ring 3
1017 Wien

Stellungnahme der Datenschutzbehörde

per E-Mail: begutachtungsverfahren@parlament.gv.at

**Betrifft: Stellungnahme der Datenschutzbehörde zum do. Gesetzesentwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden**

Die Datenschutzbehörde nimmt in o.a. Angelegenheit aus Sicht Ihres Wirkungsbereiches wie folgt Stellung:

Zu § 134 Z 4a und Z 5 StPO:

Gemäß § 134 Z 4a StPO ist die „Überwachung von Nachrichten, die im Wege eine Computersystems übermittelt werden“ das Ermitteln von Nachrichten und sonstigen Daten (§ 74 Abs. 2 StGB), die im Wege eines Computersystems (§ 74 Abs. 1 Z 8 StGB) übermittelt und empfangen werden, durch Installation eines Überwachungsprogramms im Computersystem ohne Kenntnis des Inhabers eines solchen Systems oder sonstiger Verfügungsberechtigter.

Trotz des in § 134 Z 4a StPO vorgenommenen Verweises auf § 74 Abs. 2 StGB, wonach unter Daten sowohl personenbezogene und nicht personenbezogene Daten als auch Programme zu verstehen sind, geht aus § 134 Z 4a und Z 5 StPO nicht hervor, was genau unter dem verwendeten Begriff der „sonstigen Daten“ zu verstehen ist.

Zu §136a StPO:

1. Die Erläuterungen zu § 136a StPO sehen vor, dass die Installation der Überwachungssoftware ausschließlich durch physischen Zugriff auf das Computersystem, nicht jedoch eine Ferninstallation der

Überwachungssoftware, zulässig sein soll. Dies ist dem Gesetzestext in dieser Klarheit nicht zu entnehmen. Eine Präzisierung des Gesetzestextes dahingehend, dass die Installation der Überwachungssoftware ausschließlich durch physischen Zugriff auf das Computersystem zulässig sein soll wäre aus Sicht der Datenschutzbehörde, geboten. (zum Detaillierungsgrad einer Eingriffsnorm im Sinne des § 1 Abs. 2 DSG 2000 vgl. bspw. VfSlg. 19.801/2013).

In diesem Zusammenhang wird angemerkt: Unter den Begriff des „Computersystems“ fallen auch Smartphones und Tablets (siehe dazu die Erläuterungen zu § 134 Z 4a und 5 StPO). Da gemäß § 134 Z 4a StPO die „Installation eines Überwachungsprogramms im Computersystem ohne Kenntnis des Inhabers eines solchen Systems“ erfolgen soll, eschließt sich nicht, wie die unerkannte Installation der Überwachungssoftware auf ein Smartphone, das der Betroffene in der Regel „bei sich tragen“ wird, erfolgen kann, wenn die Installation nur mittels physischem Zugriff (und nicht auch mittels Ferninstallation) zulässig sein soll.

2. Gemäß § 136a Abs. 3 Z 1 StPO soll das Überwachungsprogramm nicht nur jene Daten erfassen, die im Wege des Computersystems übermittelt und empfangen werden, sondern auch „jene Daten, die Rückschlüsse auf die Namen oder die sonstigen Identifizierungsmerkmale der Inhaber oder Verfügungsbefugten (…) erlauben.“ Demnach soll das Überwachungsprogramm auch bereits auf dem Computersystem gespeicherte Daten erfassen, weshalb – entgegen den Ausführungen in den Erläuterungen zu § 136a StPO - eine Online-Durchsuchung vorliegen dürfte.

Des Weiteren geht aus den Erläuterungen zu § 136a StPO hervor, dass zur Identifizierung des Benutzers auf Kontaktverzeichnisse und Adressbücher zugegriffen werden soll. Dies findet jedoch keinen Niederschlag im Gesetzestext, weshalb es hier einer Präzisierung des Gesetzestextes bedürfte.

3. Aus § 136a Abs. 3 Z 1 StPO ergibt sich, dass eine undifferenzierte Überwachung aller eingehenden und ausgehenden Nachrichten des überwachten Computersystems vorgesehen ist. Im Gegensatz dazu könnte eine spezifizierte Überwachung der empfangenen und übermittelten Daten durch Programmierung eines Kontrollwörterbuches, das ein- und ausgehende Nachrichten ausschließlich nach im Kontrollwörterbuch gespeicherten Stichwörtern durchsucht, erfolgen. Im Hinblick darauf, dass der Eingriff in das Grundrecht auf Datenschutz nur in der gelindest möglichen Form erfolgen sollte (vgl. dazu § 1 Abs. 2 letzter Satz DSG 2000), erschiene diese Vorgangsweise angemessen.

Im Übrigen entspräche dies etwa auch dem in Artikel 25 der Datenschutz-Grundverordnung (Verordnung (EU) Nr. 2016/679) vorgesehenen Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

<u>§ 136a StPO iVm § 76 StPO:</u>

§ 76 Abs. 4 Z 1 StPO sieht – unter den darin normierten Voraussetzungen – vor, dass Daten, die durch eine Ermittlungsmaßnahme nach dem 4. bis 6. Abschnitt des 8. Hauptstücks ermittelt worden sind, an Staatsanwaltschaften, Sicherheitsbehörden sowie Gerichte und andere Behörden übermittelt werden dürfen. § 136 a StPO ist eine Ermittlungsmaßnahme nach dem 5. Abschnitt des 8. Hauptstückes und ist demnach vom Anwendungsbereich des § 76 Abs. 4 Z 1 StPO umfasst. Es stellt sich somit die Frage, ob diese Art der Datenübermittlung im vorliegenden Fall aufgrund der Eingriffsintensität erforderlich ist.

Schlussbemerkung:

Es wird darauf hingewiesen, dass es sich bei der gemäß § 136a StPO vorgesehenen „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“ um eine Datenanwendung gemäß § 4 Z 7 DSG 2000 handelt. Datenanwendungen – auch jene, die der ordentlichen Gerichtsbarkeit (Art. 82 ff B-VG) zuzurechnen sind – unterliegen im Regelfall der Meldepflicht nach §§ 17 ff DSG 2000 (vgl. dazu auch *Jahnel*, Datenschutzrecht [2010] 324). § 17 Abs. 3 DSG 2000 normiert, dass eine Ausnahme von der Meldepflicht nur dann vorliegt, „soweit dies zur Verwirklichung des Zwecks der Datenanwendung notwendig ist“.

10. Mai 2016
Die Leiterin der Datenschutzbehörde
JELINEK

| | | |
|---|---|---|
| REPUBLIK ÖSTERREICH DATENSCHUTZBEHÖRDE @ AMTSSIGNATUR | Unterzeichner | serialNumber=1119505,CN=Datenschutzbehörde,C=AT |
| | Datum/Zeit | 2016-05-10T10:25:49+02:00 |
| | Prüfinformation | Informationen zur Prüfung der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at<br>Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bka.gv.at/verifizierung |
| | Hinweis | Dieses Dokument wurde amtssigniert. |