Einführung einer Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden

Mag. Angelika Zotter, BA

I. Strafprozessordnung

1. Allgemeines

Am 31.03.2016 wurde ein Entwurf für eine Änderung der Strafprozessordnung[1] sowie des Staatsanwaltschaftsgesetzes[2] vorgelegt.[3] Ziel der Neuerungen ist es, eine gesetzliche Grundlage für die Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, zu schaffen. Die vorgesehene Ermittlungsmaßnahme orientiert sich in Hinblick auf ihre materiellen und formellen Voraussetzungen an den bereits bestehenden Bestimmungen zur optischen und akustischen Überwachung von Personen in **§ 136 StPO**. Ihre Einführung wird mit der Änderung des Kommunikationsverhaltens von Tätern aufgrund der fortgeschrittenen technischen Möglichkeiten begründet. Die neue Maßnahme soll die Strafverfolgungsbehörden mit effektiven Reaktionsmöglichkeiten ausstatten und dadurch zur Aufklärung schwerster Straftaten in den Bereichen organisierte Kriminalität und Terrorismus beitragen.[4] Im Folgenden werden die wichtigsten Inhalte kurz zusammengefasst.

2. Definition

In **§ 134** ist eine neue **Ziffer 4a** vorgesehen, die – systemkonform – eine Definition des Begriffes „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden" bietet. Darunter ist folglich das Ermitteln von Nachrichten[5] und sonstigen personen- und nicht personenbezogenen Daten und Programmen[6] zu verstehen, die im Wege eines Computersystems iSd **§ 74 Abs 1 Z 8 StGB**[7] übermittelt und empfangen werden. Dies soll durch Installation eines entsprechenden Überwachungsprogramms im Computersystem ohne Kenntnis des jeweiligen Inhabers oder sonstigen Verfügungsbefugten geschehen. Der Begriff des „Ergebnisses" in **§ 134 Z 5** soll entsprechend angepasst werden.

---

[1] BGBl. Nr. 631/1975.
[2] BGBl. Nr. 164/1986.
[3] 192/ME, siehe http://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00192/fname_521691.pdf.
[4] Vgl. Erläut 192/ME 25. GP 1f.
[5] Also die Inhaltsdaten einer Kommunikation, vgl. *Lewisch* in *Höpfel/Ratz,* WK² StGB § 119 Rz 9a; *Reindl-Krauskopf* in *Fuchs/Ratz*, WK StPO § 134 Rz 42.
[6] Verweis auf § 74 Abs 2 StGB; „Daten" sind also sowohl Gedankeninhalt eines E-Mails als auch eine bloße Zahlenabfolge, die einen PIN-Code, ein Passwort oder eine Kreditkartennummer beschreibt, siehe *Reindl-Krauskopf* in *Höpfel/Ratz,* WK² StGB § 119a Rz 8.
[7] Dies umfasst neben klassischen Computergeräten wie PC oder Notebook auch sämtliche Geräte, die eine Internetverbindung ermöglichen, wie Smartphones, Tablets oder auch Spielekonsolen; vgl. Erläut 192/ME 25. GP 4.

3. Materielle Voraussetzungen

Die vorgesehene Überwachung von Nachrichten soll in einem neuen **§ 136a** geregelt werden. Ihre Zulässigkeit orientiert sich an den Voraussetzungen des „großen Lauschangriffs" in **§ 136 Abs 1 Z 3**. Sie muss also entweder der Aufklärung eines mit mehr als 10 Jahren Freiheitsstrafe bedrohten Verbrechens, des Verbrechens der kriminellen Organisation[8] oder der terroristischen Vereinigung[9] dienen, der Aufklärung oder Verhinderung von im Rahmen dieser Gruppierungen begangenen oder geplanten strafbaren Handlungen, oder der Aufenthaltsermittlung eines wegen einer solchen Straftat Beschuldigten. Die Nachrichtenüberwachung soll dann zum Einsatz kommen, wenn ohne sie die Erreichung dieser Ziele aussichtslos oder wesentlich erschwert wäre. Darüber hinaus muss die von der Überwachung betroffene Person dringend verdächtig sein, eines der genannten Verbrechen begangen zu haben, oder es muss aufgrund bestimmter Tatsachen anzunehmen sein, dass ein Kontakt einer solcherart dringend verdächtigen Person mit der von der Überwachung betroffenen Person hergestellt wird.

In Angleichung mit **§ 136 Abs 4** soll eine solche Überwachung nur unter Wahrung der Verhältnismäßigkeit[10] zulässig sein. Zur Verhinderung von Straftaten, die im Rahmen einer kriminellen Organisation oder terroristischen Vereinigung begangen oder geplant werden, müssen bestimmte Tatsachen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen. Sind diese Voraussetzungen erfüllt, dann muss der Eingriff außerdem notwendig sein, um die Überwachung und Aufzeichnung von Nachrichten in unverschlüsselter Form zu ermöglichen (**§ 136a Abs 1**).

Nach dem vorgesehenen **§ 136a Abs 2** soll es auch zulässig sein, in Wohnungen oder andere durch das Hausrecht geschützte Räume einzudringen[11], Sicherheitsvorkehrungen wie beispielsweise Passwörter zu überwinden und auch Behältnisse wie etwa Schreibtischladen oder auch die Kleidung des Betroffenen zu durchsuchen, um Zugang zu dem Computersystem erhalten zu können.[12]

Im Lichte der Verhältnismäßigkeit finden sich in **§ 136a Abs 3** des Entwurfes weitere Einschränkungen. Demnach soll sich die neue Bestimmung nur auf jene Daten beziehen, die im Wege des Computersystems empfangen oder übermittelt werden, oder die mit dieser Übertragung in unmittelbarem Zusammenhang stehen. Eine umfassende „Online-Durchsuchung" nach anderen Daten zur Identifizierung einer Person oder sonstigen im System gespeicherten Daten ist nach dem Entwurf unzulässig.[13] Darüber hinaus ist sicherzustellen, dass das Überwachungssystem nach Beendigung der Ermittlungsmaßnahme dauerhaft funktionsunfähig ist oder jedenfalls so entfernt werden kann, dass keine dauerhafte Beschädigung oder Beeinträchtigung des betroffenen Computersystems, der in ihm gespeicherten Daten oder dritter Computersysteme eintritt, die nicht Gegenstand der Überwachung sind.

---

[8] § 278a StGB.
[9] § 278b StGB.
[10] § 5 StPO.
[11] Die Installation der Überwachungssoftware soll ausschließlich durch physischen Zugriff auf ein Computersystem im Gegensatz zu einer remote-Installierung erfolgen, vgl. Erläut 192/ME 25. GP 5.
[12] Vgl. Erläut 192/ME 25. GP 5.
[13] Siehe Erläut 192/ME 25. GP 5.

4. Formelle Voraussetzungen

Auch hinsichtlich der formellen Bedingungen sollen sich die vorgesehenen Bestimmungen in das System der **§§ 134 ff** einfügen. Dementsprechend soll die Maßnahme nach **§ 137 Abs 1** einer Anordnung der Staatsanwaltschaft auf der Grundlage einer gerichtlichen Bewilligung bedürfen. Das Eindringen in Räume, Durchsuchen von Behältnissen und Überwinden spezifischer Sicherheitsvorkehrungen, wie in **§ 136a Abs 2** vorgesehen, soll jeweils im Einzelnen einer gerichtlichen Bewilligungspflicht unterliegen. Die Maßnahme soll nur für einen künftigen oder auch vergangenen Zeitraum angeordnet werden dürfen, der zur Erreichung des Zwecks der Maßnahme voraussichtlich erforderlich ist, wobei die nachträgliche Legitimierung eines ohne staatsanwaltschaftliche Anordnung und gerichtliche Bewilligung durchgeführten Einsatzes dadurch nicht erreicht werden kann.[14] Auch die Anordnung der Überwachung für einen vergangenen Zeitraum setzt daher eine rechtmäßige Bewilligung voraus. **§ 138** soll in Hinblick auf den notwendigen Inhalt der Anordnung sowie auf Zustellungen nach Beendigung der Maßnahme entsprechend angepasst werden.

5. Sonstige Bestimmungen

Zufallsfunde sollen, um den strengen Zulässigkeitserfordernissen gerecht zu werden,[15] nach **§ 140 Abs 1 Z 4** nur zum Nachweis einer vorsätzlich begangenen Straftat verwendet werden, derentwegen der Einsatz der Maßnahme nach **§ 136a** zulässig gewesen wäre. Durch geeignete Protokollierung, vorgesehen in **§ 145 Abs 4**, sollen die Eingriffe in ein betroffenes Computersystem sowie jede nachträgliche Änderung daran nachvollzogen werden können, um insgesamt die Authentizität und Verlässlichkeit der ermittelten Daten zu gewährleisten.[16] Nach **§ 147 neu** soll der Einsatz der Ermittlungsmaßnahme darüber hinaus der Prüfung und Kontrolle des Rechtsschutzbeauftragten der Justiz unterliegen, dem zu diesem Zweck Einsicht in sämtliche Unterlagen und Protokolle sowie das Recht, einen Sachverständigen zu beantragen, gewährt werden sollen.[17]

II. Staatsanwaltschaftsgesetz

Die Bestimmungen zum Berichtswesen in **§ 10a StAG** sollen dahingehend angepasst werden, dass die Staatsanwaltschaften auch im Falle der Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, den Oberstaatsanwaltschaften über die beabsichtigte Anordnung der Ermittlungsmaßnahme zu berichten haben. Darüber hinaus soll die vorgesehene Maßnahme in den jährlichen Bericht des BMJ über den Einsatz besonderer Ermittlungsmaßnahmen an den Nationalrat, den Datenschutzrat und die Datenschutzbehörde aufgenommen werden.

Die vorgesehenen Änderungen sollen sowohl im Bereich der StPO sowie des StAG mit dem 1. Jänner 2017 in Kraft treten.

---

[14] Siehe Erläut 192/ME 25. GP 5.
[15] Vgl. Erläut 192/ME 25. GP 6.
[16] Erläut 192/ME 25. GP 6.
[17] Siehe § 147 Abs 3a.