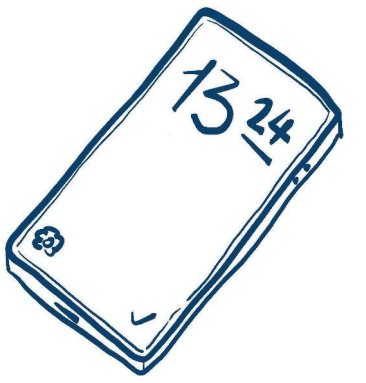
Die importierte Überwachung ist keine Lösung

Gastbeitrag. Während die Behörden legalen Zugriff auf Messenger-Dienste fordern, nutzen sie – rechtsstaatlich bedenklich – Daten aus dem Ausland. Wie eine Regelung in Österreich mehr Akzeptanz finden könnte.



VON ANDREAS POLLAK

Wien. Der Anschlag auf das Taylor-Swift-Konzert konnte aufgrund der Warnung durch einen ausländischen Geheimdienst vereitelt werden. Der Anschlag nahe dem israelischen Konsulat erfolgte durch einen bereits amtsbekannten Österreicher. Hätte dieser Anschlag durch bessere staatliche Überwachung verhindern werden können? In Frankreich wurde der Gründer des Messenger-Dienstes Telegram festgenommen. Der Vorwurf ist laut Medien, er habe zu wenig gegen die Nutzung von Telegram durch Kriminelle getan.

Durch die Ende-zu-Ende-Verschlüsselung ist angeblich die gesamte Kommunikation während der Übermittlung selbst für den Betreiber des Messenger-Dienstes nicht lesbar; sie soll daher umfassenden Schutz vor Überwachung bieten, solang nicht das Endgerät direkt überwacht wird. Terroristen und Kriminelle machen sich diese Verschlüsselung zunutze. WhatsApp, Signal, Telegram und viele andere Ende-zu-Ende-verschlüsselte Messenger erfreuen sich aber auch bei der großen Mehrheit von unbescholtenen Bürgern großer Beliebtheit.

In Österreich ist derzeit eine Überwachung von Ende-zu-Ende-verschlüsselten Messenger-Diensten nicht erlaubt, da es dafür keine gesetzliche Grundlage gibt. Der VfGH hatte nämlich 2019 ein entsprechendes Gesetzespaket als verfassungswidrig aufgehoben. Dieses hätte die geheime Installation von Überwachungssoftware auf Computersystemen, die Messenger-Dienste betreiben bzw. Endgeräte darstellen, erlauben sollen.

Strenge Vorgaben des VfGH

Der VfGH sprach sich zwar nicht grundsätzlich dagegen aus, doch waren die gesetzlichen Kriterien nicht streng genug. Auch fehlte dem VfGH eine effektive gerichtliche Kontrolle genehmigter und damit laufender Überwachungen. Nun fordern Geheimdienste und Polizei vehement einen neuen gesetzlichen Anlauf.

In anderen EU-Staaten werden Messenger-Dienste kritischer behandelt, wobei Frankreich besonders herausstechen dürfte, wie etwa die jüngste Festnahme des Telegram-Gründers, Pawel Durow, veranschaulicht. In einem anderen Fall hat ein französisches Gericht die Überwachung sämtlicher Nutzer des verschlüsselten Mobiltelefondienstes Encrochat genehmigt. Encrochat verwendete speziell programmierte Mobiltelefone, die mittels eines eigenen Serverdienstes verschlüsselt kommunizierten.

Die französischen Behörden begründeten die Überwachung damit, dass infolge der Verschlüsselung der gesamten Mobiltelefone, der eher klandestinen Bezugsmöglichkeiten der verschlüsselten Encrochat-Telefone und deren Verbreitung im Drogenmilieu mehr oder weniger grundsätzlich von einer kriminellen Nutzung auszugehen sei.

Die Behörden infiltrierten den Encrochat-Server, um sodann mit einem Update eine Überwachungssoftware auf die verschlüsselten Handys aller Encrochat-Nutzer einzuspielen. Dann wurde die gesamte gespeicherte Kommunikation aller Nutzer abgesaugt, die laufenden Gespräche wurden aufgezeichnet. Die Nutzer konnten in der Regel erst durch die Überwachung ermittelt werden, und erst in der Folge wurde geprüft, ob der Betroffene überhaupt einer Straftat konkret verdächtig war.

Solch eine Überwachung ist in Österreich derzeit nicht möglich. Selbst das durch den VfGH aufgehobene Gesetzespaket hätte für eine derartig groß angelegte pauschale Überwachung der gesamten Kommunikation aller Nutzer eines – fragwürdigen – Dienstes wohl keine Grundlage geliefert. Österreichs Behörden greifen aber sehr gern auf die von den französischen Behörden gewonnenen Daten zu und verwenden diese bei der Strafverfolgung.

Es gibt zig Anlassfälle, vor allem im Bereich der Drogenkriminalität. In anderen vergleichbaren Fällen hat Österreich beispielsweise vom FBI über Erkenntnisse aus einer ähnlichen Massenüberwachung Daten besonders verschlüsselter Mobiltelefone erhalten. Der Widerstand der Verteidiger in Österreich gegen die Nutzung von Daten aus ausländischen Massenüberwachungen verschlüsselter Dienste ist groß, aber bislang vor dem Obersten Gerichtshof wiederholt erfolglos geblieben.

Das eine Extrem ist, jede Überwachung gänzlich auszuschließen. Das andere ist, alle Daten abzusaugen und die Betreiber strafrechtlich zu verfolgen. Aus rechtsstaatlicher Sicht braucht es klare gesetzliche Vorgaben. Auch Mitarbeiter der Behörden werden den Wert des Datenschutzes wohl nicht negieren. Ähnlich werden Verteidiger anerkennen, dass die Überwachung von Ende-zu-Ende-verschlüsselter Kommunikation nicht immer ausgeschlossen sein darf. Gegen eine funktionierende Strafverfolgung und die Verhinderung von terroristischen Anschlägen wird sich doch hoffentlich niemand ernsthaft aussprechen wollen.

In diesem Sinne hat auch der VfGH die Überwachung verschlüsselter Computersysteme nicht prinzipiell verboten, sondern grundrechtliche Anforderungen vorgegeben, die ein neues Gesetzespaket erfüllen muss. So wird die Überwachung jedenfalls auf einzelne Anschlüsse, die in Zusammenhang mit einer konkreten Verdachtslage stehen, eingeschränkt sein müssen. Das hat erst recht zu gelten, wenn eine Infiltration des gesamten Servers und nicht bloß einzelner Endgeräte erfolgt. Auch darf eine Überwachung nur bei schweren Straftaten erlaubt sein, und es muss eine effektive – auch laufende – Kontrolle erfolgen.

Kontrolle als Knackpunkt

Gerade die laufende Kontrolle und die Qualität richterlicher Genehmigungen von Überwachungen sind Knackpunkte. Es ist eine klare grundrechtliche Voraussetzung, dass derartige Überwachungsmaßnahmen neben einer staatsanwaltschaftlichen Anordnung auch zusätzlich richterlich bewilligt werden müssen.

Bereits jetzt gibt es viele gesetzliche Fälle richterlicher Bewilligungen. In der Praxis erfolgt die Freigabe meist mittels eines Stempels. Das Gericht erklärt also nicht selbst, weshalb es der Staatsanwaltschaft zustimmt. Diese Praxis lässt bei manchen Verteidigern Zweifel aufkommen, inwieweit eine gerichtliche Kontrolle effektiv erfolgt ist.

Ein Lösungsansatz könnte sein, zusätzliche Prüfungen durch eine unabhängige Expertenkommission vorzusehen. Sie könnte neben dem Rechtsschutzbeauftragten etwa aus Universitätsprofessoren sowie Staatsanwälten und Strafverteidigern bestehen, die unterschiedliche Sichtweisen beisteuern. Das würde eine breite Akzeptanz der Überwachungspraxis fördern.

Die Kommission könnte auf eine österreichweite Vereinheitlichung der erst- und zweitinstanzlichen Bewilligungspraxis hinwirken und notwendigenfalls in Einzelfällen korrigierend eingreifen, beispielsweise indem Empfehlungen der Kommission durch ministerielle Weisungen an die Staatsanwaltschaften verbindlich gemacht werden.

Andreas Pollak ist Partner von Petsche Pollak Rechtsanwälte.

IMPRESSUM: RECHTSPANORAMA

Redaktion: Mag. Benedikt Kommenda, Dr. Philipp Aichinger
Telefon: 01/514 14-447, 01/514 14-552
E-Mail: benedikt.kommenda@diepresse.com
philipp.aichinger@diepresse.com
Gastbeiträge müssen nicht der Meinung der „Presse" entsprechen.
Anzeigen: René Gruber
Telefon: 01/514 14-263
E-Mail: rene.gruber@diepresse.com
DiePresse.com/Rechtspanorama