Stand 18. August 2014

FAQ –Häufig gestellte Fragen zur Überwachung des Post- und Fernmeldeverkehrs

Gemäss Statistik des Dienstes ÜPF haben Strafverfolgungsbehörden in den letzten Jahren deutlich mehr Überwachungen angeordnet. Warum?

Der Dienst ÜPF setzt Post- und Fernmeldeüberwachungen auf Anordnung der Schweizer Strafverfolgungsbehörden um. Tatsächlich hat die Anzahl Überwachungen in den letzten Jahren zugenommen. Die Statistik 2013 zeigt, dass die Zahl der sogenannten rückwirkenden Massnahmen, bei denen Verbindungsdaten ausgewertet wurden, in den letzten fünf Jahren um einen Viertel zugenommen hat. Der Anstieg ist jedoch deutlich kleiner als die Zunahme der Nutzung von Telekommunikationsmitteln in der Schweiz. So ist etwa die Gesamtdauer der Verbindungen von 2008 bis 2012 um einen Drittel angestiegen (von rund 8000 Millionen Minuten auf 10‘500 Millionen Minuten). Das Volumen der Daten, die via Handy übertragen werden, hat sich mehr als verzwanzigfacht (von rund 700 auf 16‘600 Terabytes). Und schliesslich gibt es heute viel mehr Handyanschlüsse als noch vor wenigen Jahren: Diese Zahl hat sich seit 2002 von 5,2 auf 10,6 Millionen verdoppelt. (Quelle: Fernmeldestatistik 2012; Statistik Schweiz; ComCom)

Ist der Entscheid des Gerichtshofs der Europäischen Union (EuGH) vom 8. April 2014 betreffend die Vorratsdatenspeicherung für die Schweiz verbindlich?

Nein, die Schweiz hat in ihren bilateralen Verträgen mit der EU die Richtlinie über die Vorratsdatenspeicherung nicht übernommen. Diese Richtlinie findet daher in der Schweiz keine Anwendung.

Bei der Vorratsdatenspeicherung geht es nicht um Gesprächsinhalte, sondern ausschliesslich um Informationen darüber, wer mit wem wann wie lange wo und mit welchen technischen Mitteln kommuniziert hat. Diese Informationen können helfen, strafbares Verhalten im Nachhinein nachzuvollziehen oder den Aufenthaltsort vermisster Personen zu ermitteln (Notsuche).

Der EuGH untersagt mit seinem Entscheid nicht diese Speicherung auf Vorrat an sich. Das Gericht verlangt aber, dass die Aufbewahrung, die Verwendung und der Zugriff auf die Randdaten strikt geregelt werden. Diese flankierenden Regeln fehlen in der Richtlinie, sind im schweizerischen Recht jedoch vorhanden. Somit stellt der Entscheid des EuGH die Speicherung von Randdaten in der Schweiz gemäss einer ersten Einschätzung des Bundesamtes für Justiz auch nicht indirekt in Frage. Das gilt sowohl für das geltende Recht als auch für die vorgeschlagene Gesetzesänderung, die die Aufbewahrungsfrist von sechs auf zwölf Monate verlängern will.

Weshalb soll die Vorratsdatenspeicherung in der Schweiz zulässig sein?

In der Schweiz bleibt der Eingriff in die Grundrechte durch die Speicherung der Randdaten auf das Notwendigste beschränkt. Die Daten werden zwar ohne Tatverdacht auf Vorrat aufbewahrt, aber Polizei und Staatsanwaltschaften haben darauf nicht unbeschränkt Zugriff, denn sie sind nicht im Besitz des Staates, sondern bei der jeweiligen Fernmeldedienstanbieterin gespeichert. Das Gesetz sieht zudem hohe Hürden für den Zugriff vor: So können die Strafverfolgungsbehörden die Daten nur einsehen, wenn mehrere Voraussetzungen erfüllt sind.

In Straf- und Rechtshilfeverfahren darf die Überwachung namentlich nur angeordnet werden, wenn ein dringender Tatverdacht auf ein Verbrechen oder Vergehen besteht; zudem muss die Schwere der Straftat die Überwachung rechtfertigen. Schliesslich ist erforderlich, dass die bisherigen Untersuchungshandlungen erfolglos geblieben sind oder die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden. Zur Notsuche ist die Überwachung nur dann zulässig, wenn dringende Anhaltspunkte für eine schwere Gefährdung von Gesundheit oder Leben der vermissten Person vorliegen. Ob die Voraussetzungen erfüllt sind, wird in jedem Einzelfall von Amtes wegen durch ein Gericht geprüft. Die Überwachung bleibt dabei nicht geheim, sondern der überwachten Person werden der Grund, die Art und die Dauer der Überwachung mitgeteilt – spätestens wenn das Vorverfahren abgeschlossen ist.

Welche Folgen hätte ein Verzicht auf die Vorratsdatenspeicherung?

Ein Verzicht auf die Vorratsdatenspeicherung würde die Verfolgung von Straftaten erschweren und hätte damit unerwünschte Auswirkungen auf die öffentliche Sicherheit. Die Polizei könnte Spuren, die Täter am Telefon und im Internet hinterlassen, nicht mehr auswerten, ob es sich nun um Cyberkriminalität, Kinderpornographie, Drogenhandel, Tötungs- und Vermögensdelikte oder Terrorismus handelt. Ohne Randdatenspeicherung würde auch die Suche nach vermissten und verurteilten Personen erschwert: Es liesse sich zum Beispiel nur schwer rekonstruieren, wo jemand zuletzt telefoniert hat.

In welchen Fällen dürfen sogenannte Bundestrojaner (in der Fachsprache GovWare oder Government Ware) eingesetzt werden und von wem genau?

Der Bundesrat hat entschieden, eine klare rechtliche Grundlage für den Einsatz von sogenannter GovWare zu schaffen. Der Einsatz soll nur für einen Katalog von schweren Straftaten zulässig sein, der im Vergleich zur herkömmlichen Überwachung des Post- und Fernmeldeverkehrs (Art. 269 ff. StPO) eingeschränkt ist. Es handelt sich dabei um Straftaten, zu deren Verfolgung auch eine verdeckte Ermittlung angeordnet werden könnte (Art. 286 Abs. 2 StPO). Der Einsatz soll ausdrücklich auf die Überwachung des Fernmeldeverkehrs beschränkt bleiben. Nicht gestattet bleiben also Online-Durchsuchungen von Computern oder etwa die Überwachung eines Raumes mit dem Mikrofon oder der Kamera eines Computers. Der Einsatz muss darüber hinaus in jedem Fall von der Staatsanwaltschaft angeordnet und vom Zwangsmassnahmengericht genehmigt werden.

Weshalb braucht es GovWare oder Bundestrojaner überhaupt?

Die GovWare ist erforderlich, damit die Strafverfolgung von Kriminellen mit der technischen Entwicklung Schritt halten kann. Es geht nicht darum, mehr zu überwachen, geschweige denn, auf Vorrat zu "schnüffeln" oder einen Computer zu durchsuchen. Den Strafverfolgungsbehörden müssen aber jene Mittel zur Verfügung stehen, die sie brauchen, um schwere Straftaten verfolgen zu können. Sonst können Kriminelle moderne Kommunikationsmittel nutzen und die Strafverfolgung hat das Nachsehen: Drogenhändler können zum Beispiel via verschlüsselte Internet-Telefonie ihre Geschäfte abwickeln – im Wissen darum, dass sie dabei sicher nicht überwacht werden.

Was tun die Strafverfolgungsbehörden, um GovWare und deren Einsatz so sicher wie möglich zu machen und Missbräuche zu verhindern?

Um einen Missbrauch der GovWare zu verhindern, ist eine Kombination aus technischen und organisatorischen Vorkehrungen nötig. Technisch ist Folgendes vorgesehen: Die Strafverfolgungsbehörden definieren die nötigen Sicherheitsfunktionen; eine unabhängige Stelle verifiziert, ob diese Sicherheitsfunktionen vollständig sind und ob sie nach den anerkannten Standards eingebaut sind. Zu den organisatorischen Massnahmen gehört, dass die Strafverfolgungsbehörden einen detaillierten Prozess für den Einsatz und den Betrieb der GovWare beschreiben. Bestimmt werden dabei unter anderem die Berechtigungen der beteiligten Personen oder der Umgang mit dem Informatiksystem. Schliesslich sorgt eine lückenlose Protokollierung dafür, dass sämtliche Schritte von der Beantragung über die Bewilligung bis zum Abschluss der Überwachung nachvollziehbar sind, auch für das Gericht. All das minimiert die Wahrscheinlichkeit, dass es zu einem Missbrauch der GovWare kommt.; Vor Gericht dürfen Erkenntnisse aus einer Telefonüberwachung nur dann als Beweise verwertet werden, wenn die Überwachung auch für die Erhebung dieser Beweise angeordnet und korrekt bewilligt worden war.

Es wird behauptet, dass das Eidgenössische Justiz- und Polizeidepartement (EJPD) und das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) die Software für die GovWare gemeinsam erwerben und einsetzen wollen. Ist diese Aussage richtig? Laufen dazu bereits Vorbereitungen?
Es besteht keine Absicht, dass das EJPD und das VBS eine GovWare gemeinsam beschaffen oder nutzen werden. Deshalb wird eine solche Zusammenarbeit auch nicht vorbereitet.

Sind die Bedenken eines "Schnüffelstaates" bzw. die Angst vor Übergriffen in die Privatsphäre wirklich unberechtigt?
Ja, denn es ist unzulässig, die Inhalte der Telefongespräche und der Internet-Aktivitäten präventiv und im Sinne eines Geheimdienstes zu überwachen. Die Überwachung ist nur dann möglich, wenn ein Strafverfahren wegen eines schweren Delikts eröffnet wurde, und sie muss immer auch von einem Gericht genehmigt werden. Der Blick in die Statistik zeigt, dass es in etwa 1,5 Prozent aller Delikte zu einer Überwachung kommt. Konkret standen 2013 den 725'678 Delikten 10'860 Überwachungen gegenüber, wobei wie üblich mehrere Überwachungen auf ein Delikt entfielen, wenn zum Beispiel der Festnetzanschluss und mehrere Handys eines Drogendealers überwacht werden müssen.

Wie sieht es mit der Einführung des so genannten Interception System Schweiz (ISS) aus? Müsste dazu nicht eigentlich zuerst die Revision der BÜPF abgeschlossen sein?
Der Dienst ÜPF betreibt ein Informationssystem, über das er den Strafverfolgungsbehörden die Daten der Fernmeldeanbieterinnen zur Verfügung stellt, wenn die gesetzlichen Voraussetzungen dafür erfüllt sind. Dieses System ist am Ende seiner Lebensdauer angelangt und wird derzeit abgelöst durch ein Ersatzsystem, das Interception System Schweiz (ISS). Dessen Funktionsumfang entspricht demjenigen des bisherigen Systems und wird den aktuellen rechtlichen Anforderungen genügen. Wenn das revidierte Bundesgesetz betreffend Überwachung des Post- und Fernmeldeverkehrs (BÜPF) in Kraft tritt, kann das neue Informatiksystem den neuen Anforderungen angepasst werden. Das System ISS wird nach aktueller Planung in der ersten Hälfte 2015 in Betrieb gehen, in Abstimmung mit den Anbietern von Telefon- und Internetverbindungen sowie den Strafverfolgungsbehörden.