SSK | CPS
Schweizerische Staatsanwälte-Konferenz
Conférence des procureurs de Suisse
Conferenza dei procuratori della Svizzera

Informationen der Schweizerischen Staatsanwälte-Konferenz (SSK I CPS) zur Revision des BÜPF

Die Revision des BÜPF und vor allem die damit verbundenen Anpassungen der Strafprozessordnung haben für die Praxis der Strafverfolgungsbehörden eine zentrale Bedeutung, da die dadurch gewonnenen Beweismittel vorab in Verfahren gegen Schwerkriminelle für den Verfahrensausgang oft entscheidend oder zumindest mitentscheidend sind. Zu einigen revidierten Punkten vertritt die SSK folgende Positionen.

1. Keine Überwachung nach BÜPF ohne Strafverfahren durch die Staatsanwaltschaft

Die SSK betont zunächst, dass eine nach BÜPF angeordnete Überwachung des Fernmeldeverkehrs ein Strafverfahren voraussetzt. Einzige Ausnahme ist die Suche nach vermissten Personen. Zur Eröffnung eines Strafverfahrens sind konkrete Fakten nötig, die einen hinreichenden Verdacht für die Staatsanwaltschaft begründen. Vermutungen genügen nicht. Zudem ist nötig, dass sich dieser hinreichende Verdacht zu einem dringenden Verdacht hin verdichtet. **Die Überwachung des Fernmeldeverkehrs unterliegt sodann der Überprüfung durch das unabhängige Zwangsmassnahmengericht**.

Gestützt auf das BÜPF können in keiner Weise Überwachungsmassnahmen für den Nachrichtendienst des Bundes (NDB) angeordnet werden.

2. Anwendungsbereich: kleine Anbieterinnen von Fernmeldedienstleistungen sind nicht verpflichtet, Überwachungen durchzuführen, sondern lediglich zu dulden

Die Revision des BÜPF sieht vor, dass auch kleine Anbieterinnen von Fernmeldedienstleistungen (Hotels, Restaurants, Cafés, Cybercafés,…) grundsätzlich diesem Gesetz unterstellt sind. Das BÜPF sieht für diese kleinen Anbieterinnen jedoch keine Pflicht vor, Überwachungen selber durchzuführen. Diese haben lediglich eine Duldungspflicht. Es ist deshalb irreführend zu behaupten, dass jeder, der einem Kollegen einen Hotspot zur Verfügung stellt, die Pflichten nach BÜPF erfüllen muss. Dieser ist nur verpflichtet, mit den Behörden mitzuwirken.

3. GovWare: sie sind zur heutigen Kriminalitätsbekämpfung notwendig; ihr Einsatz ist an strenge gesetzliche Voraussetzungen gebunden und bewirkt keinen unverhältnismässigen Eingriff in die Privatsphäre und die Informatiksicherheit

Der Einsatz von GovWare („Staatstrojaner“) ist notwendig, damit die Strafverfolgung mit der technischen Entwicklung (z.B. Verschlüsselung und Internettelephonie) Schritt halten kann und eine wirksame Kriminalitätsbekämpfung gewährleistet ist. Die Revision des BÜPF beschränkt gesetzlich den Einsatz von GovWare in verschiedener Weise, um die Privatsphäre zu schützen und unverhältnismässige Überwachungen zu verhindern:

- **Der Einsatz der GovWare gemäss Gesetzesentwurf schafft keine neuen Überwachungsmöglichkeiten, sondern ermöglicht einzig, dass bisher mögliche Überwachungsmassnahmen, die aufgrund der technischen Entwicklung nicht mehr möglich sind, möglich bleiben.**

- **Der Einsatz von GovWare darf nur dazu dienen, den Inhalt der Kommunikation und die Randdaten des Fernmeldeverkehrs zu erheben.** Die Angst, es könnten mit solchen Programmen "beliebige System- und Nutzerdaten ohne Wissen des Inhabers kopiert, verändert, gelöscht oder hinzugefügt werden", ist verständlich, aber unbegründet. Jede GovWare muss individuell auf die Besonderheiten des benützten Zielgerätes programmiert werden. Der Hersteller (in aller Regel ein Privatunternehmen) wird dazu verpflichtet das Programm so zu entwickeln, dass dieses nur auf die erlaubten Überwachungsmassnahmen beschränkt ist.

- **Die Staatsanwaltschaft muss genau bezeichnen, welche Datentypen durch GovWare ausgeleitet werden.** Das Zwangsmassnahmengericht wird so den Umfang der ausgeleiteten Datentypen präzis überprüfen.

- **Die Überwachung mittels GovWare ist nur zulässig, wenn eine konventionelle Überwachung erfolglos blieb oder aussichtslos ist.**

- **Der Einsatz von GovWare ist nur zulässig, wenn es um schwerste Delikte geht, zu deren Aufklärung auch eine verdeckte Ermittlung zulässig ist.** Dies ist eine klare Einschränkung gegenüber der konventionellen Überwachung. Diese kann zur Aufklärung von weitaus mehr Delikten angeordnet werden.

- **Die Staatsanwaltschaft ist verpflichtet, alle Daten zu vernichten, die über den Inhalt der Kommunikation und die Randdaten des Fernmeldeverkehrs hinausgehen,** Falls ungenau programmierte GovWare unerwünschte Daten liefert, ordnet das Gesetz klar an, dass die Erkenntnisse aus diesen Daten nicht verwendet werden dürfen.

- **GovWare schaffen auf dem Zielsystem keine Sicherheitslücken.** Aus der Diskussion über die in Deutschland enttarnte GovWare stellt sich die Frage, ob ein Angreifer die so entdeckte Sicherheitslücke zu eigenen Zwecken ausnützen konnte. Dieses Risiko ist in der Schweiz nicht zu befürchten. GovWare wird wegen der hohen technischen und finanziellen Vorgaben sehr selten eingesetzt. Dazu wird es auf die Besonderheiten des benützten Zielgerätes und der angeordneten Überwachung programmiert. Es ist deshalb grundsätzlich nicht damit zu rechnen, dass bei allen GovWare-Einsätzen ein gemeinsames Grundmodul wie in Deutschland benützt wird.

4. Verlängerung der Randdaten-Frist: eine Frist von 12 Monaten ist zur Aufklärung von schweren Straftaten und von der Schweiz über Internet begangene Delikte (z.B. Kinder-pornografie) notwendig

Es ist zu betonen, dass durch die Fristverlängerung auf 12 Monate nur die sogenannten Randdaten (Mobil- und Festnetznummern, IP-Adressen) betroffen sind, jedoch nicht die Gesprächsinhalte. Aus der Erfahrung der Strafverfolgungsbehörden geht hervor, dass die 6 Monatefrist zur Aufklärung von schweren oder über Internet begangenen Straftaten zu kurz ist. Im Wesentlichen sind folgende Fall-Konstellationen relevant:

- Bei **Gewaltdelikten** (Tötungsdelikte, Raub, bewaffneter Überfall,…) gelingt es bisweilen erst nach mehr als 6 Monaten, einen Verdächtigen zu ermitteln, z.B. wenn der Täter sich auf der Flucht befindet (grenzüberschreitende Kriminalität). Seine Randdaten zur Tatzeit können ohne verlängerte Frist nicht mehr überprüft werden. Die Strafverfolgung ist durch diese zu kurze Frist behindert und der Straftäter wird begünstigt.

- Im Bereich der **Cyberkriminalität** erfordern die von ausländischen Behörden selbst oder auf Begehren der Schweiz durchgeführten Untersuchungen mehr als 6 Monate, da Rechtshilfeersuchen nötig sind. Dies gilt insbesondere bei Verfahren gegen **Kinderpornografie-Konsumenten sowie den Verfahren wegen sexuellen Handlungen mit Kindern, die sich aufgrund vorgefundener Beweismittel daraus ergeben können**. Ohne Fristverlängerung kann dann nicht mehr ermittelt werden, wer die fragliche IP-Adresse zur Tatzeit verwendet hat, so dass die Täter unbestraft bleiben.

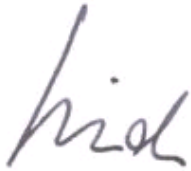
In Deutschland, hat der Europäische Gerichtshof (EuGH) eine EU-Richtlinie zur „Vorratsdatenspeicherung“ als verfassungswidrig bezeichnet. Er erwägt, es sei unverhältnismässig, die Kommunikationsdaten aller Bürgerinnen und Bürger zu speichern, auch wenn sie keinen Anlass zur Strafverfolgung geben würden. Zum anderen bemängelt er, dass die EU-Richtlinie keine Vorschriften darüber enthalte, nach welchen Kriterien welche Behörden auf die Daten zugreifen können. Damit bestünden keine einschränkenden Vorschriften für die Auswertung der Daten durch die Polizei.

Dieser Entscheid des EuGH ist für die Schweiz nicht relevant. Es sind die Anbieterinnen von Fernmeldedienstleistungen (Swisscom, Orange, Sunrise, …), welche die relevanten Kommunikationsdaten speichern und nicht der Staat. Diese Speicherung erfolgt bereits aus vertraglichen Gründen (Rechnungsstellung, Buchhaltung, usw.) während mehr als 6 Monaten, sodass die Daten ohnehin vorhanden sind. **Wenn im EU-Raum Polizeibehörden direkt auf Randdaten zugreifen dürfen, so ist ein solcher Zugriff in der Schweiz unzulässig.** Hier muss ein durch die Staatsanwaltschaft eröffnetes Strafverfahren vorliegen und es muss ein dringender Verdacht auf ein Verbrechen oder Vergehen gegeben sein. Die Erhebung der Randdaten unterliegt sodann der Genehmigung durch das Zwangsmassnahmengericht, das die gesetzlichen Voraussetzungen und die Verhältnismässigkeit überprüft. Der Betroffene muss über die Datenerhebung nachträglich informiert werden und kann dagegen auch Beschwerde erheben.

Mit den strengen gesetzlichen Voraussetzungen des BÜPF ist die Fristverlängerung auf 12 Monate für die Erhebung von Randdaten zur Aufklärung von Straftaten im Rahmen hängiger Strafverfahren gerechtfertigt.

Bern, im Juli 2014

Für die Schweizerische Staatsanwälte-Konferenz (SSK I CPS)



Rolf Grädel, Generalstaatsanwalt des Kantons Bern, Präsident