

Thomas Hansjakob

Einführung von GovWare weiterhin auf Kurs

Zum Revision von Art. 269ter StPO im Rahmen der laufenden BÜPF-Revision

The National Council is the second of the two parliament chambers to deliberate upon the revision of the Federal Mail and Telecommunications Monitoring Act and agrees with the Council of States about permitting the use of GovWare («Staatstrojaner»). The author presents the specifications by the National Council and their practical impacts. (ah)

Category: Articles

Region: Switzerland

Field of law: Data Protection; Data Security

Citation: Thomas Hansjakob, Einführung von GovWare weiterhin auf Kurs, in: Jusletter IT 24 September 2015

Inhaltsübersicht

- I. Das Problem der Überwachung von Internettelefonie
- II. Die Revision des BÜPF
 - 1. Zielsetzung
 - 2. Die Diskussion im Ständerat
 - 3. Die Diskussion in der Rechtskommission des Nationalrates
 - 4. Die Diskussion im Nationalrat
- III. Kurze Würdigung der aktuellen Version
 - 1. Zur Pflicht der Führung von Statistiken (Art. 269ter Abs. 4 StPO)
 - 2. Zur Pflicht der lückenlosen Protokollierung (Art. 269quater Abs. 1 StPO)
 - 3. Zur Pflicht der gesicherten Ausleitung (Art. 269quater Abs. 2 StPO)
 - 4. Zur Pflicht der Überprüfung der Quellcodes (Art. 269quater Abs. 3 StPO)
 - 5. Zum Bundesdienst (Art. 269quater Abs. 4 StPO)
 - 6. Zur Exklusivität (Art. 269quater Abs. 5 StPO)
- IV. Ausblick

I. Das Problem der Überwachung von Internettelefonie

[Rz 1] Warum der Einsatz von GovWare für die Strafverfolger erforderlich und wichtig ist, ob schon dessen Zulässigkeit bisher umstritten war, wurde in Jusletter IT bereits dargestellt¹. Das Wichtigste sei in Kürze wiederholt: Weil die weit verbreiteten universellen Programme für Internet-Telefonie, insbesondere Skype oder Viber, mit einer End-zu-End-Verschlüsselung ausgerüstet sind, läuft eine konventionelle Telefonüberwachung ins Leere: Der Internet-Provider wickelt zwar den Datenverkehr ab, kann ihn aber nicht entschlüsseln. Die Lieferanten der Software, die zur Entschlüsselung allenfalls in der Lage wären, verfügen nicht über den Datenverkehr der Kunden. Die einzige Möglichkeit, solchen Internet-Telefonverkehr zu überwachen, besteht darin, ein besonderes Programm einzusetzen, das von den Strafverfolgungsbehörden üblicherweise als Government Software oder GovWare bezeichnet wird, während die Medien eher den Begriff «Staatstrojaner» verwenden. Dieses Programm wird unbemerkt auf das Endgerät der Zielperson aufgespielt. Es greift dort den noch unverschlüsselten Gesprächsverkehr ab und leitet ihn unverschlüsselt an die Strafverfolgungsbehörden weiter. Ob das nach geltendem Recht zulässig ist, war bisher umstritten.

II. Die Revision des BÜPF

1. Zielsetzung

[Rz 2] Mit der Revision des Gesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs² soll die Kontroverse um die Frage der Zulässigkeit des Einsatzes von GovWare beendet werden. Die Bestimmung soll eine saubere Rechtsgrundlage für den Einsatz von Informatikprogrammen schaffen, die dazu dienen, den Fernmeldeverkehr direkt auf dem zur Kommunikation benützten Gerät (und nicht wie die normale Überwachung erst bei der Fernmeldediensteanbieterin) abzugreifen. Es geht nicht um den Einsatz von GovWare an sich, sondern ausschliesslich darum, dass solche Software «den Inhalt der Kommunikation und die Randdaten des Fernmeldeverkehrs

¹ Vgl. THOMAS HANSJAKOB, Der Einsatz von GovWare in der Schweiz, in: Jusletter IT 15. Mai 2014.

² Botschaft vom 27. Februar 2013 in BBl 2013 2683 ff.

in unverschlüsselter Form» abgreifen und an die Strafverfolgungsbehörden ausleiten soll.

2. Die Diskussion im Ständerat

[Rz 3] Der Gesetzgeber hat erkannt, dass der Einsatz solcher Software nicht unproblematisch ist. Im Wesentlichen drehte sich die Diskussion im Ständerat³ um drei Fragen:

- Wie wird sichergestellt, dass solche Programme nur diejenigen Daten liefern, die sie liefern dürfen?
- Wie wird sichergestellt, dass solche Programme im Zielsystem keine Sicherheitslücken schaffen, die auch von Dritten ausgenützt werden könnten?
- Wie wird dem Umstand Rechnung getragen, dass der Einsatz solcher Programme tiefer in die Rechte des Betroffenen eingreift als eine konventionelle Fernmeldeüberwachung?

[Rz 4] Der Ständerat hat diese Diskussion ausführlich geführt und wollte in Art. 269^{ter} StPO schliesslich nur einen Abs. 4 einführen, der die Staatsanwaltschaft verpflichtet, eine Statistik über Überwachungen, bei denen GovWare eingesetzt wird, zu führen, damit jederzeit klar ist, welche praktische Bedeutung solche Überwachungsmassnahmen haben.

3. Die Diskussion in der Rechtskommission des Nationalrates

[Rz 5] Die Rechtskommission des Nationalrates hat diese Diskussion nochmals aufgenommen und ebenfalls sehr gründlich geführt. Während die Mehrheit der Kommission der Auffassung des Ständerates folgen wollte, gab es eine Reihe von Minderheitsanträgen mit unterschiedlicher Zielsetzung:

- Eine kleine Minderheit wollte auf die Regelung des Einsatzes von GovWare ganz verzichten; damit wäre aber die Kontroverse, ob eine gesetzliche Regelung überhaupt nötig ist, nicht beendet gewesen.
- Eine etwas grössere Minderheit wollte den Einsatz von GovWare ausdrücklich verbieten.
- Ein weiterer Antrag verlangte, dass der Einsatz von GovWare nur zur Verfolgung der Delikte nach Art. 260^{bis} StGB (strafbare Vorbereitungen) zulassen. Der Einsatz wäre dann also nur zur Verfolgung von vorsätzlicher Tötung und Mord, schwerer Körperverletzung, Genitalverstümmelung, Raub, Freiheitsberaubung und Entführung, Geiselnahme, Brandstiftung, Völkermord, Verbrechen gegen die Menschlichkeit und Kriegsverbrechen möglich gewesen.
- Weitere Anträge zielten darauf ab, dass GovWare möglichst sicher ist, indem sie z.B. nicht in Ländern beschafft wird, in denen «grossangelegte Fernmeldeüberwachung» betrieben wird (gemeint sind wohl vorwiegend die USA), oder indem Programme verboten werden, welche die Systemintegrität gefährden oder Sicherheitslücken öffnen. Eine kleine Minderheit verlangte, dass nur in der Schweiz entwickelte Programme eingesetzt werden dürfen.
- Schliesslich schlug die Kommission vor, in einem neuen Art. 269^{quater} StPO besondere Anforderungen an GovWare zu formulieren und insbesondere auch vorzusehen, dass der Bund einen Dienst führt, der solche Programme beschafft und überprüft. Eine Minderheit wollte die Einhaltung dieser Bestimmung mit einem zusätzlichen Verwertungsverbot sicherstellen.

³ Vgl. AB 2014 S 300 ff.

- Eine Minderheit wollte den vom Ständerat beschlossenen Abs. 4 der Bestimmung («Die Staatsanwaltschaft führt eine Statistik über diese Überwachungen. Der Bundesrat regelt die Einzelheiten.») um die Pflicht ergänzen, diese Statistik zu veröffentlichen.

4. Die Diskussion im Nationalrat

[Rz 6] Der Nationalrat führte seine öffentliche Diskussion in der Junisession 2015. Es wurde eine ungewöhnliche Koalition ersichtlich: Eine Mehrheit von SP und Grünen sah sich unterstützt durch Teile der SVP. Lukas Reimann (SVP), der bei anderen Gelegenheiten für eine Ausweitung und Verschärfung des Strafrechts eintritt und dem Nachrichtendienstgesetz zugestimmt hatte, das präventive Überwachungen zulässt, beschwor sogar: «Ja, heute entscheiden wir tatsächlich, ob die Schweiz weiterhin ein Land der Freiheit und der Bürgerrechte sein will oder ob sie zu einem Polizei- und Überwachungsstaat verkommt.»⁴ Daniel Jositsch (SP), der sonst der Ausweitung von staatlichen Befugnissen eher kritisch gegenübersteht, konterte: «Es hat offenbar mit dem zuständigen Bundesrat zu tun, dass Sie im einen Fall zustimmen und in diesem Fall jetzt ablehnen wollen. Das ist aber weiss Gott kein Grund, ein Gesetz abzulehnen! Oder es hat damit zu tun, dass Sie der Telekommunikationsbranche nahestehen, die das Gesetz nicht will.»⁵

[Rz 7] Das Ergebnis der langen und gründlichen Diskussionen war dann allerdings klar: Der Nationalrat übernahm gegenüber dem Vorschlag des Bundesrates die Änderung von Abs. 4, also der Pflicht, eine Statistik über GovWare-Einsätze zu führen, und ergänzte das Gesetz durch einen neuen Art. 269^{quater} StPO (Anforderungen an die besonderen Informatikprogramme zur Überwachung des Fernmeldeverkehrs) mit folgendem Wortlaut:

¹ Es dürfen nur besondere Informatikprogramme eingesetzt werden, welche die Überwachung lückenlos und unveränderbar protokollieren. Das Protokoll gehört zu den Verkehrsakten.

² Die Ausleitung aus dem überwachten Datenverarbeitungssystem bis zur zuständigen Strafverfolgungsbehörde erfolgt gesichert.

³ Die Strafverfolgungsbehörde stellt sicher, dass der Quellcode überprüft werden kann zwecks Prüfung, dass das Programm nur über gesetzlich zulässige Funktionen verfügt.

⁴ Der Bund führt einen Dienst, welcher die besonderen Informatikprogramme beschafft. Der Dienst hat die Aufgabe, die Informatikprogramme zur Überwachung des Fernmeldeverkehrs zu entwickeln oder sie bei Dritten einzukaufen.

⁵ Die Staatsanwaltschaft setzt ausschliesslich die vom Bund freigegebenen Informatikprogramme ein und entrichtet eine angemessene Gebühr für die Kosten der Beschaffung und Prüfung der besonderen Informatikprogramme.

⁴ AB 2015 N 1147.

⁵ AB 2015 N 1146.

III. Kurze Würdigung der aktuellen Version

1. Zur Pflicht der Führung von Statistiken (Art. 269ter Abs. 4 StPO)

[Rz 8] Grundsätzlich ist es sinnvoll, wenn über den Einsatz von GovWare eine Statistik geführt wird; es geht vor allem auch darum, den Eingriff in die Freiheitsrechte richtig beurteilen zu können und zu überprüfen, ob die (z.B. auch von mir vertretene) Prognose richtig ist, dass nicht in erster Linie restriktive rechtliche Regelungen, sondern vor allem die praktischen Schwierigkeiten und der finanzielle Aufwand dazu führen werden, dass GovWare nicht häufig eingesetzt wird. Der Dienst ÜPF, der heute die konventionellen Überwachungen durchführt, publiziert seine detaillierte Statistik schon bisher⁶; es ist also (auch ohne gesetzliche Vorgabe) davon auszugehen, dass auch künftige Statistiken zum GovWare-Einsatz publiziert werden.

[Rz 9] Systemfremd ist allerdings, dass «die Staatsanwaltschaft» diese Statistik führen soll, wenn es andererseits gemäss dem neuen Art. 269^{quater} StPO eine Bundesstelle ist, welche diese GovWare beschafft. Das ist damit zu erklären, dass gemäss Version des Ständerates noch die Kantone für die Beschaffung der GovWare zuständig waren. Der Nationalrat hat übersehen, dass er mit der Einführung der Pflicht, die GovWare zentral zu beschaffen, auch diese zentrale Stelle damit beauftragen müsste, die entsprechende Statistik zu führen.

2. Zur Pflicht der lückenlosen Protokollierung (Art. 269quater Abs. 1 StPO)

[Rz 10] Dass die eingesetzten Programme die Überwachung lückenlos protokollieren, ist selbstverständlich im Interesse der Strafverfolgungsbehörden. Schwierig bei der Umsetzung dürfte nur die Frage sein, was denn eigentlich lückenlos protokolliert werden soll, nachdem ja eben nicht der gesamte Internetverkehr, sondern nach Art. 269^{ter} Abs. 1 StPO richtigerweise nur «der Inhalt des Kommunikationsverkehrs und die Randdaten» protokolliert werden dürfen. Bei der rasanten Entwicklung der Technologie dürfe es zum Teil fraglich sein, was genau dazu gehört: Bei WhatsApp-Verkehr z.B. nur der Inhalt der Meldungen, oder auch der Status der Übertragung (vom Empfänger erhalten, gelesen, beantwortet) und das Portraitbild, die Mobilnummer und die Statusmeldung, die jeder WhatsApp-User hinterlegt und die jeder Empfänger bei jeder Meldung angezeigt bekommt?

[Rz 11] Klar ist, was der Gesetzgeber mit der Auflage meint, dass die Protokollierung «unveränderbar» sein muss. Bedeuten kann das allerdings nur, dass die Strafbehörden Protokolle erhalten, die sie selbst auf dem Ursprungssystem nicht verändern können. Schon heute kann beispielsweise ein Protokoll eines Telefongesprächs auf dem System des ÜPF abgehört, aber auch als Ton-Datei heruntergeladen werden. Diese Datei könnte dann selbstverständlich vom Benutzer auch bearbeitet, insbesondere geschnitten werden, und das lässt sich denn auch technisch gar nicht verhindern. Abgesehen davon, dass es für die Strafverfolgungsbehörden gar keinen Sinn machen würde, Überwachungsergebnisse «nachzubearbeiten», gibt es seit Einführung des Dienstes im Jahr 1998 nicht den geringsten Hinweis darauf, dass irgend eine Behörde oder gar der Dienst in irgend einem der mittlerweile wohl über 50'000 Überwachungsfälle das Ergebnis einer Überwachung in diesem Sinn bearbeitet (oder anders gesagt: gefälscht) hätte. Die vorgeschlagene Bestimmung ist etwa so sinnvoll und erforderlich, wie es eine analoge Bestimmung in Art. 255 StPO wäre, die verbieten würde,

⁶ Abzurufen unter <https://www.li.admin.ch/> (alle Internetquellen zuletzt besucht am 18. September 2015).

dass ein abgenommenes DNA-Profil nachträglich verändert wird.

3. Zur Pflicht der gesicherten Ausleitung (Art. 269quater Abs. 2 StPO)

[Rz 12] Auch hier wird eine Selbstverständlichkeit geregelt: Weder der Dienst noch die Strafverfolgungsbehörden hätten ein Interesse daran, dass Überwachungsdaten auf ungesicherten Leitungen ausgetauscht werden.

4. Zur Pflicht der Überprüfung der Quellcodes (Art. 269quater Abs. 3 StPO)

[Rz 13] Es handelt sich dabei um eine Bestimmung, die einer Zusicherung der Polizeibehörden in den Hearings des Ständerates entspricht: Dem Einwand, man wisse nie, was ein von einem privaten Anbieter beschafftes Programm ausser dem, wofür es bestellt wurde, sonst noch könne, wurde entgegengehalten, dass die Lieferanten verpflichtet würden, den Quellcode der Programme offen zu legen.

5. Zum Bundesdienst (Art. 269quater Abs. 4 StPO)

[Rz 14] Der Dienst ÜPF beim Bund, der heute die konventionellen Überwachungen abwickelt, hat sich stets dagegen gewehrt, auch Funktionen bei der Überwachung mittels GovWare zu übernehmen. Er tat dies in der Regel einerseits mit dem Argument, dass das Einspielen solcher Programme auf den Geräten der Beschuldigten eine klassische Polizeiaufgabe sei; zum andern befürchtete er auch einen gewissen Reputationsschaden, der mit dem Einsatz solcher Programme verbunden sein könnte. Der Dienst ÜPF ist denn auch nicht als operative Behörde konzipiert, welche polizeiliche Aufgaben wahrnehmen soll, sondern er versteht sich (zu Recht) nur als Mittler zwischen Anbieterinnen und Polizeibehörden, welcher den Datenverkehr der Anbieterinnen in definierter Form entgegennimmt und den Polizeibehörden zur Verfügung stellt, ohne sich um taktische Fragen oder um die Inhalte der Daten kümmern zu müssen.

[Rz 15] Es macht allerdings zweifellos Sinn, wenn die schwierige Aufgabe, GovWare zu beschaffen und zu überprüfen und allenfalls sogar selbst zu entwickeln, von nur *einer* Behörde in der Schweiz übernommen wird, die sich dann genügend Erfahrung verschaffen kann. Der Bundesrat wird sorgfältig prüfen müssen, ob er diese Aufgabe dem Dienst ÜPF überträgt oder ob sie nicht anderswo – beispielsweise bei fedpol – besser aufgehoben ist.

6. Zur Exklusivität (Art. 269quater Abs. 5 StPO)

[Rz 16] Es ist konsequent, den Staatsanwaltschaften vorzuschreiben, dass sie nur zentral beschaffte GovWare einsetzen, wenn schon ein solcher zentraler Dienst geschaffen wird. Die Regelung der Gebührenpflicht will wohl auf Umwegen erreichen, dass die Staatsanwaltschaften für alle Kosten aufkommen müssen, welche bei der Beschaffung und Prüfung von GovWare entstehen, wenn sie die Programme im Einzelfall einsetzen. Die Schwierigkeit dabei wird vor allem in der Einführungsphase darin bestehen, eine Abschätzung darüber vorzunehmen, wie oft ein zentral beschafftes Programm

insgesamt eingesetzt werden wird, um zu kalkulieren, welche Gebühr dafür in Rechnung zu stellen ist. Wie bisher beim Dienst ÜPF wird es auch bei der Beschaffung von GovWare so sein, dass gewisse Kosten zunächst vom Bund zu tragen sind und unklar ist, wie weit sie tatsächlich auf die Endkunden, also die einzelnen Staatsanwaltschaften, abgewälzt werden können.

IV. Ausblick

[Rz 17] Die Differenzen zwischen National- und Ständerat sind nicht nur betreffend GovWare, sondern auch mit Blick auf die meisten übrigen Bestimmungen der BÜPF-Revision relativ gering. Es kann deshalb davon ausgegangen werden, dass diese Differenzen in der September-Session bereinigt werden können und dass das Gesetz auch in der Schlussabstimmung eine komfortable Mehrheit finden wird.

[Rz 18] Allerdings hat sich – ungewöhnlich für die Schweiz – schon vor den Beratungen im Parlament eine Gruppe gebildet, die das Referendum gegen die BÜPF-Revision ergreifen will. Gemäss Homepage⁷ kommen die Opponenten «aus allen politischen Lagern von SVP und FDP bis hin zu SP und AL. Vor allem die Jugendparteien gehören zu den grossen Gegnern des Überwachungsgesetzes, aber auch zivilgesellschaftliche Organisationen wie die digitale Gesellschaft, Grundrechte.ch oder der Chaos Computer Club. Wirtschaftsverbände wie zum Beispiel der Verband der ICT-Anbieter Swico gehören ebenfalls zu den Organisationen, welche das Referendum unterstützen. Die konkreten Vorbereitungen für die Unterschriftensammlung wurden von dieser breiten Allianz am 24. Juni 2015 in Olten in die Wege geleitet.» Nachdem vor allem die Internetbranche erhebliche finanzielle Interessen daran hat, dass die Vorratsdatenspeicherung abgeschafft oder zumindest die Frist dafür nicht verlängert wird, ist damit zu rechnen, dass das Referendumsverfahren ohne Weiteres finanziert werden kann. Damit dürfte es im Lauf des Jahres 2016 zu einer Volksabstimmung kommen, sodass die Strafverfolger jedenfalls noch bis ins Jahr 2017 hinein ohne GovWare auskommen müssen. Das wird vor allem wegen der zunehmenden Verbreitung von WhatsApp, Skype und andern verschlüsselten Kommunikationsdiensten in der Strafverfolgung zu immer grösser werdenden Überwachungslücken führen.

Dr. THOMAS HANSJAKOB ist Erster Staatsanwalt des Kantons St. Gallen und publiziert regelmässig zu Fragen der verdeckten Beweiserhebung.

⁷ <http://stopbuepf.ch>.