www.jusletter-it.eu

Thomas Hansjakob

Der Einsatz von GovWare in der Schweiz

Zum geplanten Art. 269ter StPO

Der Ständerat hat als Erstrat die Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs beraten und damit auch den Vorschlag befürwortet, künftig den Einsatz von GovWare («Staatstrojanern») zuzulassen. Der Autor stellt die geplanten Änderungen und ihre Auswirkungen auf die Praxis vor.

Kategorie: Beiträge
Rechtsgebiete: Datenschutz; Datensicherheit
Region: Schweiz

Zitiervorschlag: Thomas Hansjakob, Der Einsatz von GovWare in der Schweiz, in: Jusletter IT 15. Mai 2014

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

1 Das Problem der Überwachung von Internettelefonie

1.1 Das technische Problem

[Rz 1] Wenn Strafverfolgungsbehörden normale Telefonie überwachen wollen, dann erteilen sie dazu der Fernmeldedienstanbieterin, welche das Abonnement des betreffenden Kunden verwaltet (üblicherweise als Provider bezeichnet), den Auftrag, den Gesprächsverkehr samt den Randdaten an die Polizeibehörden auszuleiten. In der Schweiz besteht zu diesem Zweck ein eigener Dienst beim Eidgenössischen Justiz- und Polizeidepartement (Dienst zur Überwachung des Post- und Fernmeldeverkehrs, Dienst ÜPF), der die Verfügungen der Staatsanwaltschaft entgegennimmt, an die betroffene Anbieterin weiter leitet und von ihr dann den Fernmeldeverkehr in elektronischer Form entgegennimmt und so auf einem EDV-System ablegt, dass die zuständige Polizeibehörde ihn dort abrufen und auswerten kann.

[Rz 2] Dieses System funktioniert dann nicht, wenn die Zielperson nicht über einen Provider telefoniert, sondern eines der weit verbreiteten universellen Programme für Internet-Telefonie, meist Skype oder Viber, benützt. Diese Systeme sind mit einer End-zu-End-Verschlüsselung ausgerüstet; die Gespräche werden direkt auf dem Gerät des Absenders verschlüsselt, paketweise weitergeleitet und erst auf dem Gerät des Empfängers wieder entschlüsselt. Bei diesem System läuft die konventionelle Überwachung ins Leere, weil der Internet-Provider den Datenverkehr zwar abwickelt, aber nicht entschlüsseln kann, während die Lieferanten der Software, die zur Entschlüsselung allenfalls in der Lage wären, nicht über den Datenverkehr der Kunden verfügen.

[Rz 3] 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 unverschlüsselten Gesprächsverkehr ab und leitet ihn unverschlüsselt an die Strafverfolgungsbehörden weiter.

1.2 Das rechtliche Problem

[Rz 4] In der Schweiz ist allerdings umstritten, ob eine genügende rechtliche Grundlage für den Einsatz von GovWare vorhanden ist. Während gewisse Autoren und Gerichte davon ausgehen, dass Fernmeldeüberwachungen nach Art. 269 der Strafprozessordnung (StPO) unabhängig von

der eingesetzten Technik zulässig seien oder dass jedenfalls die Möglichkeit der technischen Überwachung nach Art. 280 StPO auch den Einsatz von GovWare ermöglichen, sind andere Autoren und Gerichte der Auffassung, Art. 269 StPO sei nur als gesetzliche Grundlage für den Eingriff ins Fernmeldegeheimnis und nicht auch für das Eindringen in ein Datenverarbeitungssystem tauglich, und Art. 280 StPO regle den versteckten Einsatz von Computerprogrammen nicht, sodass eine gesetzliche Grundlage für den Einsatz von GovWare fehle.[1]

2 Die Revision des BÜPF

2.1 Zielsetzung

[Rz 5] Mit der Revision des Gesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)[2] soll die Kontroverse um die Frage 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 Fernmeldedienstanbieterin) abzugreifen. Es geht also nicht um den Einsatz von GovWare an sich, sondern ausschliesslich darum, dass solche Software «den Inhalt der Kommunikation und die Randdaten des Fernmeldeverkehrs in unverschlüsselter Form» abgreifen und an die Strafverfolgungsbehörden ausleiten soll.

2.2 Problematik

[Rz 6] Der Gesetzgeber hat erkannt, dass der Einsatz solcher Software nicht unproblematisch ist. Im Wesentlichen drehte sich die Diskussion im Ständerat[3] 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?

2.3 Etwas Technik

[Rz 7] Um die tatsächliche Problematik des Einsatzes von GovWare zu verstehen, sollte man wissen, in welcher Weise solche Programme heute tatsächlich eingesetzt werden. Denn wer die Rahmenbedingungen solcher Einsätze kennt, der weiss auch, dass die in der öffentlichen Diskussion

---

1 Näheres zur Kontroverse bei T. Hansjakob, Einsatz von Gov-Ware – zulässig oder nicht?, in: Jusletter 5. Dezember 2011; O.Jotterand/J. Müller/J. Treccani, L'utilisation du cheval de Troie comme mesure de surveillance secrète, in: Jusletter 21. Mai 2012; S. Métille, Les mesures de surveillance prévues par le CPP: quelles places pour le cheval de Troie, l'IMSI-Catcher ou les puces RFID ?, in: Jusletter 19. Dezember 2011; C. Riss/N. Beranek Zanon, Art. 280 StPO genügt nicht als gesetzliche Grundlage für den Einsatz von Staatstrojanern, in: Jusletter 9. Juli 2012

2 Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27. Februar 2013 in BBl 2013 2683ff.

3 Vgl. AB 2014 S 300ff.

geäusserten Bedenken zu einem grossen Teil unbegründet sind.

[Rz 8] GovWare gibt es auf dem Markt nicht «ab Stange» zu kaufen, weil solche Programme auf die von der Zielperson benützte Hard- und Software angepasst werden muss[4]. Natürlich sind gewisse Komponenten solcher Programme immer gleich aufgebaut, für den konkreten Einsatz spielt aber eine Rolle, wie das Zielgerät mit dem Internet verbunden wird und welche Programme die Zielperson benützt. Wesentlich sind insbesondere das verwendete Betriebssystem[5], der eingesetzte Internetbrowser[6], das benützte Virenschutzprogramm[7] und die Applikation, die zur verschlüsselten Kommunikation verwendet wird[8], denn an diese Rahmenbedingungen muss die GovWare individuell angepasst werden, damit sie auf dem überwachten Gerät überhaupt funktioniert und vom Rechner, aber nicht vom Benutzer erkannt wird. Diese Informationen erhält man in der Regel nur mit einer konventionellen Internetüberwachung. Das heisst also, dass der Einsatz von GovWare normalerweise erst möglich wird, wenn vorher eine konventionelle Internetüberwachung verfügt, bewilligt und durchgeführt wurde.

[Rz 9] Um die GovWare auf das System einspielen zu können, gibt es grundsätzlich zwei Möglichkeiten: Entweder verschaffen sich die Polizeibehörden Zugriff auf das Gerät selbst, oder sie spielen die GovWare über Internet so auf, wie auch Schadprogramme normalerweise auf den Rechner kommen[9]. Die erste Variante setzt voraus, dass man die Zielperson observiert und einen geeigneten Weg findet, für kurze Zeit unbemerkt an das Endgerät zu kommen, das allerdings zu diesem Zeitpunkt laufen muss und nicht mit einem Passwort geschützt sein darf. Die zweite Variante ist nur umsetzbar, wenn man das Surfverhalten der Zielperson kennt, weil man nur auf diese Weise die Software unbemerkt einschleusen kann.

[Rz 10] Wer GovWare einsetzt, hat also einen ausserordentlich grossen Aufwand zu leisten: Mit einer konventionellen Internetüberwachung muss festgestellt werden, welche Hard- und Software die Zielperson benützt. Anschliessend muss die GovWare anhand dieser Rahmenbedingungen so programmiert werden, dass sie auf das Zielsystem aufgespielt werden kann und dort dann auch tatsächlich funktioniert. Schliesslich ist ein weiterer sehr hoher Aufwand notwendig, um die GovWare tatsächlich auf das Zielsystem aufzuspielen. Insgesamt sind also die persönlichen, aber auch die technischen und finanziellen Ressourcen für den Einsatz von GovWare mit einer konventionellen Überwachung in keiner Art zu vergleichen: Der Einsatz von GovWare kostet in jedem Fall ein Mehrfaches des Einsatzes einer konventionellen Überwachung.

2.4 Die Umsetzung der Rahmenbedingungen durch den Gesetzgeber

2.4.1 Überwachbare Daten

[Rz 11] Die Frage, welche Daten mit dem Einsatz von GovWare überhaupt erhältlich sind, beantwortet Art. 269ter SPO genau: es geht nur um «den Inhalt der Kommunikation und die Randdaten des Fernmeldeverkehrs». Die Angst, es könnten mit solchen Programmen «beliebige System- und

4 GovWare kann auf Computern, aber auch auf Smartphones, also auf modernen Handys, eingesetzt werden.

5 Z.B. Windows 8, Android oder iOs.

6 Z.B. Internet Explorer, Mozilla Firefox oder Safari.

7 Z.B. Norton Antivirus, Kaspersky Internet Security oder Avira.

8 Z.B. Skype, WhatsApp oder Viber.

9 Z.B. in einem Mail, das die GovWare getarnt in einem Anhang enthält.

Nutzerdaten ohne Wissen des Inhabers kopiert, verändert, gelöscht oder hinzugefügt werden»[10], ist unbegründet. Zwar wäre es möglich, GovWare so zu programmieren, und in Deutschland wurden denn auch Programme mit solchen Fähigkeiten entwickelt.

[Rz 12] Weil aber nicht einfach Standardprogramme eingesetzt werden können, sondern jede GovWare ohnehin auf die Besonderheiten des benützten Zielgerätes programmiert werden muss, kann der Hersteller auch gleich verpflichtet werden, die rechtlichen Rahmenbedingungen einzuhalten. Er wird dann schon aus eigenem Interesse nicht ein Programm entwickeln, das mehr kann, als es dürfte. Weil die Anbieterinnen von GovWare von den Polizeibehörden vertraglich verpflichtet werden, den Quellcode ihrer Programme offen zu legen, sodass jederzeit überprüft werden kann, wie sie technisch funktionieren, ist sichergestellt, dass die GovWare vom Lieferanten richtig programmiert wird. Sie leitet deshalb nur diejenigen Daten aus, deren Ausleitung von der Staatsanwaltschaft tatsächlich angeordnet und vom Zwangsmassnahmengericht auch genehmigt wurde.

[Rz 13] Art. 269ter Abs. 2 lit. a StPO stellt zudem sicher, dass die Staatsanwaltschaft in der Anordnung genau bezeichnen muss, welche Datentypen ausgeleitet werden sollen, und Art. 269ter Abs. 3 StPO sieht für den (praktisch unwahrscheinlichen) Fall, dass ungenau programmierte GovWare unerwünschte Daten liefert, vor, dass diese Daten sofort vernichtet und Erkenntnisse daraus nicht verwendet werden.

[Rz 14] Der Gesetzgeber tut also alles, was notwendig ist, um den Einsatz von GovWare auf die Überwachung von verschlüsselter Kommunikation zu begrenzen, die unverschlüsselt nach Art. 269 StPO überwachbar wäre. Das überzeugt nicht alle Kritiker: Natürlich kann immer behauptet werden, was technisch möglich sei, werde in Wirklichkeit dann auch getan, ohne dass man es genügend kontrollieren könne[11]. Dem wäre allerdings entgegenzuhalten, dass die Polizei auch auf andern Gebieten mehr tun könnte, als sie tun darf, ohne dass Anhaltspunkte dafür vorhanden sind, dass sie Beweisverbote systematisch missachtet – ohne ein Minimum an Vertrauen in die Strafverfolger kommt der Gesetzgeber nirgends aus.

[Rz 15] Der Ständerat hat denn auch bei der Beratung von Art. 269ter StPO eine einzige Anpassung vorgenommen: Die Staatsanwaltschaften sollen verpflichtet werden, eine Statistik über den Einsatz von GovWare zu führen[12]. Das ist sinnvoll und führt zu nur unerheblichem zusätzlichen Aufwand, weil ohnehin nur in seltenen Fällen GovWare eingesetzt wird[13].

---

10 So noch die Botschaft (Fn. 2), BBl 2013 2775.

11 Beispielhaft die Argumentation von Ständerätin Fetz in den Beratungen: «Staatliche Schadsoftware darf unter bestimmten Bedingungen eingesetzt werden, und zwar ohne dass klar definiert würde, wo die Grenzen der Möglichkeiten dieser Programme und damit ihre Schadensgrenzen liegen. Das ist das Heikle. Es ist eine hochtechnische Angelegenheit, die aber im Artikel überhaupt nicht definiert wird; es werden keine Grenzen gesetzt.» (AB 2014 S 301).

12 AB 2014 S 300. Diese Pflicht richtet sich nicht an den Dienst ÜPF, weil nicht er, sondern die zuständigen Polizeibehörden von Bund und Kantonen die GovWare einsetzen – zu hoffen ist allerdings, dass der dadurch abgegriffene Kommunikationsverkehr in der Regel weiterhin an den Dienst und nicht direkt an die auswertende Polizeibehörde ausgeleitet wird.

13 Die Zahl solcher Einsätze dürfte zwar etwas steigen, wenn eine saubere gesetzliche Grundlage vorhanden ist; wegen des Aufwandes solcher Massnahmen wird die konventionelle Überwachung aber wohl auch in den nächsten fünf Jahren etwa 100 mal häufiger sein als die Überwachung nach Art. 269ter StPO.

2.4.2 Schaden durch GovWare

[Rz 16] Die Befürchtung, GovWare könnte auf dem Zielsystem nicht nur vorhandene Sicherheitslücken ausnützen, sondern neue Sicherheitslücken schaffen, sodass Schäden auf dem Zielsystem entstehen oder Dritte leichter Schäden anrichten könnten, stammt aus der Diskussion über die in Deutschland eingesetzte und schliesslich enttarnte GovWare. Ich halte diese Befürchtung nicht für realistisch:

[Rz 17] Zum einen muss GovWare individuell programmiert werden. Sie wird in der Schweiz so selten eingesetzt, dass nicht damit zu rechnen ist, dass die gemeinsam eingesetzten Grundmodule rasch identifiziert werden können. Zum andern: Selbst wenn (wie in Deutschland) von einem bestimmten Programm bekannt wird, welche Module es enthält und welche Sicherheitslücken es allenfalls auf dem Zielsystem verursacht, wie sollte dann ein Angreifer herausfinden, wo die fragliche GovWare (vom Benutzer unbemerkt) installiert wurde, um dann die Sicherheitslücke zu eigenen Zwecken ausnützen zu können? Schadsoftware muss breitflächig gestreut werden und zielt auf Sicherheitslücken, die auf zahlreichen Systemen vorhanden sind; es lohnt sich nicht, sie auf nur vereinzelt vorhandene Sicherheitslücken anzupassen[14].

[Rz 18] Ziel des Designs von GovWare ist ohnehin, sie so zu programmieren, dass sie nach Ablauf der bewilligten Überwachungsdauer vom System der Zielperson spurlos gelöscht werden kann. Das ist nötig, damit die entsprechenden Module von der Zielperson nicht nachträglich untersucht werden können. Denn die Zielperson muss ja wie bei jeder Überwachung spätestens vor dem Abschluss der Untersuchung darüber informiert werden, dass ihr Gerät überwacht und dabei GovWare eingesetzt wurde (Art. 279 StPO). Wenn man aber das Programm spurlos entfernen können muss, dann ist das nur realistisch, wenn keine neuen Sicherheitslücken geschaffen oder zumindest allfällig geöffnete Sicherheitslücken wieder geschlossen werden.

2.4.3 Die Frage der Eingriffsschwere

[Rz 19] Der Gesetzgeber führt für den Einsatz von GovWare gegenüber konventionellen Überwachungen zwei zusätzliche Hürden ein, indem das Prinzip der doppelten Subsidiarität und ein engerer Deliktskatalog zu beachten sind:

[Rz 20] Die Überwachung mittels GovWare ist nach Art. 269ter lit. c StPO nur zulässig, wenn eine konventionelle Überwachung erfolglos blieb oder ohnehin aussichtslos wäre. Es gilt also gewissermassen eine doppelte Subsidiarität: Zunächst sind nach Art. 269 Abs.1 lit. c StPO die konventionellen Ermittlungsmethoden auszuschöpfen, erst dann ist eine normale Kommunikationsüberwachung zulässig. Nur wenn auch sie nicht zum Ziel führt, kann gestützt auf Art. 269ter lit. c StPO GovWare eingesetzt werden.

[Rz 21] Während für konventionelle Überwachungen der Deliktskatalog von Art. 269 Abs. 2 StPO gilt, ist der Einsatz von GovWare nur zulässig, wenn es um Delikte nach Art. 286 Abs. 2 StPO geht; es gilt also der Katalog für verdeckte Ermittlungen. Die Idee dahinter war nicht, dass der Einsatz von GovWare mit einer verdeckten Ermittlung vergleichbar wäre (es gäbe denn auch keinen sachlichen Grund dafür), sondern es ging schlichtweg darum, einen engeren Deliktskatalog zu definieren, um der grösseren Eingriffsintensität beim Einsatz von GovWare Rechnung zu tra-

[14] Das zeigt schon der Umstand, dass der einfachste Schutz vor Computerviren darin besteht, auf dem eigenen System ein wenig verbreitetes Betriebssystem und einen selten benützten Browser zu installieren.

gen, und deshalb griff man auf den bereits vorhandenen, etwas engeren Deliktskatalog von Art. 286 Abs. 2 StPO zurück.[15]

[Rz 22] Diese Idee des Gesetzgebers überzeugt allerdings nicht. Zum einen ist der Deliktskatalog von Art. 286 Abs. 2 StPO nur unwesentlich enger als derjenige von Art. 269 Abs. 2 StPO. Zum andern sollte bei der Auswahl der Delikte für die beiden Kataloge neben der Schwere der Straftaten eigentlich eine wesentliche Rolle spielen, für die Aufklärung welcher Delikte die zu regelnde Massnahme überhaupt geeignet ist. Weil es auch bei Art. 269ter StPO um Kommunikationsüberwachung geht, passt der Katalog von Art. 286 StPO deshalb nicht.

[Rz 23] Ein einschränkender Deliktskatalog wäre aber für den Einsatz von GovWare gar nicht nötig: Erstens ist die Hürde für den Einsatz von GovWare ohnehin schon faktisch wesentlich höher als für eine konventionelle Überwachung, weil diese Massnahme um ein Vielfaches aufwändiger und teurer ist. Zweitens müsste der Umstand, dass der Einsatz von GovWare wegen des unbemerkten Aufspielens von Software auf das Gerät der Zielperson mit einem schwerer wiegenden Eingriff in die Rechte des Betroffenen verbunden ist als die konventionelle Überwachung, in Anwendung von Art. 269 Abs. 1 lit. b StPO bei der Prüfung der Verhältnismässigkeit durch Staatsanwaltschaft und Zwangsmassnahmengericht ohnehin berücksichtigt werden. Drittens fragt sich allerdings, ob der Unterschied in der Eingriffsschwere wirklich so erheblich ist, denn letztlich geht es in der Praxis ja nur darum, dass neben konventionellen Telefongesprächen auch Gespräche über Skype überwacht werden, und die Zielperson ist vom einen nicht mehr oder weniger betroffen als vom andern.

3 Gesamtwürdigung

[Rz 24] Mit Art. 269ter StPO will der Gesetzgeber nicht eine neue Form der Überwachung einführen, sondern nur eine neue technische Barriere, die bei der Überwachung des Kommunikationsverkehrs in den letzten Jahren immer wichtiger geworden ist, nämlich die Verschlüsselung von Gesprächen, überwinden. Die damit verbundenen Risiken hat der Bundesrat beim Entwurf von Art. 269ter StPO ausreichend berücksichtigt und eine Regelung geschaffen, die nicht ein Mehr an Überwachung ermöglicht, sondern lediglich die technische Entwicklung berücksichtigt. Es besteht kein Grund, den Strafverfolgungsbehörden zu misstrauen, weil die gesetzlichen, aber auch die faktischen Hürden zum Einsatz von GovWare noch einmal deutlich höher sind als die Hürden für eine konventionelle Kommunikationsüberwachung. Anders als die NSA können die Schweizer Strafverfolgungsbehörden Überwachungen nur dann anordnen, wenn gegen die Zielperson ein dringender Tatverdacht besteht, eine Strafuntersuchung bereits eröffnet wurde, eine Überwachungsverfügung der Staatsanwaltschaft und eine Genehmigung des Zwangsmassnahmengerichtes vorliegt und wenn der Betroffene nachträglich über die Massnahme orientiert wird.

[Rz 25] Das hat denn auch der Ständerat zu Recht so gesehen und den Entwurf des Bundesrates praktisch unverändert übernommen.

Dr. iur. Thomas Hansjakob ist Erster Staatsanwalt des Kantons St. Gallen und publiziert regelmässig zu Fragen der verdeckten Beweiserhebung.

[15] So sinngemäss der Kommissionssprecher, Ständerat Engler, in AB 2014 S 300.