Recht im digitalen Zeitalter

Festgabe Schweizerischer Juristentag 2015 in St. Gallen

Herausgegeben im Auftrag der Rechtswissenschaftlichen Abteilung der Universität St. Gallen von

Lukas Gschwend
Peter Hettich
Markus Müller-Chen
Benjamin Schindler
Isabelle Wildhaber

DIKE

Das Kunstwerk auf dem Umschlagbild stammt von Felice Varini «Dix disques évidés plus neuf moitiés et deux quarts», 2014, Acryl und Folien. Es befindet sich im Bibliotheksgebäude der Universität St. Gallen.

Abgedruckt mit freundlicher Genehmigung des Künstlers. Das Copyright liegt bei Felice Varini und der Universität St. Gallen (HSG).

Fotografie: Hannes Thalmann

Bibliografische Information der ‹Deutschen Bibliothek›.
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über ‹http://dnb.ddb.de› abrufbar.

ISBN 978-3-03751-708-6

www.dike.ch

Einsatz von GovWare in der Strafverfolgung

Zu Notwendigkeit und Anwendungsbereich von Art. 269ter StPO

THOMAS HANSJAKOB

Inhaltsübersicht

I. Das Problem

1. Die Entwicklung der gesetzlichen Regelung

Dass der Fernmeldeverkehr von Personen für die Strafverfolgung interessant sein kann, weiss man schon, seit Fernmeldeverkehr überhaupt existiert. Zwar schrieb das erste Bundesgesetz über das Telephonwesen vom 27. Juni 1889[1] in Art. 17 das Fernmeldegeheimnis fest, ohne vorerst Ausnahmen davon zu statuieren. Bereits im Bundesgesetz über den Telegraphen- und Telephonverkehr vom 14. Oktober 1922[2] (TVG) wurde aber erkannt, dass die Justiz- und Polizeibehörden im Rahmen von Strafuntersuchungen (oder zur Verhinderung von Verbrechen oder Vergehen) Zugang zu Aufzeichnungen über den Fernmeldeverkehr haben müssen.

[1] AS 11 256.
[2] AS 39 13; BBl 1921 III 280; vgl. Art. 7 TVG.

Die Konkretisierung dieser Vorschriften erfolgte zunächst in den Kantonalen Strafprozessordnungen sowie (im Bereich der präventiven Überwachung) allenfalls in den Polizeigesetzen. Mit dem Erlass des Bundesgesetzes über den Schutz der persönlichen Geheimsphäre vom 23. März 1979[3] präzisierte der Bundesgesetzgeber näher, unter welchen Voraussetzungen der Fernmeldeverkehr für Zwecke der Strafverfolgung überwacht werden dürfe und welches Verfahren einzuhalten sei. Diese Regeln galten nicht nur für den Bundesstrafprozess: Ins StGB wurde Art. 179^{octies} eingefügt, der die amtliche Überwachung als straflos erklärte, sofern die Genehmigung des zuständigen Richters eingeholt worden war. Es wurde präzisiert, dass die Genehmigung nur erteilt werden könne zur Verfolgung oder Verhütung eines Verbrechens oder eines Vergehens, dessen Schwere oder Eigenart den Eingriff rechtfertige, oder einer mit Hilfe des Telefons begangenen Straftat. Art. 400bis StGB setzte den Kantonen eine Übergangsfrist von drei Jahren für die Anpassung der kantonalen Prozessordnungen und sah vor, dass der Richter in dieser Zeit, solange das kantonale Recht nicht angepasst sei, unter den Voraussetzungen von Art. 66 BStP Überwachungen verfügen könne.

Vorläufiger Endpunkt dieser Entwicklung war dann der Erlass des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 6. Oktober 2000[4] (BÜPF), das – trotz grundsätzlicher Hoheit der Kantone zum Erlass des Prozessrechts – gesamtschweizerische Regeln für die Fernmeldeüberwachung schuf. Es blieb weiterhin unbestritten, dass der gesamte Fernmeldeverkehr für Zwecke der Strafverfolgung überwachbar sein müsse, wenn auch nur unter einschränkenden Rahmenbedingungen. Art. 3 BÜPF machte die Anordnung von Überwachungen von drei Voraussetzungen abhängig: Es musste (1) ein dringender Tatverdacht auf eine Straftat gemäss einem abschliessenden Deliktskatalog gegen die Zielperson vorliegen; die Schwere der Straftat musste (2) die Überwachung rechtfertigen; es galt (3) das Subsidiaritätsprinzip, eine Überwachung war also nur zulässig, wenn andere Untersuchungshandlungen erfolglos geblieben waren oder die Ermittlungen ohne die Überwachung aussichtslos oder unverhälnismässig erschwert würden.

Die Einführung der Schweiz. Strafprozessordnung änderte an der gesetzlichen Regelung nur wenig: Im Wesentlichen wurden die materiellen Bestimmungen des BÜPF in Art. 269 ff. StPO überführt, während das BÜPF weiterhin die technischen Einzelheiten und die praktische Organisation der Überwachung regelt.

[3] AS 1979 I 1170; BBl 1976 I 529 und BBl 1976 II 1569.
[4] AS 2001 3096; SR 780.1.

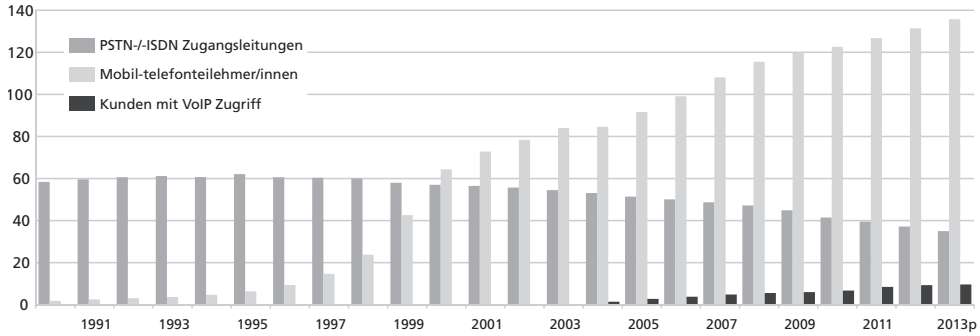
2. Die Entwicklung der Technik

Geändert haben sich aber mittlerweile die Technik und damit das Kommunikationsverhalten der Bevölkerung, und zwar nicht nur unwesentlich, sondern grundlegend:

Während 100 Jahren war im Wesentlichen nur die Festnetztelefonie bekannt; damit war auch klar, wo welcher Telefonanschluss vorhanden war und wer in der Regel damit telefonierte. 1975 wurde in der Schweiz das erste mobile Telefonnetz aufgebaut; das **N**ationale **A**uto**tel**efonnetz prägte denn auch den nur in der Schweiz üblichen Begriff NATEL für diese neue Technologie. Sehr mobil war diese Art der Telefonie nicht, weil die Geräte mehrere Kilogramm wogen. Kommerziell erfolgreich wurde dieses System erstmals mit der Einführung der Natel-C-Technologie im Jahr 1987, welche kleinere Geräte ermöglichte. Erst anfangs der 1990er Jahre stand dann das Natel-D-Netz zur Verfügung, das auch über die Landesgrenzen hinaus funktionierte. Gleichzeitig wurden die Geräte weiterhin kleiner und billiger. Das führte zu einer geradezu explosionsartigen Verbreitung der Mobiltelefonie[5]:

Telefoninfrastruktur in der Schweiz, Entwicklung 1990–2013

pro 100 Einwohner/innen



Mobiltelefone wurden nicht nur zum Führen von Telefongesprächen verwendet: Rasch setzte sich auch der Versand von Textmeldungen via Short Message System (SMS) durch. Im Jahr 1998 wurden in der Schweiz 38 Mio. SMS verschickt, 1999 waren es bereits 288 Mio. schon 2000 wurde dann die Milliardengrenze überschritten. Der Höhepunkt war erst im Jahr 2011 erreicht, als in der Schweiz 6,8 Mia. SMS

[5] Bundesamt für Statistik, abgerufen unter <www.bfs.admin.ch>, Themen, 16.1. Informationsgesellschaft, besucht am 8.1.2015.

verschickt wurden[6]. Seither geht die Zahl jährlich deutlich zurück, was mit einem weiteren Technologiesprung zu tun hat:

Mittlerweile können Mobiltelefone nicht nur zum Telefonieren verwendet werden, sondern wegen der Breitbandzugänge ist auch Datenverkehr über Internet möglich. Auch diese Technologie, die erst seit 2007 in nennenswertem Umfang zur Verfügung steht, hat sich sehr rasch entwickelt: Ende 2014 lag die Zahl der Schweizer Mobilanschlüsse mit Breitbandzugang bereits bei über 6 Mio.[7]; insgesamt waren etwa 10,5 Mio. Mobiltelefone im Betrieb. Die neue Technologie erlaubt es einerseits, jederzeit mit dem Smartphone auf beliebige Internetseiten zuzugreifen, und zwar mittlerweile in einer Geschwindigkeit, die auch flüssiges Surfen zulässt. Möglich ist nun aber auch internetbasierte Kommunikation, die vor allem in zwei Formen verbreitet ist:

- Internettelefonie (im Wesentlichen über Skype, aber auch über Google Hangout, Viber und Facetime) ist vor allem im internationalen Telefonverkehr interessant, weil nur die nationalen Internetgebühren anfallen (und weil neben dem Ton auch das Bild übertragen werden kann, sodass Videotelefonie möglich ist)[8]. Mittlerweile ist die Technik so weit ausgebaut, dass Skype-Nutzer auch mit Leuten telefonieren können, die über das normale Handynetz oder das Festnetztelefon kommunizieren und Skype deshalb gar nicht auf ihrem Gerät installiert haben.
- Textmeldungen über Internet erfolgen heute vorwiegend über Messenger (vor allem über den Marktleader WhatsApp). Anders als bei SMS können mit diesem System neben Text- auch Bild-, Ton- und sogar Filmmeldungen übertragen werden.

Internettelefonie hat sich heute aus nur schwer erklärbaren Gründen noch nicht breit durchgesetzt. Dagegen gilt WhatsApp als der am raschesten wachsende Internetdienst: Das Programm wurde 2009 entwickelt und hatte Ende 2014 weltweit bereits über 700 Mio. Nutzer. In der Schweiz dürften zwei von drei Mobiltelefonbesitzern das Programm geladen haben, jeder von ihnen erhält durchschnittlich über 2'000 (!) Meldungen pro Monat. WhatsApp gehört seit Februar 2014 zum Facebook-Konzern.

3. Die Entwicklung des Marktes

Für die Entwicklung des Marktes ist nicht nur der technologische Fortschritt, sondern auch die Marketingstrategie der Anbieterinnen von Bedeutung. Mobiltelefone setz-

[6] Bundesamt für Kommunikation, Amtliche Fernmeldestatistik 2012, abgerufen unter <www.bakom.admin.ch>, besucht am 30.1.2015.

[7] Bundesamt für Statistik (Fn. 5).

[8] Vgl. dazu Charlet François/Bocquet Cédric, De l'application de la LSCPT aux fournisseurs de services de VoIP, in: Jusletter vom 10. November 2014.

ten sich Mitte der 90er Jahre bei Privatpersonen schneller durch, weil die Anbieterinnen begannen, Verträge mit fixen Laufzeiten von 12 bis 24 Monaten anzubieten und im Gegenzug sehr grosse Rabatte auf die Geräte zu geben, welche indirekt über höhere Abonnementsgebühren finanziert wurden. Die Ablösung von SMS durch WhatsApp hat vorwiegend damit zu tun, dass ein SMS bei den meisten Anbieterinnen jahrelang 20 Rappen kostete, während der WhatsApp-Benützer nur die anfallenden Kosten für den Internetverkehr trägt. Weil in den meisten Abonnementen mittlerweile Internetverkehr in mehr oder weniger grossem Umfang schon in der Grundgebühr inbegriffen ist, sind WhatsApp-Meldungen faktisch kostenlos. Den Trend zum Umsteigen konnten die Anbieterinnen auch nicht dadurch auffangen, dass mittlerweile in den meisten Abonnementen eine bestimmte Anzahl SMS bereits inbegriffen ist.

4. Die Probleme der Strafverfolgungsbehörden

a) Die Identifikation der Kommunikationsbenutzer und -kanäle

Mit der Einführung der Mobiltelefonie entstand für die Strafverfolgungsbehörden zunächst das Problem, dass nicht mehr klar war, wer einen bestimmten Telefonanschluss benützte. Das Problem wurde verschärft durch den Umstand, dass die Anbieterinnen eine neue Form der Kundenbeziehung lancierten: Mittels Prepaid-Abonnementen konnten die Gesprächsgebühren im Voraus bezahlt werden, sodass die Kunden zunächst nicht einmal mehr namentlich registriert wurden. Das hatte zur Folge, dass in Strafverfahren vermehrt Anschlüsse auftauchten, die keiner Person zugeordnet werden konnten. Im Jahr 2004 wurden die Anbieterinnen dann zwar verpflichtet, auch die Personalien dieser Prepaid-Kunden zu erfassen[9]; das geschieht aber seither nur mit ungenügender Genauigkeit.

Mit der Einführung der Breitbandtechnologie auf Smartphones wurde es dann möglich, über diese Geräte auf ganz unterschiedlichen Kanälen zu kommunizieren: Es können Telefongespräche über das Mobilnetz, aber (z.B. via Skype) auch über Internet geführt werden. Die Teilnehmerinnen und Teilnehmer sind nicht nur über die Telefonnummer auf dem Mobiltelefon erreichbar, sondern auch über SMS via Mobilnetz und über Messenger (v.a. WhatsApp) via Internet. Dazu stehen auch alle Kommunikationskanäle des Internet zur Verfügung, also die Mailadresse, aber beispielsweise auch die Nachrichtendienste von Social Media, etwa von Facebook oder Twitter oder LinkedIn. Technisch gesprochen muss deshalb nicht nur ein Adressierelement (wie bisher

[9] Art. 15 Abs. 5bis BÜPF, eingefügt durch das Bundesgesetz vom 21. März 2003 betreffend Finanzierung des Terrorismus, AS 2003 3043, AS 2004 3693.

die Telefonnummer) überwacht werden, sondern alle andern Adressierelemente, die über das Mobiltelefon verwendbar sind.

b) Die Verschlüsselung und Übertragung der Kommunikation

Besonders problematisch für die Strafverfolgungsbehörden ist, dass die am weitesten verbreiteten modernen Dienste, nämlich Skype und WhatsApp, verschlüsselt kommunizieren: Jedes Skype-Gespräch und jede WhatsApp-Meldung werden bereits auf dem Gerät des Absenders verschlüsselt und bei längerer Kommunikation in mehrere Datenpakete zerlegt. Jedes dieser Datenpakete erreicht dann den Empfänger auf anderem Weg.

Dazu kommt eine weitere Schwierigkeit: Moderne Smartphones kommunizieren nicht nur über das Handynetz. Wenn sie sich im Bereich eines ihnen bekannten Wireless-Lan-Netzes befinden, dann loggen sie sich dort ein, und der Datenverkehr fliesst dann über dieses Netz. Wireless-Lan-Netze sind immer beliebter, und es gibt auch immer mehr Anbieterinnen, die solche Netze gratis der breiten Öffentlichkeit zur Verfügung stellen. In St. Gallen etwa (aber auch in anderen grösseren Städten) ist das Open Wireless in grossen Teilen der Innenstadt und in einigen Bussen frei verfügbar. Der Benutzer eines Smartphones muss sich nur bei der ersten Verwendung mit seiner Handynummer identifizieren und hat dann immer dort gratis Zugang, wo er sich im Empfangsbereich einer Antenne befindet.

Beide Technologien verunmöglichen die bei Mobiltelefonen noch heute übliche Überwachung: Bei dieser konventionellen Methode wird der Kommunikationsverkehr von den Strafverfolgungsbehörden bei der Anbieterin des Kunden abgefangen und in Kopie an die Strafverfolger weitergeleitet. Der Verkehr über Wireless-Lan-Netze führt allerdings gar nicht über die Anbieterin, bei welcher der Kunde sein Mobiltelefonabonnement hat. Die Strafverfolgungsbehörde weiss also von vornherein gar nicht, wo sie diesen Verkehr abgreifen soll. Wird der Verkehr verschlüsselt, dann wird er zwar allenfalls von der Mobiltelefonanbieterin weiter geleitet, sie kann ihn aber nicht entschlüsseln, weil sie den Schlüssel nicht besitzt. Die Anbieterinnen der Programme (v.a. Skype und WhatsApp) können ebenfalls nicht weiter helfen, weil sie zwar den Schlüssel hätten, aber natürlich nicht über den Datenverkehr des Kunden verfügen, denn sie stellen ja nur das Programm, aber nicht den Übermittlungsweg zur Verfügung. Dazu kommt, dass diese Anbieterinnen sich in der Regel im Ausland befinden[10] und strittig ist, ob sie als Fernmeldedienstanbieterinnen zu gelten haben und deshalb die

[10] Immerhin soll das Übereinkommen über Cyberkriminalität vom 23. November 2001, das in der Schweiz seit 1. Januar 2012 in Kraft ist (SR 0.311.43), den internationalen Datenaustausch erleichtern; siehe dazu Schweingruber Sandra, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, in: Jusletter vom 10. November 2014.

Pflichten überhaupt erfüllen müssten, die das BÜPF solchen Anbieterinnen überbindet.[11] In der Totalrevision des BÜPF soll der Anwendungsbereich allerdings ausgedehnt werden.[12]

Alle diese Schwierigkeiten führen zur gleichen Konsequenz: Die Kommunikation über Smartphones kann zu einem immer grösser werdenden Teil von den Strafverfolgungsbehörden nicht überwacht werden.

II. Der neue Art. 269ter StPO

1. Das Ziel des Gesetzgebers

Der Gesetzgeber hat diese Problematik erkannt und mit der hängigen Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs[13] wenigstens eine Lösung in Bezug auf die verschlüsselte Kommunikation vorgelegt: Durch Einsatz besonderer Informatikprogramme soll es möglich sein, den Verkehr über verschlüsselte Kanäle vor der Verschlüsselung direkt auf dem überwachten Gerät abzufangen und an die Strafverfolgungsbehörden weiterzuleiten[14]. Nur auf diese Weise wird es den Strafverfolgungsbehörden auch in Zukunft möglich sein, die gängigen Kommunikationskanäle zu überwachen. Praktikable Alternativen zum Einsatz besonderer Informatikprogramme gibt es nicht. Insbesondere können die zumeist ausländischen Anbieterinnen von Programmen zur verschlüsselten Kommunikation nicht gezwungen werden, den Schweizer Strafverfolgungsbehörden die jeweiligen Schlüssel zur Verfügung zu stellen.[15]

Die eingesetzten Programme werden unter Strafverfolgern Government Software oder GovWare genannt. In den Medien hält sich hartnäckig der Begriff Staatstrojaner, obwohl sich GovWare von Trojanern in sehr wesentlichen Punkten unterscheidet: Unter einem Trojaner versteht man üblicherweise ein Programm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt. In der harmloseren Variante werden solche Trojaner benützt,

---

[11] Zur Kontroverse vgl. Charlet/Bocquet (Fn. 8), Rz. 5 und Rz. 28 ff. mit Hinweis auf Morscher Lukas, Aktuelle Entwicklungen im Technologie- und Kommunikationsrecht, in: ZBJV 147 (2011), S. 177 ff.

[12] Details bei Charlet/Bocquet (Fn. 8), Rz. 34 ff.

[13] Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27. Februar 2013, BBl 2013 2683 ff.; Entwurf zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), BBl 2013 2789 ff.

[14] Näheres dazu bei Hansjakob Thomas, Der Einsatz von GovWare in der Schweiz, in: Jusletter IT vom 15. Mai 2014.

[15] So die Botschaft BÜPF 2013 (Fn. 13), BBl 2013 2777.

um den infizierten Computer für den Massenversand von Werbemails zu benutzen. Gefährliche Trojaner spionieren auch Daten, insbesondere Passwörter, aus oder löschen bzw. manipulieren Daten des Benutzers oder Systemdaten so, dass der Computer im schlimmsten Fall nicht mehr benutzt werden kann. GovWare will dagegen keinen Schaden verursachen, sondern im Rahmen des strafprozessual Zulässigen bloss ohne Wissen des Beschuldigten Kommunikationsverkehr ausleiten, der in einem Strafprozess als Beweismittel von Bedeutung ist. GovWare soll denn auch nichts zerstören und dient auch nicht unlauteren Zwecken, sondern sie erfüllt genau definierte Aufgaben bei der Erhebung von Beweisen, die auf andere Art nicht (oder nicht geheim) beschafft werden könnten[16].

Trojaner werden für den Massenversand programmiert und sind deshalb meistens so ausgelegt, dass sie auf möglichst vielen Computern oder Smartphones funktionieren und ihre Aufgabe erfüllen können; dass sie trotzdem auf vielen Geräten gar nicht funktionieren, nehmen die Programmierer gerne in Kauf. GovWare muss gezielt auf das System der Zielperson programmiert werden. Es ist also nötig, vor dem Einsatz der GovWare Informationen über dieses System zu sammeln: Wichtig ist insbesondere, welches Betriebssystem (Windows, iOS oder Android), welche Virensoftware und welche Kommunikationsprogramme die Zielperson benützt, denn nur mit diesen Informationen kann GovWare so programmiert werden, dass sie auf dem Zielsystem richtig läuft, von der Anti-Virensoftware nicht erkannt wird und aus den benützten Kommunikationsprogrammen diejenigen Informationen herausliest, die erforderlich sind.

2. Zur Notwendigkeit der Bestimmung

Ob der Einsatz von GovWare überhaupt gesetzlich geregelt werden muss, war bisher umstritten: Befürworter der Regelung weisen darauf hin, dass Art. 269 StPO nur den Eingriff ins Fernmeldegeheimnis rechtfertigt, nicht aber den Eingriff in eine Datenverarbeitungsanlage. Dagegen wird ins Feld geführt, dass Art. 269 StPO die gesetzliche Grundlage für die Überwachung des Fernmeldeverkehrs schaffe und dass die Frage, wie man diese Überwachung technisch durchführe, keine eigene Regelung benötige bzw. dass diese Regelung mit der Bestimmung über die technische Überwachung

[16] Hansjakob Thomas, Einsatz von GovWare – zulässig oder nicht?, in: Jusletter vom 5. Dezember 2011, Rz. 2 f.

nach Art. 280 StPO schon bestehe.[17] Die unterschiedliche Beantwortung dieser Frage hat auch dazu geführt, dass auch in der Schweiz bereits vor Inkrafttreten von Art. 269ter StPO in seltenen Fällen der Einsatz von GovWare angeordnet und durch die Zwangsmassnahmengerichte genehmigt wurde. Es besteht also schon eine – allerdings geringe – Erfahrung mit dieser Technologie. Der Gesetzgeber hat sich zu Recht für den sicheren Weg entschieden und eine klare gesetzliche Bestimmung vorgelegt.

3. Der Regelungsgegenstand

Der Entwurf[18] von Art. 269ter StPO regelt «das Einschleusen von besonderen Informatikprogrammen in ein Datenverarbeitungssystem». Das ruft Skeptiker auf den Plan, die von der falschen Annahme ausgehen, solche Programme würden gewissermassen die Fernsteuerung des betroffenen Computers oder Smartphones ermöglichen.

Die Angst, es könnten mit solchen Programmen «beliebige System- und Nutzerdaten ohne Wissen des Inhabers kopiert, verändert, gelöscht oder hinzugefügt werden»[19], ist allerdings theoretischer Natur: Natürlich öffnet GovWare eine «Hintertür» beim betroffenen Computer; durch diese Hintertür werden aber nicht alle vorhandenen oder bei Internetverkehr generierten Daten ausgeleitet, sondern die GovWare muss so programmiert werden, dass sie gezielt nur klar bezeichnete Daten (eben z.B. eine unverschlüsselte Kopie des verschlüsselten Kommunikationsverkehrs über eine bestimmte App) ausleitet.

Etwas anderes wäre denn auch technisch gar nicht möglich: Wollte man etwa mittels GovWare eine gesamte Festplatte spiegeln und damit alle auf einem Smartphone vorhandenen Daten ausleiten, dann würde das über das Mobile-Netz nicht nur mehrere Tage dauern, sondern es bliebe vom Benutzer kaum unbemerkt, weil dann dauernd Datenverkehr ausgeleitet würde. Das würde einerseits den Akku des Smart-

[17] Vgl. Näheres zur Kontroverse bei Hansjakob (Fn. 16); Jotterand Olivier/Müller Jérémie/Treccani Jean, L'utilisation du cheval de Troie comme mesure de surveillance secrète, in: Jusletter vom 21. Mai 2012; Métille Silvain, Les mesures de surveillance prévues par le CPP: quelles places pour le cheval de Troie, l'IMSI-Catcher ou les puces RFID?, in: Jusletter vom 19. Dezember 2011; Riss Ciril/Beranek Zanon Nicole, Art. 280 StPO genügt nicht als gesetzliche Grundlage für den Einsatz von Staatstrojanern, in: Jusletter vom 9. Juli 2012.

[18] Der vorliegende Aufsatz konnte noch die Erstberatungen des Ständerates und des Nationalrates berücksichtigen. Bei Abschluss des Beitrages war die Differenzbereinigung noch nicht abgeschlossen.

[19] Der vorliegende Aufsatz konnte noch die Erstberatungen des Ständerates und des Nationalrates berücksichtigen. Bei Abschluss des Beitrages war die Differenzbereinigung noch nicht abgeschlossen.

phones stark belasten, anderseits würde aber bei den heute meistens noch vorhanden Abonnementen mit beschränktem Datenvolumen die Anbieterin rasch eine Warnmeldung schicken, dass das Datenvolumen aufgebraucht sei. Solche Online-Durchsuchungen wären also nur bei stationären Computern, die per Datenkabel mit dem Internet verbunden sind, überhaupt realistisch. Sie bringen allerdings beweismässig wenig, weil sie kein statisches Abbild einer Festplatte liefern und deshalb schwierig zu interpretieren sind.

Um den Bedenken der Kritiker Rechnung zu tragen, schlägt der Nationalrat einen neuen Art. 269^{quater} vor, der die Sicherheit von GovWare-Programmen und deren zentrale Beschaffung durch den Dienst garantieren soll.

4. Das Ziel der GovWare

Der Gesetzgeber verunmöglicht die schrankenlose Erhebung von Daten schon dadurch, dass er genau definiert, welche Daten mittels GovWare erhoben werden dürfen: Es geht nur um «den Inhalt der Kommunikation und die Randdaten des Fernmeldeverkehrs». Ausgeschlossen sind damit gestützt auf Art. 269ter StPO insbesondere

- der Abruf von Daten, die auf dem Computer oder Smartphone *gespeichert* sind (sog. Online-Durchsuchung); es geht nur um Daten, die im Rahmen des Kommunikationsverkehrs von bestimmten Programmen generiert werden;
- die *Fernsteuerung* des Computers, etwa durch unbemerktes Einschalten der Web-Cam oder des eingebauten Mikrophons und Ausleiten der damit gelieferten Bilder und Töne;
- die Überwachung des Datenverkehrs ausserhalb von eigentlichem *Kommunikationsverkehr*, also die Aufzeichnung normaler Internet-Sessionen, solange diese nicht eine Punkt-zu-Punkt-Kommunikation der überwachten Person mit anderen Personen betreffen.

Zulässig ist es allerdings, neben den reinen Kommunikationsdaten auch die Randdaten des Fernmeldeverkehrs auszuleiten, also die Angaben darüber, wer wann und wo mit wem kommuniziert hat. Es geht um die gleichen Daten, die auch im Rahmen des normalen Fernmeldeverkehrs erhältlich sind.

5. Die Voraussetzungen der Überwachung

Der Einsatz von GovWare ist nach Art. 269ter Abs. 1 StPO von vier Voraussetzungen abhängig:

Erstens müssen die Bedingungen von Art. 269 Abs. 1 und 3 StPO erfüllt sein. Gegen die beschuldigte Person muss also ein dringender Tatverdacht in Bezug auf eine Straftat bestehen, zu deren Aufklärung der Einsatz von GovWare verhältnismässig sein muss. Andere Untersuchungshandlungen müssen erfolglos gewesen sein, oder es muss zumindest klar sein, dass ohne Einsatz von GovWare die Aufklärung unverhältnismässig erschwert würde.

Zweitens muss es um die Aufklärung einer Straftat nach Art. 286 Abs. 2 StPO gehen; es ist also nicht der Deliktskatalog für Überwachungen, sondern derjenige für verdeckte Ermittlungen anwendbar. Dabei geht es nicht darum, dass der Einsatz von GovWare einer verdeckten Ermittlung ähnlich wäre; man wollte vielmehr gegenüber «normalen» Überwachungen eine zusätzliche Hürde schaffen, die darin gesehen wurde, dass der Deliktskatalog von Art. 286 Abs. 2 StPO etwas enger ist als derjenige von Art. 269 Abs. 2 StPO. Die Anwendung dieses Katalogs ist allerdings eigentlich sachfremd: Die Auswahl der Delikte nach Art. 286 StPO erfolgte (vorwiegend oder zumindest auch) mit Blick darauf, zur Aufklärung welcher Straftaten eine verdeckte Ermittlung überhaupt sinnvoll ist; im vorliegenden Zusammenhang geht es aber um die ganz anders zu beantwortende Frage, wann eine Kommunikationsüberwachung Sinn macht. Praktisch wird die Anwendung dieses engeren Katalogs von Art. 286 StPO allerdings wohl nicht zu nennenswerten Schwierigkeiten führen.

Drittens müssen die bisherigen Massnahmen zur Überwachung des Fernmeldeverkehrs nach Art. 269 StPO erfolglos geblieben sind sein, oder die Überwachung mit diesen Massnahmen wäre von vornherein aussichtlos oder würde die Aufklärung unverhältnismässig erschweren. Man kann von doppelter Subsidiarität sprechen: Eine Fernmeldeüberwachung darf erst eingesetzt werden, wenn die Aufklärung der Delikte mit konventionellen Massnahmen unverhältnismässig schwierig wäre; die GovWare darf erst eingesetzt werden, wenn dies auch für die konventionelle Fernmeldeüberwachung gilt.

Viertens schliesslich ist zum Einsatz von GovWare wie bei einer konventionellen Fernmeldeüberwachung die Genehmigung des Zwangsmassnahmengerichtes erforderlich.

Damit der auswertenden Behörde (der Polizei) und der Genehmigungsbehörde klar ist, welche Daten ausgeleitet werden dürfen, verpflichtet Art. 269ter Abs. 2 Bst. a StPO die Staatsanwaltschaft, die gewünschten Datentypen genau zu bezeichnen. Das bedeutet praktisch, dass die Staatsanwaltschaft bezeichnen muss, welche Programme oder Apps, die zur Kommunikation verwendet werden, zu überwachen sind und welche dabei übermittelten Daten ediert werden dürfen. Die Staatsanwaltschaft muss also z.B. anordnen, dass der WhatsApp-Verkehr überwacht werden dürfe, wobei sie bezeichnen muss, ob nur Textmeldungen oder auch Bilder oder Sprachmeldungen

ediert werden sollen. Auf diese Weise ist sichergestellt, dass die Genehmigungsbehörde die Verhältnismässigkeit der Massnahme genau überprüfen kann.

6. Durchführung der Überwachung

Wird der Einsatz von GovWare bewilligt, dann stellt sich die Frage, wie das Programm auf die überwachten Geräte kommt. Zuständig für die Installation der GovWare ist die Polizei und nicht etwa der Dienst zur Überwachung des Post- und Fernmeldeverkehrs, der im Übrigen anders als bei konventionellen Überwachungen auch den ausgeleiteten Gesprächsverkehr nicht entgegennehmen und aufzeichnen soll. Beide Aufgaben kommen der zuständigen Polizeibehörde zu.[20]

Art. 269ter Abs. 2 Bst. b StPO lässt es zu, dass die Staatsanwaltschaft anordnet, die Polizei dürfe in nicht öffentliche Räume eindringen, um die GovWare z.B. auf einen fest installierten Computer aufzuspielen. In dieser Hinsicht gibt Art. 269ter StPO die gleichen Möglichkeiten, die auch zum Verbauen von technischen Überwachungsgeräten nach Art. 280 StPO zulässig, dort allerdings nicht explizit geregelt sind.

Der einfachste Weg, wie GovWare auf die überwachten Geräte kommt, ist der physische Zugriff der Polizei auf solche Geräte. Das ist bei den üblicherweise verwendeten Smartphones ein kleines Problem, weil solche Geräte normalerweise bei einer Personenkontrolle in Betrieb sind und sichergestellt werden können, wobei es dann nur wenige Sekunden dauert, um die GovWare unbemerkt aufspielen zu können. Befindet sich ein zu überwachender Computer zu Hause bei der Zielperson, dann ist diese Art des Aufspielens nur möglich, wenn der Computer in Betrieb ist; muss er zunächst hochgefahren werden, dann ist der Passwortschutz möglicherweise bereits eine nur schwer zu überwindende Hürde. Deshalb wird bisweilen auch der Weg benützt, den Kriminelle beim Einsatz von Trojanern wählen: Die GovWare wird z.B. im Anhang einer E-Mail versteckt. Die Schwierigkeit besteht dann allerdings darin, dass es zahlreiche Möglichkeiten gibt, von verschiedensten Geräten aus auf E-Mails zuzugreifen, sodass die Polizei riskiert, dass sich ihre GovWare plötzlich etwa auf einem Computer in einem Internet-Café befindet. Deshalb wird der physische Zugriff auf das Gerät meistens favorisiert, um sicherzustellen, dass die GovWare nur dort landet, wo sie hingehört.

[20] Das ist nicht ganz überzeugend, denn es wäre besser, wenn das Knowhow zum Handling solcher Programme beim Bund zentralisiert würde und nicht jeder Kanton dafür selbst zuständig wäre; der Dienst ÜPF hat sich allerdings dagegen gewehrt, mit dieser Aufgabe betraut zu werden. Vgl. dazu Hansjakob Thomas, in: Andreas Donatsch/Thomas Hansjakob/Viktor Lieber (Hrsg.), Zürcher Kommentar zur StPO, 2. Aufl., Zürich 2014, Art. 269ter StPO Rz. 15 f.

Der Gesetzgeber hat daran gedacht, dass GovWare möglicherweise unbeabsichtigt auf Geräten landet, die gar nicht überwacht werden sollen, oder dass es bisweilen auch vorkommen kann, dass die GovWare ungenau programmiert wurde und deshalb auch Daten liefert, die von der Überwachungsanordnung und -genehmigung nicht gedeckt sind. Für solche Fälle sieht Art. 269ter Abs. 3 StPO ausdrücklich vor, dass die durch die Anordnung nicht gedeckten Daten, die beim Einsatz solcher Informatikprogramme gesammelt werden, sofort zu vernichten sind. Das stellt sicher, dass sie nicht trotzdem verwertet werden, verunmöglicht aber der Verteidigung, im Nachhinein noch zu überprüfen, welche Daten erhoben wurden, deren Verwertung nicht zulässig war.

Dieses Verwertungsverbot hat ausdrücklich Fernwirkung: Durch solche Daten erlangte Erkenntnisse dürfen nicht verwertet werden.

Die bisweilen geäusserte Befürchtung, der Einsatz von GovWare öffne im System Sicherheitslücken, die dann auch von Dritten ausgenützt werden könnten, hat keinen realen Hintergrund: Trojaner nützen in der Regel bekannte Sicherheitslücken aus, die auf einer grossen Zahl von Computern vorhanden sind; anders würde sich die Programmierung und Verteilung von Trojanern gar nicht lohnen. Selbst wenn GovWare eine neue Sicherheitslücke schaffen würde, würde es keinen Sinn machen, auch einen Trojaner für die gleiche Lücke zu programmieren, weil ja GovWare nur in sehr kleiner Zahl verwendet wird und die Suche nach Computern, auf welchen sich GovWare befindet, für einen Hacker der Suche der Nadel im Heuhaufen gleich käme.

7. Beendigung der Überwachung und Rechtsmittel

Die Beendigung der Überwachung mittels GovWare unterliegt den gleichen Regeln wie die normale Fernmeldeüberwachung (Art. 275 StPO). Auf eine Besonderheit ist allerdings hinzuweisen: Damit die GovWare nicht nachträglich enttarnt werden kann, muss sie auf dem Gerät der Zielperson unbemerkt gelöscht werden können. Zu diesem Zweck haben die eingesetzten Programme ein definierbares Verfallsdatum, an dem sich das Programm selbst löscht, es muss aber auch eine Funktion eingebaut sein, welche die ferngesteuerte vorzeitige Löschung des Programms ermöglicht.

Wie bei jeder Überwachung muss auch bei GovWare-Überwachung der Betroffene nachträglich benachrichtigt werden, und er hat dann Akteneinsicht sowie die Möglichkeit, die Zulässigkeit der Massnahme nachträglich überprüfen zu lassen (Art. 279 StPO). Dabei genügt es, dem Beschuldigten Einsicht in die Anordnungs- und Genehmigungsakten sowie in die Ergebnisse der Überwachung zu geben. Nicht erforderlich sind genaue Informationen zur Frage, wie die GovWare auf das Zielgerät aufgespielt und wie sie genau programmiert wurde.

III. Gesamtwürdigung

Was der Bundesrat vorschlägt und das Parlament mit einigen Präzisierungen mittlerweile vorerst abgesegnet hat, eröffnet im Grund genommen keine neuen Überwachungsmöglichkeiten, sondern trägt nur der Veränderung der technischen Art der Kommunikation Rechnung: Auch mittels GovWare kann nicht mehr als der Kommunikationsverkehr von Beschuldigten überwacht werden, immerhin aber nun auch dann, wenn die modernsten Technologien verwendet werden. Auf diese Weise wird verhindert, dass die Strafverfolgungsbehörden künftig auch dann, wenn die gesetzlichen Voraussetzungen eigentlich vorhanden wären, keine Überwachungsergebnisse erhalten, weil durch die Straftäter eine gängige Technologie verwendet wird, die aus technischen Gründen nicht überwachbar ist.

Den vorhandenen Gefahren wird durch eine gesetzliche Regelung, die beinahe übervorsichtig ist, Rechnung getragen. Damit können die Strafverfolger allerdings gut leben: Denn es sind nicht die rechtlichen, sondern die faktischen Hürden, welche eine Überwachung mittels GovWare so schwierig machen. Der organisatorische und finanzielle Aufwand für eine solche Überwachung ist weit grösser als der Aufwand, der bisher bei einer normalen Handy-Überwachung zu leisten war. Schon aus diesem Grund ist davon auszugehen, dass GovWare auch in Zukunft nur sehr zurückhaltend eingesetzt wird.

Umso weniger überzeugt die Kritik an der neuen Bestimmung. Wer befürchtet, man werde mit GovWare mehr tun, als man eigentlich tun dürfte, nur weil die technischen Möglichkeiten dazu an sich vorhanden wären, übersieht, dass den Strafverfolgungsbehörden auch andere technische Mittel zur Verfügung stehen, die nur unter engen Rahmenbedingungen eingesetzt werden dürfen, ohne dass bisher behauptet wurde, diese engen Bedingungen würden systematisch missachtet. Das hängt auch damit zusammen, dass die Verletzung von Rahmenbedingungen mit Verwertungsverboten sanktioniert wird – es würde also beweismässig gar nichts bringen, Informationen zu sammeln, die gar nicht ins Verfahren eingeführt werden dürfen.

Trotzdem war die bisherige Diskussion in den Kommissionen und Räten auf die Revision des BÜPF fokussiert. Dagegen war kaum Opposition gegen das Nachrichtendienstgesetz zu hören, das allerdings weit ausgedehntere Mittel zur Überwachung der Bürger vorsieht, und zwar auch dann, wenn diese gar keiner Straftaten verdächtigt werden. Im Gegensatz zur nachrichtendienstlichen Tätigkeit muss die Überwachungstätigkeit im Strafverfahren dem davon belasteten Bürger allerdings immer nachträglich offengelegt werden, und er kann die Zulässigkeit und Angemessenheit dieser Massnahmen auch nachträglich noch richterlich überprüfen lassen.

In diesem Sinne hat das Parlament seine Hausaufgaben nur ungenügend erledigt: Nicht die Möglichkeiten der rein repressiv tätigen Strafverfolgungsbehörden, sondern diejenigen der präventiv tätigen Nachrichtendienste sollten besonders engen Rahmenbedingungen unterliegen, weil sie erstens nicht von einem Tatverdacht abhängig und zweitens vom Betroffenen weit weniger kontrollierbar sind. Wer den Strafverfolgungsbehörden allerdings nicht die Mittel in die Hand gibt, auch moderne Kommunikationsformen von Straftätern zu überwachen, begünstigt damit letztlich Straftaten.