Seminararbeit

Die Überwachung gesellschaftlicher Kommunikation in der Schweiz durch staatliche Behörden

Die aktuellen Gesetzesrevisionen in der Schweiz und ihre Folgen für die Gesellschaft

ONLINEPUBLIKATION – Kontakt nur über www.michael-baenziger.ch

eingereicht von:

Michael Bänziger
Matrikel-Nr. 11-717-980

Student im 4. Semester
Hauptfach: Publizistik- und Kommunikationswissenschaft
Nebenfach: Recht

Thema und Zeitpunkt des Seminars:

„Big Data, Big Brother, Big Business: Datensammlung, Datenverwertung und Datenschutz im Internet“ im Schwerpunkt 1
Frühjahrssemester 2013

betreut von:

Mag. Dr. des. Florian Saurwein, M. A. Konstantin Dörr
IPMZ – Institut für Publizistikwissenschaft und Medienforschung
der Universität Zürich
Andreasstrasse 15
8050 Zürich

Abgabetermin: 26. Juni 2013

Inhaltsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BÜPF	Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (SR 780.1)
BWIS	Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (SR 120)
Dienst ÜPF	Dienst Überwachung Post- und Fernmeldeverkehr, ehemals „Dienst für besondere Aufgaben“ (DBA)
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz (SR 235.1)
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (zum Zeitpunkt der Arbeit: Hanspeter Thür)
FMG	Fernmeldegesetz vom 30. April 1997 (SR 784.10)
GebV-ÜPF	Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (SR 780.115.1)
NDB	Nachrichtendienst des Bundes
NDG	Nachrichtendienstgesetz (in der Entwurfsphase)
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0)
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007 (SR 312.0)
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VÜPF	Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (SR 780.11)

1 Einleitung

Der Bundesrat revidiert das aktuell geltende Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). Die zugehörige Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) wurde bereits revidiert und auf den 1. Januar 2012 in Kraft gesetzt. Ebenso wird die Schweizerische Strafprozessordnung (StPO) vom 5. Oktober 2007 geändert.

Mit der Revision will der Bundesrat die Gesetze den neusten technischen Entwicklungen und Fortschritten anpassen und rechtliche Möglichkeiten und Schranken der Überwachung definieren. Dies ist erforderlich, weil das BÜPF über zwölf Jahre alt ist und moderne Kommunikationstechnologien nicht direkt umfasst. Neu könnte auch der Einsatz von Spionageprogrammen, die umgangssprachlich als „Staatstrojaner" bezeichnet werden, unter bestimmten Voraussetzungen zur Aufklärung besonders schwerer Straftaten erlaubt werden. Trojaner, die auch als nützliche Programme getarnt werden können, sind in der Lage, Daten eines Computers unbemerkt zu übermitteln (beispielsweise zu Beweiszwecken an Behörden, vgl. Hansjakob 2011: 2) oder auch die Tastatureingaben des Benutzers aufzuzeichnen (vgl. Rhyner/Stüssi 2008: 469). Weitere Funktionen wie das Aktivieren von Mikrofon oder Kamera (vgl. Gless 2012: 18; Hansjakob 2006: 106) oder auch das „Keylogging", also das Aufzeichnen der Tastatureingaben (vgl. Hansjakob 2006: 106) sind denkbar, sollen aber verboten sein (Botschaft zum BÜPF 2013: 20). Allerdings sei darauf hingewiesen, dass sich Trojaner in vielen Fällen selbst verbreiten können, was GovWare nicht bezweckt (vgl. Botschaft zum BÜPF 2013: 90).

Der neue Gesetzesentwurf stiess auf heftige Kritik von mehreren Seiten – hauptsächlich von Anbieterinnen von Fernmeldediensten (Anmerkung: Nachfolgend wird, wie im BÜPF auch, die weibliche Form verwendet), aber auch von interessierten Verbänden, Unternehmen und Bürgern. Einerseits wird kritisiert, dass der Entwurf zu ungenau sei und die geplanten Ziele zur besseren Überwachung nicht erreiche. Andererseits wird insbesondere zum Thema des Staatstrojaners die Meinung vertreten, die Schweiz werde zunehmend zu einem Überwachungsstaat, in dem keine Sicherheit über die freie Kommunikation herrsche, und dass die Gesetzesänderung ein zu tiefer Eingriff in die Grundrechte der Menschen sei.

2 Fragestellung und Zielsetzung

In der Diskussion über die rechtliche Zulässigkeit der Strafverfolgung im Internet geht es nicht mehr um das „ob“, sondern nur noch um das „wie“ (vgl. Gless 2012: 3). Unter welchen Umständen darf der Bund die Post und den Fernmeldeverkehr (hauptsächlich Mobiltelefonie und Internet) momentan überwachen? Welche Massnahmen kommen bei dieser Überwachung zum Einsatz? Was hat es mit der „verdeckten Ermittlung“ auf sich und inwiefern ist sie rechtlich zulässig? Was wird sich durch die Gesetzesrevisionen ändern? Diese Fragen sind momentan Teil einer wichtigen Diskussion.

Im Jahr 2008 war zum Thema Staatstrojaner noch vergleichsweise wenig bekannt (Platz 2008: 839). Nachdem der Bundesrat die Totalrevision des BÜPF am 19. Mai 2010 in die Vernehmlassung geschickt hatte (vgl. EJPD 2011a: o. S.), entstanden hitzige Diskussionen und Kritik wurde von vielen Seiten laut. Ebenso wurde publik, dass GovWare bereits verwendet worden war, allerdings ohne genaue gesetzliche Grundlage (siehe dazu Kapitel 5.1.3).

Da das revidierte BÜPF „frühestens 2013, eher erst 2014 in Kraft treten wird“ (Hansjakob 2011: 4), muss die Gesellschaft jetzt über die möglichen Folgen informiert werden und ihre Kritik dazu ausdrücken können. Im Rahmen dieser Arbeit wird analysiert, wie sich die Gesetzesrevisionen auf die Gesellschaft auswirken können – der Schwerpunkt liegt hierbei auf der Überwachung mittels GovWare.

Diese Arbeit basiert demnach auf den folgenden Fragestellungen:

- Welche Überwachungsmassnahmen über das Internet können staatliche Behörden in der Schweiz anwenden, um gesellschaftliche Kommunikation zu überwachen?
- Welche möglichen Folgen der Gesetzesänderungen zeichnen sich für die Gesellschaft ab?

Ziel dieser Arbeit ist es, das Thema aus beiden Perspektiven (Staat und Gesellschaft) kritisch zu betrachten und Klarheit zu schaffen.

3 Theoretischer Hintergrund

Wie viel staatliche Kontrolle kann eine moderne, liberale Gesellschaft vertragen? Im Spannungsfeld von Sicherheit und Recht geht es, aus rechtswissenschaftlicher Perspektive gesehen, um das Verhältnis zwischen Individuum und Staat (vgl. Hornung 2007: 149). Dieses wird problematisch, wenn das Recht erst nach der Einführung einer neuen Technologie auf diese reagiert und nicht bereits im Vorfeld steuernd einwirkt – es bildet sich ein „strukturelles Ungleichgewicht zwischen den Polen Sicherheit und Privatheit" (Hornung 2007: 149).

Hier knüpfen Theorien zur Privatheit an. Rössler (2001: 25) unterscheidet drei Dimensionen der Privatheit: Die dezisionale, die informationelle und die lokale. Für diese Arbeit relevant ist die informationelle Privatheit. Rössler (2001: 201/Hervorheb. i. O.) schreibt dazu: „Wenn Privatheit im Allgemeinen bedeutet, den ‚Zugang' zur eigenen Person kontrollieren zu können, dann […] muss dies in einer Hinsicht verstanden und interpretiert werden als Kontrolle darüber, was andere über die Person wissen können". Entstanden ist der Diskurs über die informationelle Privatheit bereits Ende des 19. Jahrhunderts: Mit der Verbreitung der Klatschpresse und der zunehmenden Popularität der Fotografie (vgl. Rössler 2001: 13) rückten berühmte Personen ins Rampenlicht der Berichterstattung. Um 1950 machte die Computertechnologie Fortschritte und der Staat zeigte ein verstärktes Interesse an der Informationssammlung und -verarbeitung (vgl. Warren/Brandeis 1984: o. S., zit. nach Rössler 2001: 13). Insbesondere mit dem Internet ist später eine „noch nie dagewesene Herausforderung für die Privatheit" (Eggimann 2013: 112) entstanden.

Die Privatsphäre ist ein Teil der juristischen Sphärentheorie, deren Ziel es ist, „objektiv verschiedene Bereiche privater Lebensgestaltung räumlich voneinander abzugrenzen, wobei der Schutz des Betroffenen nach den einzelnen Sphären abgestuft wird" (Weniger 2005: 186). Diese drei Sphären sind nach Maurer-Lambrou/Kunz (2006: 35) die Gemeinsphäre, die Privatsphäre und die Geheim- oder Intimsphäre. Ein tiefer Eingriff erfordert demnach auch höhere Anforderungen an die Rechtfertigung. Diese Theorie ist aber nicht so auf das DSG anwendbar (vgl. Maurer-Lambrou/Kunz 2006: 36), weil die Klassifizierung der Informationen einzelfallabhängig ist und jeweils zwischen öffentlichen und privaten Interessen abgewogen werden muss – der Begriff der Privatsphäre ist also variabel. Im Strafrecht ist die Sphärentheorie allerdings ausdrücklich verankert, wobei der Straftatbestand objektiv abgegrenzt werden muss, weil das Strafrecht täterorientiert ist (vgl. Aebi-Müller 2005: 249).

Werden die Bürger insbesondere von staatlicher Seite überwacht, können sie nicht mehr wissen (und somit nicht mehr kontrollieren), was andere über sie wissen können. Dann ist die Rechtsordnung nicht mehr mit dem Recht auf informationelle Selbstbestimmung vereinbar – abweichende Verhaltensweisen würden vermieden und sowohl individuelle Entfaltungschancen als auch das Gemeinwohl würden beeinträchtigt (vgl. Denninger 1985: 219). Somit verbin-

den sich Fragen zur persönlichen Identität immer enger mit Fragen zum persönlichen Sicherheitsgefühl: „Die Grenzen der Privatsphäre [geraten/M.B.] aufgrund eines individuell motivierten, jedoch politisch geschürten Sicherheitsbedürfnisses in Gefahr“ (Henatsch 2007: 177). Die oben aufgeworfene Frage, wie viel staatliche Kontrolle eine liberale Gesellschaft vertragen kann, lässt sich weder aus rechtlicher noch aus technischer Sicht abschliessend beantworten – dies ist die Aufgabe der Gesellschaft und der Politik, weil die Grundsätze einer Demokratie (vgl. Hornung 2007: 161) nicht durch technologischen Determinismus umgangen werden dürfen.

Eine Demokratie ist ohne die Garantie der Privatsphäre nicht denkbar, weil die notwendige politische Willensbildung gesellschaftliche Freiräume erfordert (vgl. Müller 2008: 196). Die direkte Demokratie geht dabei von einem positiven Menschenbild aus (Schweizer Fernsehen 2010: o. S.). Dieses tritt jedoch nicht tatsächlich so in Erscheinung – in jeder Gesellschaft und in jedem Staat existiert Kriminalität. Nicht alle Bürger kommen direkt mit ihr in Kontakt; die Medien verstärken jedoch unser Unsicherheitsgefühl (genaueres dazu in Kapitel 6.1.6). Wenn verstärkt gegen die Kriminalität vorgegangen werden soll, dürfen die Prinzipien der Demokratie deshalb nicht vernachlässigt werden.

4 Ansatz und Methode

Die Fragestellung wird mittels einer qualitativen Inhaltsanalyse beantwortet. Es geht nicht darum, den Diskurs statistisch zu „vermessen“, sondern genannte Argumente zu prüfen, einfliessen zu lassen und kritisch zu würdigen. Die Ergebnisse, d. h. die möglichen Folgen der Gesetzesrevisionen auf die Gesellschaft, ergeben sich primär aus der Analyse von Leserkommentaren, die zu Online-Zeitungsartikeln verfasst worden sind. Diese Methode bietet sich an, weil die Kommentatoren mit höchster Wahrscheinlichkeit den Zeitungsartikel zuvor gelesen haben und sich ihre Meinung zuerst bilden können – bei einer Befragung wären vermutlich viele Personen nicht ausreichend über das Thema informiert. Die Leserkommentare werden anschliessend hauptsächlich mit Informationen aus juristischen Quellen kritisch gewürdigt.

Dies ist erforderlich, weil sie falsche Behauptungen oder aus dem Zusammenhang gerissene Themen beinhalten können. Kommentare auf www.20min.ch werden beispielsweise aussortiert, wenn sie nur ein Wort oder mehr als 30 Ausrufezeichen beinhalten oder in Dialekt bzw. Fremdsprache geschrieben wurden (vgl. Büsser 2013: 27). Sie zeigen aber, ob und wie die Thematik im gesellschaftlichen Diskurs aufgenommen wurde, und sollen jeweils auf die Frage „Welche positiven oder negativen Folgen werden in Form von Hoffnungen oder Befürchtungen geäussert?“ untersucht werden. Die juristischen Fachartikel sind von hoher Qualität und beziehen sich meistens auf die Auslegung von Gesetzesartikeln oder auf zukünftige Probleme bei Gesetzesrevisionen. Um die rechtliche Situation vor und nach den Gesetzesrevisionen zu erklären, werden zudem Gesetze bzw. Gesetzesentwürfe, deren Botschaften und Erläuterungen sowie Onlinepublikationen gelesen.

Auf den Webseiten der Zeitungen 20 Minuten, Blick, Tages-Anzeiger und NZZ wurde direkt nach „BÜPF“, „Staatstrojaner“ und „Trojaner“ gesucht, weil LexisNexis nur gedruckte bzw. Agenturmeldungen ohne Kommentarfunktion lieferte. Letztere Suchanfrage brachte viele Artikel hervor, die keinen Zusammenhang zu den Gesetzesrevisionen bzw. der Schweiz aufwiesen. Allerdings fanden sich auch thematisch relevante Artikel, die mit der Suche nach „BÜPF“ nicht gefunden worden waren. Doppelte Artikel (teilweise wurden dieselben Artikel mit exakt denselben Kommentaren unter anderem Titel ein zweites Mal verlinkt) und Artikel ohne Leserkommentare wurden nicht berücksichtigt. Insgesamt wurden 1722 Leserkommentare analysiert; davon entfielen 1536 auf die 20 Minuten, 183 auf den Tages-Anzeiger und 3 auf die NZZ. Diese sehr unterschiedlichen Häufigkeiten lassen sich dadurch erklären, dass die 20 Minuten für die Kommentarabgabe keine Registrierung verlangt und anonym kommentiert werden kann. Rund 4000 Kommentare gehen täglich ein; davon werden etwa 60% veröffentlicht (vgl. Büsser 2013: 27). Die Links zu den Artikeln, deren Kommentare analysiert wurden, sind im Literaturverzeichnis unter „Analysierte Leserkommentare“ aufgeführt.

5 Überwachung aus rechtlicher Sicht

Dieses Kapitel beschreibt die technischen Überwachungsmassnahmen aus rechtlicher Sicht. Da diese Arbeit auf den Internetverkehr fokussiert, wird auf die Überwachung des Postverkehrs nicht eingegangen. Die Überwachung der herkömmlichen Telefonie wird vereinfacht beschrieben, weil bereits dort die Unterscheidung der zwei Überwachungstypen ansetzt.

5.1 Aktuelle Situation

Nachfolgend werden die aktuell möglichen Überwachungsmassnahmen beschrieben. Erwähnungen der VÜPF beziehen sich auf die aktuell gültige (bereits revidierte) Version. Das Ausführungsorgan der nachfolgenden Überwachungsmassnahmen ist jeweils der „Dienst ÜPF“.

5.1.1 Überwachung der Telefonie

Telefonie kann auf zwei verschiedene Arten überwacht werden. Es wird unterschieden zwischen der „Echtzeit-Überwachung“ und der „rückwirkenden Überwachung“. Jede Anbieterin muss laut Art. 15 Abs. 3 BÜPF die für die Teilnehmeridentifikation notwendigen sowie die Verkehrs- und Rechnungsdaten während sechs Monaten aufbewahren. Bei der Echtzeit-Überwachung werden Telefone abgehört und die Gespräche aufgezeichnet. Diese werden zusätzlich zu den Daten simultan, leicht verzögert oder periodisch übermittelt. Bei der rückwirkenden Überwachung handelt es sich aber nur um Verkehrs- und Rechnungsdaten (keine Gesprächsinhalte). Diese können bis zu sechs Monate später beantragt werden.

Bei den gesammelten Daten handelt es sich beispielsweise um das Datum, die Uhrzeit oder auch die Dauer des Gesprächs, die Rufnummern, IMEI-Nummern, bei Mobiltelefonie zusätzlich

der Zell-Identifikator (Cell ID) oder auch der „Standort und die Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person zum Zeitpunkt der Kommunikation verbunden ist“. Die Überwachungstypen (Echtzeit und rückwirkend) sind in Art. 16 VÜPF detailliert festgehalten.

5.1.2 Straftat über das Internet

Dem Internet ist momentan nur ein Absatz gewidmet – Art. 14 Abs. 4 BÜPF lautet: „Wird eine Straftat über das Internet begangen, so ist die Internet-Anbieterin verpflichtet, der zuständigen Behörde alle Angaben zu machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen.“ Hier besteht kein beschränkter Straftatenkatalog (vgl. Hansjakob 2006: 357). Der Absatz ist jedoch sehr unspezifisch formuliert, was bereits mehrere Diskussionen entfacht hat. Der ganze Art. 14 BÜPF zielt auf die Daten über Fernmeldeanschlüsse ab und soll den Behörden lediglich ermöglichen, beispielsweise einen Inhaber einer Webseite, Telefonnummer oder IP-Adresse zu ermitteln. Um diese Daten zu erhalten, wird kein Strafverfahren vorausgesetzt (vgl. Hansjakob 2006: 352). Der Artikel ist aber nicht geschaffen worden, um Verbindungsdaten abfragen zu können – er wurde aber zu diesem Zweck benutzt (vgl. Heiniger 2013: 5). Bei dynamischen IP-Adressen (dies ist der Normalfall) handelt es sich nämlich genau genommen um Verbindungsdaten. Es wurde erst später erkannt, dass auch diese unter Art. 14 Abs. 4 BÜPF fallen sollten (vgl. Hansjakob 2006: 358-359). Die Internetanbieterinnen sind im Übrigen gegenüber der zuständigen Behörde (und nicht wie im restlichen Art. 14 dem Dienst ÜPF) verpflichtet – dies ist vermutlich ein Fehler; in Art. 27 VÜPF und neu auch in Art. 22 des BÜPF-Entwurfs handelt es sich hierbei um den Dienst ÜPF (vgl. Hansjakob 2006: 358).

5.1.3 Überwachung durch GovWare

Nach der herrschenden Meinung darf GovWare momentan nicht zum Einsatz kommen. Der Einsatz von „technischen Überwachungsgeräten“ wird zwar in Art. 280 StPO geregelt, GovWare fällt aber nicht darunter, weil sie in das Datenverarbeitungssystem des Beschuldigten eingreift und die Software so manipuliert, dass sein technisches Gerät dazu dienen kann, seine Gespräche zu überwachen (vgl. Hansjakob 2011: 4). In vermutlich vier Fällen (vgl. Hansjakob 2011: 3) haben verschiedene Strafverfolgungsbehörden bereits GovWare anscheinend rechtswidrig unter „technische Überwachungsgeräte“ subsumiert und angewendet. Dabei ging es um die Klärung eines Terrorismusverdachtes – die verwendete Software stammte von der Firma DigiTask, die auch GovWare für Deutschland programmiert hatte (vgl. Schweizer Fernsehen 2011: o. S.). Dies geschah vor dem Inkrafttreten der neuen Strafprozessordnung am 1. Januar 2011; zuvor galten kantonale Strafprozessordnungen, die aber auch keine detaillierteren Regelungen zu diesem Thema enthielten (vgl. Steiger 2011: o. S.). Die so durchgeführten Überwachungen seien deshalb „einfach nur dreist“ (Stöckli 2011: 16).

Deshalb ist, nach der Ansicht von Hansjakob (2011: 4), die Überwachung durch Staatstrojaner „mangels klarer gesetzlicher Grundlage“ nicht zulässig. Es existiert aber auch eine Gegenstimme: Nach Jotterand/Müller/Treccani (2012: 3) ist der Einsatz von GovWare gerechtfertigt – sie legen den Begriff der „technischen Überwachungsgeräte“ grosszügig aus.

Die Überwachung durch GovWare soll hauptsächlich ermöglicht werden, weil softwarebasierte Internettelefonie bis heute nicht überwacht werden kann. Internettelefonie kann über normale Telefone (allerdings über die Internetleitung) sowie über Software (z. B. Skype) laufen. Im Rahmen dieser Arbeit und der Gesetzesrevisionen ist stets die Internettelefonie über Software gemeint. Da bei dieser die Gespräche beidseitig verschlüsselt werden und auch die Softwareanbieter keine Möglichkeit hat, die Gespräche zu überwachen (vgl. Hansjakob 2006: 62), soll mit GovWare Abhilfe geschaffen werden: Sie kann sich in den laufenden Prozess der Software einklinken, und zwar unbemerkt und vor der Verschlüsselung (vgl. Hansjakob 2011: 2-3). Dies muss klar von der (nicht geplanten) Mikrofon-Überwachung unterschieden werden.

Weil die Internettelefonie auch zum Fernmeldeverkehr zählt (vgl. Schmid 2009: 501), muss ihre Überwachung auch im BÜPF geregelt werden. Genauso wie für normale Telefonie gilt auch hier das Fernmeldegeheimnis nach Art. 43 des Fernmeldegesetzes (FMG). Bei einer Überwachung zwecks Beweissicherung wird das Fernmeldegeheimnis aufgrund Art. 269 StPO aufgehoben.

5.2 GovWare – nach den Gesetzesrevisionen

Die Überwachung durch GovWare ist an einige Bedingungen gebunden. Geregelt wird sie im folgenden Gesetzesartikel des BÜPF-Entwurfs, der nachfolgend kommentiert wird:

Art. 269ter Einsatz von besonderen Informatikprogrammen zur Überwachung des Fernmeldeverkehrs (neu)

[1] Die Staatsanwaltschaft kann das Einschleusen von besonderen Informatikprogrammen in ein Datenverarbeitungssystem anordnen, um den Inhalt der Kommunikation und die Randdaten des Fernmeldeverkehrs in unverschlüsselter Form abzufangen und auszuleiten, wenn:

a. die Bedingungen von Artikel 269 Absatz 1 und 3 erfüllt sind;
b. es sich um eine Strafverfolgung nach Artikel 286 Absatz 2 handelt;
c. die bisherigen Massnahmen zur Überwachung des Fernmeldeverkehrs nach Artikel 269 erfolglos geblieben sind oder die Überwachung mit diesen Massnahmen aussichtlos wäre oder unverhältnismässig erschwert würde.

[2] Die Staatsanwaltschaft bezeichnet in der Überwachungsanordnung

a. die gewünschten Datentypen; und

b. die nicht öffentlichen Räume, in die allenfalls eingedrungen werden muss, um besondere Informatikprogramme in das betreffende Datenverarbeitungssystem einzuschleusen.

[3] Durch Absatz 1 nicht gedeckte Daten, die beim Einsatz solcher Informatikprogramme gesammelt werden, sind sofort zu vernichten. Durch solche Daten erlangte Erkenntnisse dürfen nicht verwertet werden.

5.2.1 Technischer Anwendungsbereich

„Als ‚Datenverarbeitungssystem' gilt jedes Gerät, das den Fernmeldeverkehr über das Telefonnetz oder auf einem anderen Weg ermöglicht, zum Beispiel mobile und andere Computer, Mobil- und Festnetztelefone sowie Tablet-Computer" (Botschaft zum BÜPF 2013: 90). Die unter Abs. 1 lit. c genannte Bedingung zeigt zudem an, dass GovWare nur subsidiär zur Anwendung kommen wird.

In der Schweiz soll GovWare nur zur Überwachung von Internettelefonie und verschlüsseltem Mailverkehr zum Einsatz kommen. Es wird vorgeschlagen, den sachlichen Anwendungsbereich von GovWare auf den Kommunikationsinhalt und die Randdaten zu beschränken – „die Online-Durchsuchung soll klar verboten sein" (Botschaft zum BÜPF 2013: 95). Mit dieser ist das unbemerkte Durchsuchen von Dateien gemeint; das BÜPF bezieht sich jedoch nur auf die Überwachung des Fernmeldeverkehrs und nicht auf die gespeicherten Daten. Ebenfalls nicht geplant ist die Überwachung durch das Aktivieren von Kamera oder Mikrofon (vgl. Jurius 2013: 2; Botschaft zum BÜPF 2013: 95).

Die GovWare wird für jedes zu überwachende Datenverarbeitungssystem speziell konfiguriert. Die Staatsanwaltschaft muss dabei die Art der Informationen, die sie erhalten möchte, bestimmen – beispielsweise kann das Programm auf Skype-Gespräche reduziert werden, wenn nur diese nötig sind (vgl. Botschaft zum BÜPF 2013: 93). Dabei wird sehr wahrscheinlich nach dem „Baukasten-Prinzip" vorgegangen: Benötigte Funktionen sind vorgefertigt und können einfach hinzugefügt bzw. ausgeschlossen werden. Allerdings ist zu beachten, dass mehrere Gerätetypen (Computer, Handys, Tablets etc.) überwacht werden sollen, was mehrere Versionen für die verschiedenen Betriebssysteme erfordert. Dies ist auch der Grund für die hohen Kosten, die GovWare aufwirft (vgl. Botschaft zum BÜPF 2013: 93).

5.2.2 Verdachtsgrad und Genehmigung

Laut den Artikeln, auf die verwiesen wurde, ist für die Überwachung ein dringender Tatverdacht notwendig (Art. 269 Abs. 1 lit. a StPO). Bei diesem steht die Eröffnung einer Strafunter-

suchung am Anfang und basiert nicht wie beim hinreichenden Tatverdacht auf bereits durchgeführten Ermittlungen (vgl. Omlin 2011: 2159). „Es müssen […] konkrete Anhaltspunkte vorhanden sein, dass eine strafbare Handlung gemäss Deliktskatalog begangen wurde und dass die zu überwachende Person als Täter in Frage kommt“ (Biedermann 2002: 83), wobei beispielsweise auch der Versuch und die Teilnahme (Anstiftung und Gehilfenschaft) mit erfasst sind (Riklin 2010: 429). Die Schwere der Straftat muss die Überwachung zudem rechtfertigen (lit. b), womit der Grundsatz der Verhältnismässigkeit angesprochen wird (vgl. Riklin 2010: 429). Dieser ist in Art. 5 Abs. 2 BV festgehalten und lautet: „Staatliches Handeln muss im öffentlichen Interesse liegen und verhältnismässig sein“, was für die Überwachungsmassnahmen bedeutet, dass sie gegenüber den Eingriffen in private Interessen abgewogen werden müssen. Die Überwachung einer Straftat, die in einem Katalog (siehe dazu Kapitel 5.2.3) aufgelistet wird, kann unzulässig sein, wenn ihre Schwere zu gering ist (vgl. Riklin 2010: 429). Dieser Aussage steht jedoch entgegen, dass der Deliktskatalog bereits aufgrund der Schwere zusammengestellt worden ist (vgl. Biedermann 2002: 84). Darüber hinaus müssen die bisherigen Untersuchungshandlungen entweder erfolglos geblieben oder die Ermittlungen sonst aussichtlos oder unverhältnismässig erschwert sein (lit. c). Neu wird nicht auf den Straftatenkatalog in Art. 269 Abs. 2 StPO verwiesen, sondern auf den ausgeweiteten Straftatenkatalog in Art. 286 Abs. 2 StPO (siehe dazu Kapitel 5.2.3).

Für die Überwachung durch GovWare ist zudem eine Genehmigung des Zwangsmassnahmengerichts (festgehalten in Art. 274 StPO) vorgesehen (vgl. Botschaft zum BÜPF 2013: 95). Dazu besteht eine skeptische Haltung, beispielsweise von Nationalrat Daniel Vischer: „Die Praxis zeigt aber, dass Gerichte viel zu schnell eine Bewilligung für Überwachungsmassnahmen erteilen und dem Prinzip der Verhältnismässigkeit wenig Beachtung schenken“ (Schaffner 2011: 4). Auch der Wirtschaftsverband Swico (2013: o. S.) bezweifelt die Effektivität dieser „Filterfunktion“.

5.2.3 Straftatenkatalog

GovWare soll nur bei jenen Straftaten, bei denen eine verdeckte Ermittlung zulässig wäre, zur Anwendung gelangen. Diese sind aufgelistet in Art. 286 Abs. 2 StPO. Dabei wird nicht auf den umfangreicheren Straftatenkatalog für Post- und Fernmeldeverkehr (Art. 269 Abs. 2 StPO) zurückgegriffen (vgl. Botschaft zum BÜPF 2013: 12). Allerdings ist auch der Katalog für die verdeckte Ermittlung sehr umfangreich gehalten (und gleicht dem anderen sehr): Bundestrojaner könnten demnach auch zur Aufklärung eines Diebstahls oder einer Sachbeschädigung mit grossem Schaden verwendet werden. Auffällig ist, dass das EJPD aber immer von „besonders schweren Delikten“ spricht (vgl. EJPD 2011c: 1) und immer dieselben drei aufzählt: Kriminelle Organisationen, Terrorismus und Kinderpornografie. Diese waren jedoch nur in 3,5% der Grund für die Überwachungen im Jahr 2012; der Grossteil der Überwachungen entfiel auf Drogenhandel und Finanzdelikte (vgl. Hanimann 2013: o. S.).

Bemerkenswert ist auch, dass mehrfach betont wurde, dass man die Überwachungsmassnahmen des BÜPF klar von den präventiven (nachrichtendienstlichen) Tätigkeiten des Bundes unterscheiden muss (vgl. EJPD 2011c: 2). In der Praxis ist aber eine (theoretisch) präventive Überwachung bei einigen Delikten trotzdem möglich (vgl. Kessler/Isenring 2011: 34): Die „strafbaren Vorbereitungshandlungen" nach Art. 260bis StGB sind ebenfalls Teil des Straftatenkatalogs. Diese beziehen sich auf „konkrete technische oder organisatorische Vorkehrungen", um beispielsweise einen Mord, Raub, Völkermord oder weitere ähnliche Straftaten auszuführen.

5.2.4 Flexibilität

Genauso erwähnenswert ist die Tatsache, dass mit Staatstrojanern auch Dateien ausgelesen werden könnten, die beispielsweise nicht mit einer schweren Straftat in Verbindung stehen. Dies betonte sogar das Bundesamt für Justiz, wobei der Begriff „Trojaner" eher „negativ besetzt" sei, da der Staat schliesslich kein Internetkrimineller sei, sondern im Rahmen des Gesetzes handle (vgl. Gautier 2010: o. S.). Dass mit diesen Programmen auch andere Dateien angesehen werden könnten, ist eine durchaus berechtigte Sorge – der Quellcode der Trojaner lässt sich anpassen und mit weiteren Funktionen versehen. Bei einer Telefonüberwachung werden nur die Gespräche überwacht – Computer bilden aber „sehr grosse Teile unseres Lebens" ab (vgl. Gautier 2010: o. S.): Neben privaten (oder auch geschäftlichen) Informationen könnte man mit Trojanern auch Fotos und andere Dokumente durchforsten (vgl. Botschaft zum BÜPF 2013: 20) sowie Dateien verändern oder ablegen. Da aber keine Online-Durchsuchung von Dateien geplant ist (siehe dazu Kapitel 5.2.1), würde in Fällen, in denen es nicht um die Kommunikationsinhalte, sondern um Dateien (z. B. gespeichertes pornografisches Material) geht, eine Beschlagnahmung durchgeführt.

5.2.5 Kritik und möglicherweise stossende Gesetzesartikel

Ebenfalls kritisiert wird, dass die geplanten Revisionen einen „schwerwiegenden Eingriff in die verfassungsmässig garantierten Grundrechte" darstelle (Digitale Gesellschaft 2011: o. S.). Mit diesem „Eingriff" wird angetönt, dass die geplanten Änderungen an *Art. 13 BV* stossen könnten. Dieser lautet folgendermassen:

> [1] *Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.*
>
> [2] *Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.*

Ebenfalls wurden Konflikte mit Art. 16 BV (Meinungs- und Informationsfreiheit) sowie Art. 10 EMRK (Freiheit der Meinungsäusserung) in Betracht gezogen (vgl. Schlauri 2012: 245). In der Botschaft zum BÜPF (2013: 106) wurde dazu festgehalten, dass das neue BÜPF „keine verfassungsrechtlichen Probleme oder Probleme im Zusammenhang mit dem Völkerrecht" verursa-

che. Laut Art. 36 BV (Einschränkungen von Grundrechten) und Art. 8 EMRK (Recht auf Achtung des Privat- und Familienlebens) „muss die Einschränkung eines Grundrechts durch eine gesetzliche Grundlage gedeckt sein, im öffentlichen Interesse liegen und hinsichtlich des angestrebten Ziels verhältnismässig sein“ (Botschaft zum BÜPF 2013: 106). Die Voraussetzungen seien durch diesen BÜPF-Entwurf erfüllt (vgl. Botschaft zum BÜPF 2013: 106).

5.2.6 Pflichten von Internetanbieterinnen und Betreiberinnen von internen Fernmeldenetzen

Internetanbieterinnen müssten zudem mit einem grösseren finanziellen und personellen Aufwand rechnen, um die Auflagen erfüllen zu können. Sie „sollen weiterhin für die Beschaffung, den Unterhalt und den Betrieb der Überwachungseinrichtungen aufkommen müssen“ und „werden vom Dienst [ÜPF/M.B.] pro Überwachungsmassnahme bezahlt“ (Digitale Gesellschaft 2013: o. S.). Ein Einsatz kostet in Deutschland ungefähr zwischen 10‘000 und 15‘000 Euro, wobei die Auswertung der Daten noch nicht eingerechnet ist (Hansjakob 2011: 6).

Dadurch entsteht der Eindruck, dass Provider fast schon hoffen müssen, dass möglichst viele ihrer Kunden Kriminelle sind, um die anfallenden Kosten amortisieren zu können (vgl. Digitale Gesellschaft 2013: o. S.). In der Botschaft zum BÜPF (2013: 105) wird der Kostenanstieg verharmlost: Bei Unternehmen, die viel Umsatz machen, belaufen sich die Überwachungskosten demgegenüber nur auf einen geringen Betrag und seien „auch angesichts des Effizienzgewinns zu relativieren, der dank dem neuen BÜPF bei der Verfolgung von Straftaten erzielt wird“. Der Bundesrat kann jedoch nach Art. 26 Abs. 6 BÜPF-Entwurf gewisse Anbieterinnen, beispielsweise solche mit „geringer wirtschaftlicher Bedeutung“, von bestimmten gesetzlichen Pflichten befreien.

Anbieterinnen müssen laut Art. 18 Abs. 3 VÜPF die Überwachungsanordnungen so schnell wie möglich ausführen können – auch ausserhalb der Bürozeiten. Auch der Bund müsste mit laufenden Kosten rechnen, weil GovWare ständig erweitert und gewartet werden muss, um mit den technischen Entwicklungen mithalten zu können (vgl. Gautier 2010: o. S.).

Auch die Betreiberinnen von internen Fernmeldenetzen müssen laut Art. 28 BÜPF-Entwurf gewisse Pflichten erfüllen. Sie haben eine Überwachung zu dulden, Zugang zu ihren Anlagen zu gewähren sowie notwendige Auskünfte zu erteilen. Ebenfalls müssen sie auf Verlangen Randdaten zur überwachten Person liefern, falls ihnen diese zur Verfügung stehen. Sie sollen aber nicht dazu gezwungen werden, extra die Daten zu speichern (vgl. Bundesrat 2013: o. S.). Es fragt sich, wer unter einer „Betreiberin von internen Fernmeldenetzen“ zu verstehen ist. Der Artikel soll beispielsweise Arbeitgeber, aber auch Schulen und Spitäler erfassen – nicht verpflichten will man Personen, die zu Hause ein eigenes Netzwerk betreiben (vgl. Bundesrat 2013: o. S.).

6 Mögliche Folgen für die Gesellschaft

6.1 Mögliche negative Folgen

Der Grossteil der analysierten Leserkommentare vermittelt eine klar negative Haltung gegenüber den Gesetzesrevisionen bzw. der Überwachung durch GovWare. Nachfolgend werden die gefundenen Befürchtungen aufgelistet und kritisch gewürdigt sowie mit den Meinungen aus juristischen Quellen ergänzt.

6.1.1 Missbrauch von GovWare durch Dritte

„Aus Sicht der kontaktierten Fachleute aus dem wissenschaftlichen Bereich ist es […] nicht möglich, GovWare zu entwickeln und in Betrieb zu halten, die unter allen Umständen korrekt funktioniert, d.h. keinen Einfluss auf andere Programme oder Funktionen hat“ (Botschaft zum BÜPF 2013: 93-94). Mehrfach geäussert wurde deshalb die Befürchtung, das Programm könne von Kriminellen gehackt und für eigene Zwecke missbraucht werden. Darunter leidet nicht nur die Datensicherheit, sondern auch die Sicherheit des gesamten Netzwerks (vgl. Botschaft zum BÜPF 2013: 92). Hinzu kommt, dass zur erfolgreichen Einschleusung eventuell Virenschutzprogramme umgangen werden müssen (vgl. Botschaft zum BÜPF 2013: 93). Ob diese lediglich umgangen oder deaktiviert werden, wurde nicht festgehalten; letzterer Fall hätte eine zusätzliche Sicherheitseinbusse zur Folge.

Fachleute aus dem Polizeibereich sind der Meinung, dass GovWare „genau und ausschliesslich jenen Zwecken, für die sie programmiert wurde“ dient und dass ihr Einsatz für Netzwerke kein Risiko darstelle, weil keine Komponenten von Netzwerken betroffen seien (vgl. Botschaft zum BÜPF 2013: 93). Diese Aussage ist sehr gewagt – Risiken für Netzwerke wären beispielsweise denkbar, wenn das Programm auf einen Server gelangt. Weiter wird erklärt, dass das widerrechtliche Aneignen, also das Kopieren und Einschleusen der GovWare auf einen anderen Computer, sehr schwierig sei und umfangreiche Kenntnisse und viel Zeit erfordere. Das Programm werde auf jeden zu überwachenden Computer speziell abgestimmt und sei zeitlich beschränkt (vgl. Botschaft zum BÜPF 2013: 93). Daraus zog man folgenden Schluss: „Nach Auffassung der befragten Fachleute aus dem Polizeibereich sind die im Zusammenhang mit GovWare geäusserten Befürchtungen unbegründet“ (Botschaft zum BÜPF 2013: 92).

Als es dem Chaos Computer Club gelang, den von einigen deutschen Bundesländern verwendeten Trojaner zu knacken, stellten sie fest, dass er voller „Anfängerfehler“ war – „das würde ein ambitionierter Informatikstudent im zweiten Semester besser hinbekommen“ (Biermann 2011a: o. S.). Beispielsweise seien die Daten nur ungenügend verschlüsselt und die Befehle zum Steuern des Programms gar im Klartext einsehbar. Dies hat theoretisch zur Folge, dass Kriminelle die Steuerung übernehmen oder sich als Zielcomputer ausgeben und selbst gefälschte Beweise übermitteln könnten. Sehr bedenklich ist in diesem Zusammenhang auch die

Tatsache, dass die gesammelten Daten auf einen Server in den USA übertragen wurden (vgl. Biermann 2011b: o. S.), wo die Betreiber dank dem Bundesgesetz „Patriot Act“ den Behörden Zugang zu den Servern verschaffen müssen (vgl. Peres 2011: o. S.). Dass Dritte den Trojaner für kriminelle Zwecke instrumentalisieren, ist durchaus im Rahmen des Vorstellbaren.

Das EJPD (2011b: o. S.) geht sogar noch weiter:

> „Ziel muss es sein, ein zertifiziertes und sicheres Mittel einzusetzen, das laufend weiterentwickelt und periodisch durch ein komplett neues Mittel abgelöst werden kann. Denkbar wäre also zum Beispiel eine Expertise des Quellcodes der Software durch eine unabhängige Stelle. Diese könnte mögliche Design-Mängel aufzeigen und gegenüber der Öffentlichkeit Klarheit schaffen über die einzelnen Funktionalitäten. Unter Umständen wäre gar eine Offenlegung des Quellcodes möglich. Im Moment sind hierzu noch keine Entscheide gefallen.“

Das Schaffen von Klarheit über die Funktionen des Programms ist durchaus eine begrüssenswerte Idee. Dass das EJPD aber an eine Veröffentlichung des Quellcodes denkt, erweckt den Anschein, dass krampfhaft versucht wird, die Bürger zu beruhigen.

6.1.2 Umgang mit den gesammelten Daten

Im Falle einer Überwachung müssen die gesammelten Daten sicher aufbewahrt werden. Einige Leser haben sich dazu geäussert – sie befürchten, dass mit den gesammelten Daten nicht verantwortungsvoll umgegangen wird. An dieser Stelle sollen jedoch Datenschutz und Datensicherheit nicht umfangreich erläutert werden, sondern kurz die Beziehung zwischen BÜPF und DSG erklärt werden. Nach Art. 2 Abs. 1 lit. b ist das DSG auch anwendbar, wenn Bundesorgane Daten natürlicher oder juristischer Personen bearbeiten. In Abs. 2 lit. c wurde aber festgehalten, dass es nicht anwendbar sei auf „hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren“. Im Zusammenhang mit Überwachungen wird bei den Strafverfahren angeknüpft – allerdings kann momentan nicht abschliessend gesagt werden, in welcher Unterkategorie die Überwachungsmassnahmen des BÜPF eingeordnet werden müssen. Das BÜPF enthält keine Regelungen zum Datenschutz im Umgang mit Personendaten (vgl. Beranek Zanon 2012: 141). Bemerkenswert ist aber, dass das revidierte BÜPF (als „lex specialis“) Vorrang gegenüber der Strafprozessordnung, dem Fernmeldegesetz sowie dem Datenschutzgesetz geniessen wird – deshalb sollten die Bestimmungen dieser Gesetze nicht kollidieren oder Lücken entstehen lassen, sondern sich ergänzen (vgl. Beranek Zanon 2012: 149). „Der Gesetzgeber ist in der […] Revision des BÜPF gefordert, eine Wertung vorzunehmen und klare gesetzliche Grundlagen zu schaffen, die […] ein austariertes Modell [zwischen der Wahrung der Grundrechte und den Interessen der Strafverfolgung/M.B.] ergeben“ (Beranek Zanon 2012: 156). Die Befürchtung, dass mit den gesammelten Daten nicht verantwortungsvoll (im Sinne

des Datenschutzes) umgegangen werden könnte, ist somit gerechtfertigt und zeugt von weitreichenden Überlegungen. Wie die geforderte Austarierung umgesetzt wird, ist jedoch noch unklar.

6.1.3 Kostenüberwälzung

Durch die technischen Aufrüstungen könnten Kosten auf die Kunden der Internetanbieterinnen überwälzt werden. Die hohen Kosten sind (bei der Telefonüberwachung) vor allem auf die Systemwartung und auf die Anpassungen an sich ändernde Anforderungen zurückzuführen – die Überwachungen an sich sind finanziell nicht so aufwändig (vgl. Hansjakob 2006: 23). Welche Kosten für die verschiedenen Überwachungstypen anfallen und welche Anteile entschädigt werden, ist in der GebV-ÜPF einsehbar. Swisscom-Sprecher Olaf Schulze erklärt: „Werden die Aufwände nur teilweise entschädigt, müssen die Anbieterinnen und damit letztlich deren Kunden quasi die Straftäter subventionieren“ (vgl. Schurter 2013a: o. S.). Wird dieser Gedanke fortgeführt, wird bald klar, dass die Kunden bzw. Bürger so oder so für die Überwachungen aufkommen werden – sei es durch höhere Kosten bei den Internetanbieterinnen oder durch Steuerbeiträge – was allerdings Personen, die keinen Internetanschluss besitzen, ebenfalls dazu verpflichtet. Diese Befürchtung ist somit gerechtfertigt.

6.1.4 Überwachung von Mitbenützern

Wenn ein Computer überwacht wird, den mehrere Personen benützen, könnten diese auch in die Überwachung miteinbezogen werden. Deshalb ist eine „Analyse des sozialen Umfelds der Zielperson“ erforderlich, insbesondere in Fällen der Mehrfachbenützung des Internetanschlusses (vgl. Botschaft zum BÜPF 2013: 93). Details zu dieser Analyse sind anscheinend noch nicht bekannt. Erfreulich ist, dass laut Art. 23 lit. g Ziff. 4 VÜPF eine Überwachungsanordnung „zusätzliche Vorkehren zum Schutz nicht beteiligter Benützerinnen und Benützer“ enthalten muss, was zeigt, dass dieses Problem erkannt wurde. Betroffene Mitbenützer können sich, wie in Art. 279 Abs. 3 StPO geregelt, beschweren. Ob Mitbenützer ganz von Überwachungen ausgeschlossen können, ist momentan noch nicht klar – es dürfte jedoch schwierig sein, die Überwachung so genau auf die Zielperson abzustimmen, dass keine Daten über Mitbenützer gesammelt werden. Diese Befürchtung ist somit teilweise gerechtfertigt.

6.1.5 Verwertbarkeit von Beweisen

Manche Leser haben sich gefragt, ob einerseits rechtmässig gesammelte Daten und andererseits „Zufallsfunde“ überhaupt als Beweise verwertbar seien. Wenn es dabei um die überwachte Person geht, besteht eine Regelung in Art. 278 Abs. 1 StPO: „Werden durch die Überwachung andere Straftaten als die in der Überwachungsanordnung aufgeführten bekannt, so können die Erkenntnisse gegen die beschuldigte Person verwendet werden, wenn zur Verfolgung dieser Straftaten eine Überwachung hätte angeordnet werden dürfen.“

Ist eine Drittperson betroffen, können laut Art. 278 Abs. 2 StPO „Erkenntnisse über Straftaten einer Person, die in der Anordnung keiner strafbaren Handlung beschuldigt wird, […] verwendet werden, wenn die Voraussetzungen für eine Überwachung dieser Person erfüllt sind." Im nachfolgenden Abs. 3 wurde zudem festgehalten, dass die Staatsanwaltschaft in beiden genannten Fällen unverzüglich eine Überwachung anordnet und das Genehmigungsverfahren einleitet. Dazu äussert sich der Swico (2013: o. S.): „Völlig unbeteiligte Dritte können von den Überwachungen miterfasst werden. Diese Personen haben keine Rechtsmittel, um sich dagegen zu wehren", weil sie nicht das Ziel der Überwachung seien. Weil das Bundesgericht seine Haltung zu unrechtmässig erlangten Beweisen immer wieder gelockert hat, sei die Chance der Verwertung von „Zufallsfunden" über Dritte gross – nämlich dann, wenn das „öffentliche Interesse an der Wahrheitsfindung" das „private Interesse des Angeklagten an der Unverwertbarkeit" überwiegt (vgl. Swico 2013: o. S.).

Aber auch wenn die Strafbehörden Beweise „in strafbarer Weise" erhoben haben, dürfen sie laut Art. 141 StPO verwertet werden, und zwar dann, wenn sie „zur Aufklärung schwerer Straftaten unerlässlich" sind.

Es kann abschliessend nicht allgemein gesagt werden, ob durch GovWare gesammelte Beweise verwertbar sein werden oder nicht. Wie mir Rechtsanwalt Martin Steiger auf Nachfrage bestätigt hat, wird die Verwertbarkeit im Einzelfall im Verfahren bzw. vor Gericht entschieden, wobei oft Experten beigezogen werden. In der Praxis sind noch weitere Hindernisse denkbar, welche die Beweisverwertbarkeit beeinträchtigen könnten, beispielsweise technische Defekte, Verbindungsabbrüche oder Kopierfehler.

6.1.6 Vertrauen gegenüber dem Staat sinkt

Eine häufig geäusserte Meinung ist, dass sich der Staat anscheinend vor den Bürgern fürchtet und somit deren Vertrauen gegenüber dem Staat sinkt (in diesem Zusammenhang wurde auch häufig der Fichenskandal in den 80er-Jahren erwähnt). Dies lässt sich dadurch erklären, dass der Staat scheinbar nur das nötigste an Informationen preisgibt. Im Medienrohstoff zum BÜPF und zur VÜPF ist beispielsweise mit keinem Wort die Rede von GovWare, Software oder Informatikprogrammen (vgl. EJPD 2011c: 1-3). Leser kritisieren mehrfach diese „Salamitaktik", nach der die Wahrheit „Scheibchen für Scheibchen" präsentiert wird (vgl. Schweizer Fernsehen 2010: o. S.), und befürchten, dass die Überwachung später genauso ausgeweitet wird (beispielsweise durch die Befürwortung der Webcam- bzw. Mikrofonüberwachung).

Diese Befürchtungen hängen mit Medienberichterstattungen zusammen: Untersuchungen haben gezeigt, dass Massenmedien „zweifellos ein stark deformiertes Bild der Wirklichkeit [vermitteln/M.B.], indem sie sich klar auf schwere, dramatische und vor allem ungewöhnliche Vorfälle konzentrieren" (Killias/Kuhn/Aebi 2011: 358). Zum Verlauf einer Straftat berichten die Medien heutzutage über längere Zeit – beispielsweise erscheinen umfangreiche Artikel, wenn

der Täter einem Gericht vorgeführt wird, obwohl dies ein ganz normaler Schritt in einem juristischen Prozess darstellt. Die Leser haben eine verzerrte Vorstellung vom Ausmass dieser Straftat, sie werden eingeschüchtert und das Gefühl eines Ausnahmezustandes beschleicht sie (so kann ein Terroranschlag schnell als „Kriegserklärung" verstanden werden). In diesem Zustand werden die Menschenrechte „zurückgestellt", d. h. die Sicherheit bzw. das Sicherheitsgefühl geht vor. Weil aber Gefahren und Bedrohungen diffus und nicht greifbar sind, und Massenmedien die „unstrukturierte Kommunikation über Gerüchte [fördern können/M.B.]" (Killias/Kuhn/Aebi 2011: 359), reagiert der Staat darauf selbst diffus (vgl. Schweizer Fernsehen 2010: o. S.) „Die Medien als ‚Echokammer der Massenhysterie', wie das der ‚Guardian' nach dem Mord an einem Soldaten in Woolwich genannt hat, drängen die Politik zu immer schnelleren und unüberlegteren Reaktionen: Möge nur etwas passieren, sofort, egal was" (Loser 2013: o. S.).

Diese diffuse Reaktion von staatlicher Seite wurde bereits erkannt. Der Wirtschaftsverband Swico (2013: o. S.) schreibt zum publizierten Gesetzesentwurf und zur Botschaft:

> „Die Vorlage ist insgesamt einseitig ausgerichtet und inhaltlich überzogen. Sie stellt die Strafverfolgung über die Bürgerrechte und den Anspruch auf Wahrung der Privatsphäre, ohne die Notwendigkeit ausreichend begründen zu können. Die Botschaft reitet auf der Welle einer diffusen Angst vor Kriminalität jeglicher Art sowie des Unbehagens der Staatsorgane vor dem gewaltigen (positiven und negativen) Potenzial des Internets."

6.1.7 Verwässerung unserer Werte

Einige Leser vermuten auch, dass die Gesetzesrevisionen von Änderungen im Ausland beeinflusst wurden und sich dadurch unsere Werte verwässern. Die aktuellen Entwicklungen zeigen tatsächlich, dass einige Länder die Überwachung ausweiten. So führt beispielsweise Indien ein zentrales Überwachungssystem ein, das sowohl alle Telefongespräche, E-Mails, Webseiten und auch alle Aktivitäten in sozialen Netzwerken überwacht; begründet wird dies mit den Terroranschlägen im 2008 in Mumbai (Sobiraj 2013: o. S.). Auch Grossbritannien plant eine ausgeweitete Überwachung, bei der die Vorratsdatenspeicherung ebenfalls auf zwölf Monate angehoben werden könnte und zusätzlich weitere Daten wie Facebook-Nachrichten, Daten von Online-Spielen und Chats aufgezeichnet werden sollen (vgl. Sobiraj 2012: o. S.). In der Botschaft zum BÜPF (2013: 21) wird auch kurz beschrieben, dass in Deutschland und Frankreich die Überwachung durch GovWare unter bestimmten Voraussetzungen zulässig ist, in Österreich an einer Rechtsgrundlage gearbeitet werde und die Situation in Italien nicht ausdrücklich geregelt scheint. Es gibt Anhaltspunkte, dass sich die Schweizer Gesetzgebung ausländischem Recht weiter annähert. Ein Indiz ist das streng geheime Abhörsystem „Onyx" des Nachrichtendienstes des Bundes (NDB). Die Errichtung von Parabolantennen in der Schweiz und die verdeckte und illegale Finanzierung des Systems wurden 2005 publik (vgl. Engeler 2005: o. S.). Die

Swisscom hat den Standort in Leuk zudem an ein amerikanisches Unternehmen verkauft, welches auch das US-Verteidigungsministerium beliefert (vgl. Engeler 2005: o. S.). Was genau abgehört wird, ist unklar, allerdings sind „die mit Hilfe von Onyx eingeholten Informationen […] auch ein Instrument, mit dem die Türen zu anderen Nachrichtendiensten geöffnet werden können und mit dem sich die schweizerischen Nachrichtendienste im Ausland Glaubwürdigkeit verschaffen können“ (Engeler 2005: o. S.). Ein weiterer Hinweis ist, dass die BÜPF-Revision als „Nachteil für den ICT-Standort Schweiz“ und als „Anti-Swissness-Vorlage“ angesehen wird (vgl. Urech 2013: o. S.). Aufgrund dieser Hinweise und der aktuellen Veränderungen im Ausland wird diese Befürchtung als gerechtfertigt betrachtet. Es besteht sicherlich ein Einfluss auf gewisse Werte in unserer Gesellschaft – welche Werte genau betroffen sein werden, müsste in einer detaillierten Untersuchung festgestellt werden.

6.1.8 Schwerer Eingriff in die Grundrechte

„Wer nichts zu verbergen hat, hat auch nichts zu befürchten“ – dieser Satz wurde sinngemäss unglaublich oft als Leserkommentar hinterlassen, worauf andere Leser eine Diskussion begannen. Oft wurde auch kommentiert, dass heutzutage sowieso schon unzählige Firmen, seien es Supermärkte mit Bonusprogrammen oder soziale Netzwerke, unsere Daten sammeln. Dass der Unterschied aber darin besteht, dass wir diesen unsere Daten freiwillig bekanntgeben, wurde oft übersehen; man spricht dabei von der „Entwicklung einer Indifferenz“ (Schweizer Fernsehen 2010: o. S.), d. h. man differenziert nicht mehr zwischen zwei verschiedenen Konzepten. Deshalb wird ein Eingriff in die Privatsphäre nicht automatisch gerechtfertigt, wenn man „sowieso nichts zu verbergen hat“: Das Recht auf Privatsphäre ist gesetzlich verankert und jeder hat Anspruch auf dessen Achtung. Obwohl eine Rechtfertigung des Eingriffs laut Art. 36 BV und Art. 8 EMRK besteht (siehe dazu Kapitel 5.2.4), handelt es sich immer noch um einen schwerwiegenden Eingriff in unsere Grundrechte.

6.2 Mögliche positive Folgen

Es fanden sich – wenn auch wenige – positive Folgen in Form von Hoffnungen. Diese werden nachfolgend erläutert und kritisch betrachtet.

6.2.1 Mehr Sicherheit vor Kriminellen

Ob eine Erhöhung der Sicherheit durch zunehmende Überwachungen stattfindet, ist leider nicht bekannt, weil das Bundesamt für Statistik „keine Daten zu den Vorgehen bei der Verbrechensaufklärung“ erfasst (vgl. Simonet 2011: o. S.). Es ist lediglich feststellbar, wie viele Überwachungen durchgeführt wurden: Im Zeitraum von 1998 bis 2012 verzeichnete die Anzahl rückwirkender Überwachungen einen Anstieg von über 250 Prozent, und Echtzeit-Überwachungen weisen eine leichte Zunahme auf (vgl. Hanimann 2013: o. S.).

In Deutschland wurden die konkreten Ziele von Überwachungen untersucht, wobei die Ergebnisse auch auf die Schweiz zutreffen sollten. Die Angaben stammen aus verschiedenartigen Überwachungsanträgen und sind daher nicht abschliessend. In jeweils rund 40% war das Ziel, Äusserungen der Zielperson zum Tatvorwurf zu erhalten oder Mittäter identifizieren zu können. Je rund 10% der Überwachungsanträge bezweckte die Ermittlung der Struktur einer Organisation oder deren Aufenthaltsort (vgl. Albrecht/Dorsch/Krüpe 2003: 442). In 75% der Überwachungen waren die Ergebnisse beweisrelevant. Interessant ist dabei, dass sie danach bei der Anklageerhebung nur noch in etwa einem Fünftel der Fälle eine Rolle spielten, weil in diesen allein ihr Vorhalt zu Geständnissen führte. Dies bedeutet, dass die Überwachung eher benutzt wird, um obige Beweise zu erlangen, und nicht, um die Straftat an sich zu beweisen (vgl. Albrecht/Dorsch/Krüpe 2003: 463). Dass dieser Effekt auch bei GovWare zustande kommen könnte, ist denkbar.

6.2.2 Veränderung der Kommunikation

Es wäre theoretisch möglich, dass sich die gesellschaftliche Kommunikation zum Positiven verändert. Aus Angst vor überwachten elektronischen Kommunikationsmitteln würden dann wieder vermehrt persönliche Gespräche geführt werden. Dies ist ein schöner Gedanke, allerdings darf nicht vergessen werden, dass Geräte wie Handys, Tablets oder Laptops zum alltäglichen Bestandteil des Alltags geworden sind und die Menschen auch nicht mehr darauf verzichten möchten – ausserdem sind auch in diesem Bereich noch zahlreiche technische Neuheiten zu beobachten, beispielsweise die Augmented-Reality-Brille „Google Glass“. Dieses Argument wurde in den Leserkommentaren oft ausser Acht gelassen. Interessant war aber, dass sehr viele Leser den anderen Tipps gegeben haben, wie sich diese vor GovWare schützen können. Dabei erwiesen sich einige Ratschläge als sehr differenzierte Aussagen, beispielsweise das Arbeiten mit einer Live-CD (das gesamte Betriebssystem wird von einer CD geladen; die Festplatte wird nicht benötigt). Andere Aussagen stammten eindeutig von Laien: Das Verschlüsseln der Festplatte verhindert den Zugriff des Programms nicht, wenn es bereits installiert ist, und dass die GovWare nur für Windows programmiert wird, ist denkbar unwahrscheinlich.

7 Fazit und Ausblick

Die Analyse der Leserkommentare und die kritische Würdigung durch juristische Quellen hat gezeigt, dass die Thematik vor allem in der 20 Minuten Einzug in den gesellschaftlichen Diskurs gehalten hat. Die hohe Anzahl der Leserkommentare veranschaulicht dabei, dass sich die Mehrheit der Leser entschieden gegen die Überwachungspläne des Bundes wehren, auch wenn sich in einigen Leserkommentaren Falschannahmen finden lassen. Dies rechtfertigt sich aber dadurch, dass der Bund tatsächlich zu Beginn sehr wenige Details bekanntgibt (zur „Salamitaktik“ siehe Kapitel 6.1.6). Damit wird von Vornherein eine Basis für Befürchtungen geschaffen: Beispielsweise hatten viele Leser die Online-Durchsuchung der gespeicherten Datei-

en befürchtet, weil erst im späteren Verlauf bekanntgegeben wurde, dass keine Online-Durchsuchung geplant ist.

Die nachfolgende Tabelle zeigt eine Übersicht über alle besprochenen möglichen Folgen und deren Befunde. Diese sagen aus, ob die Befürchtungen bzw. Hoffnungen gerechtfertigt sind und ob sie tendenziell eintreten werden oder nicht.

Tabelle 1: Mögliche Folgen und Befunde

+/-	Mögliche Folgen	Befund
-	Missbrauch von GovWare	gerechtfertigt, wahrscheinlich
-	Umgang mit gesammelten Daten	gerechtfertigt, Details unklar
-	Kostenüberwälzung	gerechtfertigt, wahrscheinlich
-	Überwachung von Mitbenützern	teilweise gerechtfertigt, Details unklar
-	Verwertbarkeit von Beweisen	gerechtfertigt, wahrscheinlich
-	Vertrauen gegenüber dem Staat sinkt	gerechtfertigt, wahrscheinlich
-	Verwässerung unserer Werte	gerechtfertigt, Details unklar
-	Schwerer Eingriff in die Grundrechte	gerechtfertigt, besteht
+	Mehr Sicherheit vor Kriminellen	unklar, da keine Statistiken
+	Veränderung der Kommunikation	eher unwahrscheinlich

Quelle: Eigene Darstellung

Nach Ansicht des EJPD lassen die besprochenen Gesetzesrevisionen die Schweiz nicht zu einem „Schnüffelstaat“ werden. Diese Aussage wird damit begründet, dass nicht präventiv überwacht werden darf – es gehe „nicht darum, mehr zu überwachen, geschweige denn auf Vorrat zu ‚schnüffeln‘“ (EJPD 2011b: o. S.). Die präventive Überwachung wird aber neben dem BÜPF ausgeweitet. Seit Oktober 2010 wird an einem neuen Gesetz, dem Nachrichtendienstgesetz (NDG), gearbeitet. Dieses soll „frühestens Mitte 2015“ in Kraft treten (vgl. VBS o. J.: o. S.) und sieht vor, die Post- und Fernmeldeüberwachung nur zu präventiven Zwecken anzuwenden, um Bedrohungen der inneren oder äusseren Sicherheit der Schweiz frühzeitig zu erkennen (vgl. VBS 2013: 38). Auch das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) wird revidiert. „Die [im BWIS/M.B.] zu regelnde präventive Überwachung wird jedoch nicht [wie im BÜPF/M.B.] zum Zweck der Strafverfolgung durchgeführt, sondern zur Erkennung von konkreten Gefährdungen durch Terrorismus, verbotenen politischen und militärischen Nachrichtendienst und verbotenen Handel mit Waffen und radioaktiven Materialien sowie durch verbotenen Technologietransfer“ (Bundesamt für Polizei fedpol 2006: 57).

Zum Zeitpunkt dieser Arbeit halten die Überwachungsmassnahmen der USA weltweit Einzug in die Schlagzeilen: Es ist bekannt geworden, dass die National Security Agency (NSA) mit dem Überwachungsprogramm „Prism“ weltweit die Onlinekommunikation von Menschen überwa-

chen kann. Dies geschieht über Schnittstellen, die grosse Unternehmen wie Apple, Facebook, Google oder Microsoft installiert haben, um Daten (wenn rechtlich gefordert) an die Behörde zu übertragen. Angeblich soll die NSA aber direkt auf gewisse Server und somit auf Millionen von Nutzerdaten zugreifen können (vgl. Beuth/Biermann 2013: o. S.).

Am 19. Juni 2013 war US-Präsident Barack Obama zu Besuch in Deutschland. An der Pressekonferenz fiel von Bundeskanzlerin Angela Merkel der Satz „*Das Internet ist für uns alle Neuland*, und es ermöglicht natürlich auch Feinden und Gegnern unserer demokratischen Grundordnung, mit völlig neuen Möglichkeiten und völlig neuen Herangehensweisen unsere Art zu leben in Gefahr zu bringen“ (Merkel 2013: o. S./Hervorheb. M.B.). Diese Aussage löste einen unglaublichen Sturm der Entrüstung aus – vor allem auf Twitter wurden tausende Tweets zum Hashtag #neuland abgesetzt, die überwiegend negativ waren. Dieser Satz genügt natürlich in keiner Weise als Rechtfertigung des Überwachungsprogramms Prism, aber er beleuchtet das Thema aus einer anderen Perspektive: Politiker, die die Funktionsweise und die vielen (positiven) Seiten des Internets nicht kennen, sehen es als etwas Feindliches und schränken es durch Überwachungsmassnahmen ein (vgl. „Drachenrose“ 2013: o. S.) bzw. rechtfertigen diese (zu den „Fachleuten aus dem Polizeibereich“ siehe Kapitel 6.1.1). Das soll jedoch nicht verallgemeinernd heissen, dass Politiker keine Ahnung von Technik haben – Angela Merkel hat beispielsweise auf ihrer ersten Website aus dem Jahr 2000 bereits Folgendes geschrieben: „Demokratie braucht Offenheit, denn nur sie schafft Vertrauen und nötige Kontrolle. Deshalb hat das Internet gerade in den letzten Monaten für die politische Arbeit deutlich an Bedeutung gewonnen“ (Merkel 2000: o. S.).

Allerdings ist es wahr, dass sich das Internet ständig weiterentwickelt und immer neue Plattformen, Technologien und Möglichkeiten hinzukommen, mit denen sich zwangsläufig auch unsere Kommunikation verändert und unsere Gesetze angepasst werden müssen. Deshalb sollte Merkels Aussage in dem Sinne interpretiert werden, dass wir das Internet ständig hinterfragen (vgl. Seiffert 2013: o. S.) und uns nicht blind darauf verlassen sollten.

Weiterführende Forschungen könnten beispielsweise die Veränderungen in der gesellschaftlichen Kommunikation betrachten, die mit der Legalisierung von GovWare einhergehen. Ebenfalls interessant ist und bleibt das Verhältnis von Sicherheit und Privatheit – wie wird es sich verändern? Werden in Zukunft die Interessen anders abgewogen und gewichtet? Ein anderer Ansatz könnte die Positionen von Schweizer Parteien analysieren und mögliche Tendenzen verorten. Dass die Gesellschaft auch Mittel ergreift, um gegen die Gesetzesrevisionen vorzugehen, zeigt sich an der Lancierung einer Online-Petition (www.buepf.ch), die von mehreren Organisationen und politischen Parteien unterstützt wird. Der Stand beim Abschluss dieser Arbeit betrug etwa 8000 Unterschriften.

Literaturverzeichnis

Aebi-Müller, Regina E. (2005): Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes. Unter besonderer Berücksichtigung der Rechtslage in der Schweiz und in Deutschland. Bern.

Albrecht, Hans-Jörg/Dorsch, Claudia/Krüpe, Christiane (2003): Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmassnahmen. Eine rechtstatsächliche Untersuchung im Auftrag des Bundesministerium der Justiz. Freiburg i. Br.

Beranek Zanon, Nicole (2012): Datenaufbewahrungspflichten vs. Datenlöschungspflichten. Kollision von BÜPF und DSG? In: Weber, Rolf H./Thouvenin, Florent (Hg.): Neuer Regulierungsschub im Datenschutzrecht? Zürich/Basel/Genf, S. 131-156.

Beuth, Patrick/Biermann, Kai (2013): Das Spionagesystem Prism und seine Brüder. In: http://www.zeit.de/digital/datenschutz/2013-06/nsa-prism-faq/komplettansicht (18.06.2013).

Biedermann, August (2002): Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000. In: Schweizerische Zeitschrift für Strafrecht 120, H. 1, S. 77-106.

Biermann, Kai (2011a): Schlampige Software voller Anfängerfehler. In: http://www.zeit.de/digital/datenschutz/2011-10/trojaner-software/komplettansicht (18.05.2013).

Biermann, Kai (2011b): CCC enttarnt Staatstrojaner. In: http://www.zeit.de/digital/datenschutz/2011-10/ccc-bundestrojaner-onlinedurchsuchung/komplettansicht (18.05.2013).

Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) (verabschiedet am 27. Februar 2013).

Bundesamt für Polizei fedpol (2006): Vorentwurf fedpol vom 31.01.2006 zum Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS). Erläuternder Bericht. In: http://www.ejpd.admin.ch/content/dam/data/sicherheit/bwis/erlaeuterungen_bwisiid.pdf (12.06.2013).

Büsser, Bettina (2013): Kommentare von rechts. In: EDITO+KLARTEXT o. Jg., H. 2, S. 26-27.

Denninger, Erhard (1985): Das Recht auf informationelle Selbstbestimmung und Innere Sicherheit. Folgerungen aus dem Volkszählungsgesetzurteil des Bundesverfassungsgerichts. In: Kritische Justiz 18, H. 3, S. 215-244.

Digitale Gesellschaft (2011): Stellungnahme zur geplanten Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF). In: http://grundrechte.ch/CMS//nein-zur-revision-der-verordnung-betreffend-die-ueberwachung-des-post-und-fernmeldeverkehrs-vuepf.html (07.03.2013).

Digitale Gesellschaft (2013): 12 Monate Vorratsdatenspeicherung, Trojaner Federal, IMSI-Catcher – das neue BÜPF. In: http://www.digitale-gesellschaft.ch/2013/02/28/12-monate-vorratsdatenspeicherung-trojaner-federal-imsi-catcher-das-neue-bupf (22.04.2013).

„Drachenrose“ (2013): Das eigentliche Drama von Neuland. In: http://drachenrose.wordpress.com/2013/06/20/das-eigentliche-drama-von-neuland (20.06.2013).

Eggimann, Patrick (2013): Neuer Regulierungsschub im Datenschutzrecht? In: sic! - Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht o. Jg., H. 2, S. 112-116.

Eidgenössisches Justiz- und Polizeidepartement (EJPD) (2011a): Revision des Gesetzes und der Verordnung. In: http://www.ejpd.admin.ch/content/ejpd/de/home/themen/sicherheit/ueberwachung_des_post-/revision_buepf_undvuepf.html (07.03.2013).

Eidgenössisches Justiz- und Polizeidepartement (EJPD) (2011b): FAQ – Häufig gestellte Fragen. In: http://www.ejpd.admin.ch/content/ejpd/de/home/themen/sicherheit/ueberwachung_des_post-/faq_vuepf.html (19.05.2013).

Eidgenössisches Justiz- und Polizeidepartement (EJPD) (2011c): Revision des BÜPF und der VÜPF (Medienrohstoff). In: http://www.ejpd.admin.ch/content/dam/data/sicherheit/uepf/mr_buepf_vuepf-de.pdf (25.05.2013).

Engeler, Urs Paul (2005): Was sagen Sie jetzt? In: http://www.weltwoche.ch/ausgaben/2005-10/artikel-2005-10-was-sagen-sie-je.html (20.06.2013).

Gautier, Dinu (2010): Der Staat in deinem Computer. In: http://www.woz.ch/1021/online-durchsuchungen/der-staat-in-deinem-computer (09.03.2013).

Gless, Sabine (2012): Strafverfolgung im Internet. In: Schweizerische Zeitschrift für Strafrecht 130, H. 1, S. 3-22.

Hanimann, Carlos (2013): Wir sind alle verdächtig. In: http://www.woz.ch/1312/vorratsdatenspeicherung/wir-sind-alle-verdaechtig (25.05.2013).

Hansjakob, Thomas (2006): BÜPF/VÜPF. Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs. St. Gallen.

Hansjakob, Thomas (2011): Einsatz von GovWare – zulässig oder nicht? Zum Einsatz von Computerprogrammen bei der Überwachung von Internet-Telefonie. In: Jusletter 5. Dezember 2011.

Heiniger, Andreas (2013): Das Bundesgericht geht in der Fernmeldeüberwachung weiter, als es das Gesetz erlaubt. Anmerkungen zu BGE 1B_481/2012 vom 22. Januar 2013. In: Jusletter 29. April 2013.

Henatsch, Martin (2007): Kunst im Spannungsfeld von Sicherheit und Freiheit. In: Surveillance Studies. Perspektiven eines Forschungsfeldes. Leverkusen, S. 167-180.

Hornung, Gerrit (2007): Über Möglichkeiten und Grenzen der rechtlichen Bewertung neuer Überwachungstechnologien. In: Zurawski, Nils (Hg.): Surveillance Studies. Perspektiven eines Forschungsfeldes. Leverkusen, S. 149-166.

Jotterand, Olivier/Müller, Jérémie/Treccani, Jean (2012): L'utilisation du cheval de Troie comme mesure de surveillance secrète. In: Jusletter 21. Mai 2012.

Jurius (2013): Klare Rechtsgrundlage zum Einsatz von GovWare. In: Jusletter 4. März 2013.

Kessler, Martin A./Isenring, Bernhard (2011): Die geplante Total-Revision des BÜPF im Überblick. In: Sicherheit & Recht o. Jg., H. 1, S. 24-36.

Killias, Martin/Kuhn, André/Aebi, Marcelo F. (2011): Grundriss der Kriminologie. Eine europäische Perspektive. Bern.

Loser, Philipp (2013): Diktatur der Idioten. In: http://www.tageswoche.ch/de/2013_21/schweiz/545719/diktatur-der-idioten.htm (12.06.2013).

Maurer-Lambrou, Urs/Kunz, Simon (2006): Anwendungsbereich von Art. 1 DSG. In: Maurer-Lambrou, Urs/Vogt, Nedim Peter (Hg.): Datenschutzgesetz. Basel, S. 33-41.

Merkel, Angela (2000): Homepage von Angela Merkel (Stand: 10. Mai 2000). In: http://web.archive.org/web/20000510190612/http://www.angela-merkel.de (20.06.2013).

Merkel, Angela (2013): Pressekonferenz von Bundeskanzlerin Merkel und US-Präsident Obama. In: http://www.bundeskanzlerin.de/Content/DE/Mitschrift/Pressekonferenzen/2013/06/2013-06-19-pk-merkel-obama.html (20.06.2013).

Müller, Markus M. (2008): Demokratische Anforderungen an die Herstellung von Sicherheit. In: Brodocz, André/Llanque, Marcus/Schaal, Gary S. (Hg.): Bedrohungen der Demokratie. Wiesbaden, S. 189-202.

Omlin, Esther (2011): Aufgaben der Staatsanwaltschaft. In: Niggli, Marcel Alexander/Heer, Marianne/Wiprächtiger, Hans (Hg.): Schweizerische Strafprozessordnung, Jugendstrafprozessordnung. Basel, S. 2147-2190.

Peres, Robert (2011): The American Way of Terrorbekämpfung. In: http://www.lto.de/recht/hintergruende/h/zehn-jahre-patriot-act-the-american-way-of-terrorbekaempfung (18.05.2013).

Platz, Ernst (2008): Rechtliche Zulässigkeit von "Remote Forensic Software" in der Schweiz. Inwieweit existiert in der Schweiz eine rechtliche Grundlage für den Einsatz von "Remote Forensic Software" durch die Ermittlungsbehörden? In: sic! - Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht o. Jg., H. 11, S. 839-844.

Rhyner, Beat/Stüssi, Dieter (2008): Überwachung mit technischen Überwachungsgeräten (Art. 280-281). In: Albertini, Gianfranco (Hg.)/Fehr, Bruno (Hg.)/Voser, Beat (Hg.): Polizeiliche Ermittlung: Ein Handbuch der Vereinigung der Schweizerischen Kriminalpolizeichefs zum polizeilichen Ermittlungsverfahren gemäss der Schweizerischen Strafprozessordnung. Zürich, S. 462-470.

Riklin, Franz (2010): StPO Kommentar. Schweizerische Strafprozessordnung mit StBOG, JStPO und den relevanten Bestimmungen aus BV, EMRK und BGG. Zürich.

Rössler, Beate (2001): Der Wert des Privaten. Frankfurt am Main.

Schaffner, David (2011): Sommaruga setzt der Überwachung im Internet nun Grenzen. In: Tages-Anzeiger vom 24.11.2011, S. 4.

Schlauri, Simon (2012): Fernmeldeüberwachung à discrétion? In: sic! - Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht o. Jg., H. 4, S. 238-247.

Schmid, Niklaus (2009): Schweizerische Strafprozessordnung (StPO): Praxiskommentar. Zürich.

Schurter, Daniel (2013a): «Kunden müssen Straftäter subventionieren». In: http://www.20min.ch/finance/news/story/-Kunden-muessen-Straftaeter-subventionieren--18213422 (18.05.2013).

Seiffert, Peter (2013): Frau Merkel hat Recht: Wir leben alle im #neuland. In: http://www.focus.de/panorama/seiffertsagtan/kanzlerin-und-internet-frau-merkel-hat-recht-wir-leben-alle-im-neuland_aid_1020228.html (20.06.2013).

Simonet, Denis (2011): Wo bleiben die Fakten? In: http://www.denissimonet.ch/2011/07/05/wo-bleiben-die-fakten (27.05.2013).

Sobiraj, Lars (2012): Großbritannien plant totale Überwachung: Vorratsdatenspeicherung 2.0 in Arbeit. In: http://www.gulli.com/news/19091-grossbritannien-plant-totale-ueberwachung-vorratsdatenspeicherung-20-in-arbeit-2012-06-18 (25.05.2013).

Sobiraj, Lars (2013): Indien führt zentrales Überwachungssystem ein. In: http://www.gulli.com/news/21479-indien-fuehrt-zentrales-ueberwachungssystem-ein-2013-05-08 (25.05.2013).

Steiger, Martin (2011): Bundestrojaner ohne Rechtsgrundlage in der Schweiz. In: http://www.steigerlegal.ch/2011/10/13/bundestrojaner-ohne-rechtsgrundlage-in-der-schweiz (09.03.2013).

Stöckli, Corinne (2011): „Einfach nur dreist“. In: plädoyer 29, H. 6, S. 15-17.

Swico (2013): Gegen Überwachungsexzesse der Strafverfolger. In: http://www.swico.ch/aktuell-medien/medienmitteilungen/gegen-ueberwachungsexzesse-der-strafverfolger/2131 (27.05.2013).

Urech, Marcel Maurice (2013): „Die BÜPF-Revision ist eine Anti-Swissness-Vorlage“. In: http://www.netzwoche.ch/News/2013/05/31/Die-BUePF-Revision-ist-eine-Anti-Swissness-Vorlage.aspx (22.06.2013).

VBS (2013): Nachrichtendienstgesetz (NDG). Bericht zum Vorentwurf. In: http://www.vbs.admin.ch/internet/vbs/de/home/themen/ndb/dokumente.parsys.8775.downloadList.60466.DownloadFile.tmp/ndgbericht20130308.pdf (12.06.2013).

VBS (o. J.): Nachrichtendienstgesetz. In: http://www.vbs.admin.ch/internet/vbs/de/home/themen/ndb/uebersicht.html (22.04.2013).

Warren, Samuel D./Brandeis, Louis D. (1984): The Right to Privacy. In: Schoeman, Ferdinand David: Philosophical Dimensions of Privacy. An Anthology. Cambridge, S. 75-103.

Weniger, Robert (2005): Grenzüberschreitende Datenübermittlungen international tätiger Unternehmen. Nach Maßgabe der Europäischen Datenschutzrichtlinie 95/46/EG. Hamburg.

Videos

Bundesrat (2013): Medienkonferenz des Bundesrates vom 27.2.2013. Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). In: http://www.tv.admin.ch/de/archiv?video_id=537 (12.06.2013).

Schweizer Fernsehen (2010): Alles ist durchleuchtet: Gespräch mit Juli Zeh und Ilija Trojanow. In: Sternstunde Philosophie vom 17.01.2010, http://www.srf.ch/player/tv/sternstunde-philosophie/video/alles-ist-durchleuchtet-gespraech-mit-juli-zeh-und-ilija-trojanow?id=489b3650-dce3-4072-a20b-f6ce970f6e35.

Schweizer Fernsehen (2011): Was macht ein Staatstrojaner? In: SF 10vor10 vom 14.10.2011, http://www.srf.ch/player/tv/10vor10/video/was-macht-ein-staatstrojaner?id=cde6f8d2-b733-4c3e-863a-bfe554c265bb.

Analysierte Leserkommentare

Artikel mit Autorenkürzeln, die nicht bestimmt werden konnten, sind in Klammern aufgeführt. Neben dem Abrufdatum wurde die Anzahl Leserkommentare zu diesem Zeitpunkt vermerkt.

(20minutes) (2011): Linksaktivistin Stauffacher ausgeschnüffelt. In: http://www.20min.ch/schweiz/news/story/25233283 (26.05.2013, 74 Kommentare).

(mbu/mdr) (2011): Staatstrojaner horcht mehr aus, als er darf. In: http://www.20min.ch/digital/webpage/story/23172159 (28.05.2013, 57 Kommentare).

(miw) / Schweizerische Depeschenagentur AG (2011): «Trojaner passen nicht zu einem Rechtsstaat». In: http://www.tagesanzeiger.ch/schweiz/standard/Trojaner-passen-nicht-zu-einem-Rechtsstaat/story/12528641 (24.05.2013, 118 Kommentare).

Fontana, Katharina (2013): Enge Grenzen für Staatstrojaner. In: http://www.nzz.ch/aktuell/schweiz/enge-grenzen-fuer-staatstrojaner-1.18029342 (24.05.2013, 3 Kommentare).

Kohler, Franziska (2013): Bundesrat will Staatstrojaner. In: http://www.tagesanzeiger.ch/schweiz/standard/Bundesrat-will-Staatstrojaner/story/11013344 (24.05.2013, 33 Kommentare).

Mäder, Lukas (2008): Der Staat will beim Bürger mitsurfen. In: http://www.20min.ch/schweiz/dossier/session/story/24422403 (28.05.2013, 127 Kommentare).

Mäder, Lukas (2010): Polizei soll Computer online ausspionieren. In: http://www.20min.ch/schweiz/news/story/16299326 (21.05.2013, 188 Kommentare).

Mäder, Lukas (2011a): Schweiz tauscht Know-how über Trojaner aus. In: http://www.20min.ch/schweiz/news/story/21365510 (26.05.2013, 17 Kommentare).

Mäder, Lukas (2011b): Bund nutzte Trojaner bei Terror-Verdacht. In: http://www.20min.ch/schweiz/news/story/24671074 (25.05.2013, 125 Kommentare).

Mäder, Lukas (2011c): Zürich hörte Drogendealer mit Trojaner ab. In: http://www.20min.ch/schweiz/news/story/14327156 (24.05.2013, 53 Kommentare).

Mäder, Lukas/Schurter, Daniel (2011): Bundestrojaner schnüffeln auch in der Schweiz. In: http://www.20min.ch/schweiz/news/story/21511920 (27.05.2013, 106 Kommentare).

Pfister, Jessica/Schweizerische Depeschenagentur AG (2011): «Unbescholtene Bürger spioniert niemand aus». In: http://www.20min.ch/schweiz/news/story/30063545 (20.05.2013, 327 Kommentare).

Reber, Samuel (2011): Bundesrat will Staatstrojaner teilweise erlauben. In: http://www.tagesanzeiger.ch/schweiz/standard/Bundesrat-will-Staatstrojaner-teilweise-erlauben/story/20323870 (26.05.2013, 32 Kommentare).

Schurter, Daniel (2011): «Bundestrojaner» in die Schweiz verkauft. In: http://www.20min.ch/digital/webpage/story/10042785 (28.05.2013, 72 Kommentare).

Schurter, Daniel (2013a): «Kunden müssen Straftäter subventionieren». In: http://www.20min.ch/finance/news/story/-Kunden-muessen-Straftaeter-subventionieren--18213422 (18.05.2013, 53 Kommentare).

Schurter, Daniel (2013b): Wird die Schweiz zum Big-Brother-Land? In: http://www.20min.ch/digital/news/story/28995769 (18.05.2013, 221 Kommentare).

Schurter, Daniel/Schweizerische Depeschenagentur AG (2011): Piraten laufen mit Anzeige auf Grund. In: http://www.20min.ch/digital/webpage/story/25846672 (24.05.2013, 17 Kommentare).

Schweizerische Depeschenagentur AG (2013): Mithören erlaubt – mitschauen nicht. In: http://www.20min.ch/digital/news/story/12199462 (19.05.2013, 99 Kommentare).

Lauterkeitserklärung

Universität Zürich[UZH]

IPMZ – Institut für Publizistik-wissenschaft und Medienforschung

Universität Zürich
Andreasstrasse 15
CH-8050 Zürich
Telefon +41 44 634 46 61
Telefax +41 44 634 49 34
www.ipmz.uzh.ch

Wissenschaftliche Arbeiten am IPMZ – Institut für Publizistik-wissenschaft und Medienforschung der Universität Zürich

Erklärung (am Bildschirm ausfüllen und dann drucken)

Ich erkläre ausdrücklich, dass es sich bei der eingereichten schriftlichen Arbeit mit dem Titel:

Die Überwachung gesellschaftlicher Kommunikation in der Schweiz durch staatliche Behörden

um eine von mir selbst und ohne unerlaubte Beihilfe *in eigenen Worten* verfasste Originalarbeit handelt.

Ich bestätige, dass die Arbeit weder bereits einmal zur Abgeltung anderer Studienleistungen an der Universität eigereicht worden ist, noch inskünftig durch mein Zutun als Abgeltung einer weiteren Studienleistung eingereicht werden wird.

Verwendung von Quellen

Ich erkläre weiter, dass ich sämtliche Bezüge auf fremde Quellen, welche in der obengenannten Arbeit enthalten sind, deutlich als solche gekennzeichnet habe.

Ich bestätige insbesondere, dass ich ausnahmslos sowohl bei wörtlich übernommenen Aussagen (= Zitaten), als auch bei in eigenen Worten wiedergegebenen Aussagen anderer Autorinnen und Autoren (= Paraphrasen) die Urheberschaft angegeben habe.

Ich nehme zur Kenntnis, dass Arbeiten, die diese Bestimmungen missachten - insbesondere indem sie fremde Textteile ohne entsprechenden Herkunftsnachweis enthalten – als Plagiate betrachtet werden können, welche mit den entsprechenden rechtlichen und disziplinarischen Konsequenzen verfolgt und geahndet werden können (Disziplinarordnung der Universität vom 20. November 2009, § 7 ff.).

Ich bestätige mit meiner Unterschrift die Einhaltung all dieser Angaben.

Name: Bänziger Vorname: Michael

Matrikelnummer: 11-717-980

Datum: 26. Juni 2013 Unterschrift: