ZIK

Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich

Rolf H. Weber / Florent Thouvenin (Hrsg.)

Neuer Regulierungsschub im Datenschutzrecht?

Schulthess §

54

Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich

Rolf H. Weber / Florent Thouvenin (Hrsg.)

Neuer Regulierungsschub im Datenschutzrecht?

Schulthess § 2012

54

Das 1998 geschaffene «Zentrum für Informations- und Kommunikationsrecht» an der Rechtswissenschaftlichen Fakultät der Universität Zürich (Lehrstuhl Prof. Dr. Rolf H. Weber, Rämistrasse 74/38, 8001 Zürich) dient als Forschungsstelle sowie als Anlauf- und Kontaktstelle für an diesem Rechtsgebiet interessierte Personen und Gruppen.

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7255-6692-1

www.schulthess.com

Vorwort

Das Zentrum für Informations- und Kommunikationsrecht der Universität Zürich, die Forschungsstelle für Informationsrecht der Universität St. Gallen sowie das Schweizer Forum für Kommunikationsrecht (SF•FS) haben am 28. Juni 2012 in Zürich eine Veranstaltung zum Thema «Neuer Regulierungsschub im Datenschutzrecht?» durchgeführt. Aufgrund des regen Interesses an der Tagung und den vielfältigen und interessanten Diskussionen zu den vorgestellten Themen freuen sich die Vertreter der Veranstalter, die besprochene Thematik im Rahmen eines Sammelbandes zu vertiefen und der allgemeinen Öffentlichkeit zugänglich zu machen.

Einerseits werden im vorliegenden Werk die anlässlich der Veranstaltung vorgestellten Fragestellungen vertieft besprochen. Darüber hinaus finden sich darin auch zwei weitere, auf Vorträgen an der Universität Zürich beruhende, Abhandlungen, welche sich einerseits mit den Sonderfragen zu den sich zunehmender Beliebtheit erfreuenden sozialen Netzwerke beschäftigen und andererseits einen Blick über den Atlantik werfen und die entsprechenden Entwicklungen in den USA analysieren. Ziel des vorliegenden Bandes ist, die sich abzeichnenden, aber auch die aufgrund des technischen Fortschrittes und der veränderten Verhaltensweisen als notwendig erscheinenden Entwicklungen möglichst ganzheitlich darzustellen und dadurch einen Beitrag zur Lösung der in den betroffenen Rechtsgebieten – vorab im Datenschutzrecht – anfallenden Probleme zu leisten.

Die Herausgeber möchten sich an erster Stelle bei den Autoren und der Autorin für deren gehaltvolle Arbeit bedanken, welche diese trotz vielseitiger weiterer Verpflichtungen für dieses Werk geleistet haben. Des Weiteren danken sie Herrn lic. iur. Christoph Wolf für die Mithilfe bei der Zusammenstellung des Bandes.

Zürich, im August 2012

Rolf H. Weber
Florent Thouvenin

Inhaltsverzeichnis

Lic. iur. Nicole Beranek Zanon, Exec. MBA HSG[1]

Datenaufbewahrungspflichten vs. Datenlöschungspflichten Kollision von BÜPF und DSG?

«Es ist möglich, fast ohne Erinnerung zu leben, ja glücklich zu leben, wie das Tier zeigt; es ist aber ganz und gar unmöglich, ohne Vergessen überhaupt zu leben.»

Friedrich Nietzsche, Werke I – Unzeitgemäße Betrachtungen

Inhaltsverzeichnis

[1] Rechtsanwältin & Partnerin bei de la cruz beranek Rechtsanwälte AG

I. Ausgangslage

1. Untersuchungsgegenstand

Bereits 1988 hat der Bundesrat in seiner Botschaft zum Datenschutzgesetz festgehalten, dass der Einsatz der modernen Informations- und Kommunikationstechnologien in fast allen Lebensbereichen und die enorme Intensivierung der Datenverarbeitung und -verbreitung in Gesellschaft, Wirtschaft und Staat die Risiken von Persönlichkeitsverletzungen stark anwachsen lässt.[2] Diese Aussage gilt auch heute noch.

Die Sammlung von Daten über Nutzer ergibt sich aus dem täglichen Gebrauch der Kommunikationsmittel – dem (mobilen) Telefon und dem Computer. Wenn wir telefonieren, weiss der Fernmeldedienstanbieter, mit welcher Kommunikationsadresse (z.B. Mobilenummer), wie lange und von welchem, mehr oder weniger präzis beschriebenen Bereich aus wir telefonieren. Surfen wir im Internet, hinterlässt unser Computer auf Webseiten Spuren, die auf Servern aufgezeichnet werden oder kommuniziert mit diesen. Diese Daten werden durch Webseitenbetreiber, Online-Marketing-Firmen und Social-Media-Plattformen[3] durch die auf den

[2] Vgl. BBl 1988 II 413.

[3] So Facebook, vgl. Graeme McMillan, Facebook Cookies Work Even If You Are Logged Out (for Your Own Good), abrufbar unter http://techland.time.com/2011/09/26/facebook-cookies-work-even-if-youre-logged-out-for-your-own-good/(Stand 21.10.2012).

Computer hinterlegten Cookies[4] mit den Daten anderer Besuche eines Benutzers korreliert und für Behavioral Targeting[5] verwendet.

Das Risiko von Persönlichkeitsverletzungen hat mit dem Data Warehousing, Data Mining, der Consumerization und dem Internet of Things zudem weiter zugenommen. Die Consumerization, also die Einführung neuer Technologien bei Privaten, bevor eine geschäftliche Nutzung erfolgt und das Internet of Things d.h. die informationstechnologische Vernetzung aller Dinge und deren Anschluss ans Internet führt dazu, dass jeder jederzeit und von überall Zugriff auf Daten und Dinge haben kann und auch etliche Datenspuren (ob nützlich oder nicht) hinterlässt.

Im Rahmen dieses Beitrags stellt sich die Frage, ob die Konzeption des Datenschutzgesetzes mit derjenigen des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehr kollidiert bzw. wo sich allfällige Problemfelder auftun können, insbesondere auch in Hinblick auf die Korrelation von Daten über Nutzer. Dies führt dann zur Frage, ob nicht ein veränderter Schutz der Privatsphäre, mithin des Datenschutzes, angebracht wäre.[6] Im Nachfolgenden soll aufgrund der geltenden Rechtsordnung wie auch de lege ferenda diese Frage erörtert werden.

2. Konzeption des Datenschutzrechts

Der Schutz der Personendaten ist in der Schweiz in Hinblick auf Telekommunikationsmedien durch die Bundesverfassung,[7] das Persönlichkeitsrecht[8], das

4 Cookies sind Textdateien auf dem Computer des Benutzers. Sie werden eingesetzt beim Besuch von Webseiten zur Unterstützung der Kommunikation zwischen Browser und Server. Wenn der Browser beim Surfen im Internet abhängig von den Einstellungen ein Cookie bei Sessionende nicht löscht, kann der Server einen Benutzer über mehrere Besuche hinweg erkennen und Benutzerprofile erstellen.

5 Unter Behavioral Targeting versteht man Marketing-Kampagnen, die auf gezielte Nutzer angepasst sind, die vorab durch deren Surfverhalten identifiziert worden sind.

6 Dabei wird das Thema Datenschutz und Überwachung vorderhand von Soziologen und Politikwissenschaftlern diskutiert. Siehe z.B. Gregor Wiedemann, Regieren mit Datenschutz und Überwachung, 2011; oder auch das erst im November 2012 erscheinende Werk aus IT-Sicherheitsperspektive von Sandro Gaycken, Jenseits von 1984: Datenschutz und Überwachung in der fortgeschrittenen Informationsgesellschaft. Eine Versachlichung, Bielefeld 2012.

7 Art. 13 Abs. 2 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV, SR 101).

8 Art. 28 ff. des Schweizerischen Zivilgesetzbuches vom 10. Dezember 1907 (ZGB, SR 210).

Fernmelderecht[9] und durch das Datenschutzgesetz[10] geregelt. Hinsichtlich dieser Grundrechtskonzeption und deren Instrumente kann gänzlich auf den Beitrag von Prof. Dr. Rolf H. Weber in diesem Tagungsband verwiesen werden.[11]

Der Datenschutz bzw. seine Grundrechtskonzeption soll verhindern, dass wir alle zu gläsernen Menschen werden. Mit Data Warehousing d.h. dem Anlegen einer betrieblichen Datenbank, in welcher heterogene Daten aus unterschiedlichen Quellen zusammengefasst und korreliert werden, kann es sein, dass wir für einzelne Unternehmen bereits heute gläserne Menschen sind. Zwar werden die meisten Data Warehouses für firmeninterne Prozesse wie z.B. das Controlling, die Steuerung, den Verkauf und das Supply Chain Planning bereitgestellt, doch können Datenprofile über Kunden heutzutage auch vermarktet werden.[12] Nicht immer dürfte dies datenschutzkonform erfolgen.

Es genügen nämlich bereits einige wenige Angaben über uns und wir sind gläsern. Der Datenschutz soll uns helfen, vergessen zu können, was wir einmal gedacht haben, gefühlt haben oder gewesen sind.[13] Vergessen und verzeihen sind menschliche Eigenschaften, die uns von anderen Lebewesen ja gerade unterscheiden.[14]

3. Konzeption des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs

Anders sieht das Thema des Vergessens und Verzeihens im Rahmen der Strafverfolgung aus. Solange noch keine Verfolgungsverjährung eingetreten ist, besteht ein gesellschaftliches und auch privates Interesse eines Geschädigten oder seiner Nachkommen an der Aufklärung einer Straftat. Mit der Abtretung der Sühne an den Staat überwiegt im Augenblick der Strafverfolgung das öffentliche Interesse an der Aufklärung der Straftat über das Interesse des Verdächtigten am Schutz seiner Privatsphäre. Nach Ablauf der Verfolgungsverjährung sowie nach vollzogener Strafe greift auch hier das Konzept des Vergessens. Von diesem Konzept gibt es zwar Ausnahmen, nämlich z.B. im Zusammenhang mit den Persönlichkeitsrechts-

9 Fernmeldegesetz vom 30. April 1997 (FMG, SR 781.10).

10 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (Datenschutzgesetz, DSG, SR 235.1).

11 Rolf H. Weber, Neue Grundrechtskonzeptionen zum Schutz der Privatheit, Ziff. II, S. 11.

12 Zur Frage, ob bereits ein betriebsinternes CRM eine Datensammlung nach DSG ist bzw. es sich um Persönlichkeitsprofile handelt, siehe Alex Schweizer, Customer Relationship Management, Datenschutz- und Privatrechtsverletzungen beim CRM, Zürich 2006.

13 Vgl., wie verheerend das Nichtvergessen sein kann: Miriam Meckel, Next – Erinnerungen an eine Zukunft ohne uns, Hamburg 2011.

14 Joël Luc Cachelin, Vergessen – Ein Gedankenprotokoll am Rande der Digitalität, St. Gallen 2012.

verletzungen von Verurteilten[15] oder bei registerrechtlich öffentlichen, zeitlich unbeschränkten Daten wie diejenigen des Handelsregisters[16].

Auf den Fundus der bei der Telekommunikation anfallenden Daten und Informationen über uns möchten die Strafverfolgungsbehörden im Rahmen von Strafuntersuchungen bei schweren[17] Delikten zurückgreifen können. Der Eingriff in die Privatsphäre bzw. ins Fernmeldegeheimnis[18] – beides verfassungsrechtliche Grundrechte – bedarf deshalb einer formellen gesetzlichen Grundlage, er muss dem Verhältnismässigkeitsprinzip entsprechen und im öffentlichen Interesse liegen.[19] Entsprechend wurde das Bundesgesetz vom 6. Oktober 2000 (BÜPF)[20] betreffend die Überwachung des Post- und Fernmeldeverkehrs und dessen Ausführungsverordnung, die Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)[21] erlassen. Später kam die eidgenössische Strafprozessordnung[22] hinzu.

4. Divergierende Konzeptionen?

Der Gesetzgeber hat diese Kollision geregelt, denn von ihren Konzeptionen her kollidieren das Datenschutzgesetz sowie das BÜPF. Sie haben in grundsätzlicher Weise ein anderes Schutzobjekt: Das Datenschutzgesetz den Schutz von Personendaten und das BÜPF die Überwachung des Post- und Fernmeldeverkehrs und damit in einem Teilgehalt der persönlichen Freiheit, dem Fernmeldegeheimnis.

---

15 So wie im vom deutschen Bundesverfassungsgerichtshof entschiedenen Fall Lebach II (BVerfG, 1 BvR 348/98 vom 25. November 1999), wonach nicht der Zeitablauf massgebend ist für ein Recht auf Vergessen für eine verurteilte Person, sondern in welchem Mass eine Berichterstattung die Persönlichkeitsentfaltung beeinträchtigen kann.

16 Gemäss Bundesverwaltungsgericht dürfen öffentliche Registerdaten von Dritten verwendet und publiziert werden, wenn diese Gesuche um Löschung der Publikationsdaten sofort beantworten (Entscheid des Bundesverwaltungsgerichts vom 26. Februar 2008 (BVGE 2008/16) i.S. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter gegen itonex AG, die Betreiberin von Moneyhouse. Im August 2012 hat das Bundesverwaltungsgericht erneut über den Fall im Rahmen einer Zwischenverfügung entschieden. Die Begründung des Entscheides war im Zeitpunkt des Redaktionsschlusses dieses Beitrages noch nicht öffentlich zugänglich.

17 Es ist dabei nicht nachvollziehbar, weshalb gewisse Delikte für die Überwachung zugänglich sind und andere nicht. Zumindest handelt es sich heute nicht mehr nur um schwere Delikte. Die Grenzen werden somit aufgeweicht.

18 Art. 13 Abs. 1 BV.

19 Art. 36 BV.

20 SR 780.1.

21 SR 780.11.

22 Strafprozessordnung vom 5. Oktober 2007 (StPO, SR 312.0).

Gemäss Art. 2 Abs. 2 lit. c DSG ist denn auch das Datenschutzgesetz nicht anwendbar auf Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren. Es stellt sich damit die Frage, ob sämtliche Überwachungsmassnahmen unter das Strafverfahren fallen oder ob Lücken bestehen.

Das BÜPF und die VÜPF regeln die Echtzeitüberwachung, die rückwirkende Überwachung[23] des Fernmeldeverkehrs (Art. 16, 24a, 24b VÜPF) sowie Auskünfte über Teilnehmerinnen (Art. 19 und 27 BÜPF) für die Zwecke der Strafverfolgung. Die Überwachungsmassnahmen für die Echtzeitüberwachung greifen zum einen nur bei Vorliegen eines Deliktes aus dem abgeschlossenen Deliktskatalog[24] und sind zum anderen subsidiär anwendbar, d.h., wenn bisherige Untersuchungshandlungen erfolglos geblieben sind oder die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden. Für die rückwirkende Überwachung genügt heute bereits ein Verdacht auf ein Verbrechen oder ein Vergehen oder eine Übertretung (Art. 179^{septies} StGB, Art. 273 i.V.m. Art. 269 StPO).

Bei der rückwirkenden Überwachung werden die Fernmeldedienstanbieter verpflichtet, Daten auf Vorrat anlasslos zu speichern. Zumindest die anlasslose Speicherung fällt unter keines der in Art. 2 Abs. 2 lit. c DSG erwähnten Verfahren. Ursprünglich wurde der Ausschluss gemäss Art. 2 Abs. 2 lit. c DSG aufgenommen, weil der Gesetzgeber fürchtete, dass sich die Strafprozessordnung und das Datenschutzgesetz mit zum Teil gleicher Zielrichtung überlagern könnten und sich damit Rechtsunsicherheiten, Koordinationsprobleme und schliesslich Verfahrensverzögerungen ergeben könnten.[25] Die rückwirkende Überwachung ist für den Teilbereich der anlasslosen Datenspeicherung durch die Fernmeldedienstanbieter aber gerade keine dem Strafverfahren per se zuordenbare Tätigkeit. Sie wird es erst bei der Abfrage von gespeicherten Daten durch die Strafverfolgungsbehörden.

Grundsätzlich obliegt es dem Staat, zu definieren, wann die öffentlichen Interessen an der Strafverfolgung gegenüber den Interessen des Privaten überwiegen, mithin wo die Grenzen der Möglichkeiten für die Strafverfolgung liegen sollen. Der Staat bzw. das Parlament ist bei dieser Grenzziehung und politischen Gewich-

---

23 In Deutschland spricht man von Vorratsdatenspeicherung statt von der rückwirkenden Überwachung. Der Begriff der Vorratsdatenspeicherung ist zwar eingängig, jedoch nicht korrekt, weil er nur das anlasslose Speichern von Daten erfasst, nicht auch die Handlung der Datenabfrage der Staatsanwaltschaft bzw. des Dienstes ÜPF beim Fernmeldedienstanbieter betreffend Herausgabe der gespeicherten Daten. Vorliegend wird deshalb die schweizerische Terminologie der rückwirkenden Überwachung verwendet.

24 Art. 1 Abs. 1 lit. a BÜPF i.V.m. Art. 269 Abs. 1 und 2 StPO.

25 BBl 1988 II 443.

tung an die verfassungsrechtlichen Grundsätze gebunden. Dabei hat der Gesetzgeber ein denkbar komplexes Gebilde gewählt.

Zum einen ist in der Strafprozessordung im Grundsatz geregelt, wann ein Zugriff auf Daten erfolgen kann und wie die Sicherheit der Daten und damit der Datenschutz für die Behörden aussieht (siehe dazu Ziff. II.2). Zum anderen ist im Fernmeldegesetz der Grundsatz des Fernmeldegeheimnisses und der Umgang mit Daten durch die Fernmeldedienstanbieter detailliert beschrieben (siehe dazu Ziff. II.3). Im Weiteren regelt sodann das BÜPF die Sicherheit der Daten, die Anbieterinnen an die Ausrüstungen des Dienstes ÜPF ausliefern müssen (siehe dazu Ziff. II.4).

II. Rechtlicher Rahmen

1. Erfordernis der gesetzlichen Grundlage

Aufgrund der Schwere des Eingriffs in die Grundrechte, in den Schutz der Privatsphäre i.S. von Art. 13 Abs. 2 BV und – davon abgeleitet – in das Fernmeldegeheimnis gemäss Art. 43 FMG[26] bedarf es einer gesetzlichen Regelung der Überwachung des Post- und Fernmeldeverkehrs. Für die allgemeine Grundrechtskonzeption des Datenschutzes kann hierzu auf den Beitrag von Prof. Dr. Rolf H. Weber in diesem Tagungsband verwiesen werden. Die weitergehenden Rechtsgrundlagen, namentlich in der StPO,[27] dem FMG[28] und dem BÜPF,[29] werden nachfolgend aufgeführt.

2. Überwachung in der Strafprozessordnung

a) Überwachung des Fernmeldeverkehrs

Die Schweizerische Strafprozessordnung regelt die Überwachung des Post- und Fernmeldeverkehrs in den Art. 269–279 StPO. Zur Überwachung des Fernmeldeverkehrs müssen drei Voraussetzungen kumulativ erfüllt sein: i) es muss ein dringender Tatverdacht bestehen, eine in Art. 269 Abs. 2 StPO genannte Straftat sei

[26] Vom 30. April 1997 (SR 784.10).
[27] Vgl. FN 24.
[28] Sowie der Verordnung vom 9. März 2007 über Fernmeldedienste (FDV, SR 784.11).
[29] Und seiner Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780.11).

begangen worden, ii) die Schwere der Straftat muss die Überwachung rechtfertigen und iii) die bisherigen Untersuchungshandlungen müssen erfolglos geblieben sein, bzw. es muss belegt werden, dass die Ermittlungen ansonsten aussichtslos wären oder unverhältnismässig erschwert würden (Art. 269 Abs. 1 lit. b–c StPO). Neben der eigentlichen geheimen inhaltlichen Überwachung kann die Staatsanwaltschaft auch Auskünfte betreffend Verkehrs- und Rechnungsdaten bzw. Teilnehmeridentifikation (Art. 273 StPO) verlangen. Die Überwachung und die Auskünfte über Verkehrs- und Rechnungsdaten sowie Teilnehmeridentifikation bedürfen der Genehmigung durch das Zwangsmassnahmegericht (Art. 272 Abs. 1 i.V.m. Art. 270 StPO). Davon ausgenommen sind einfache Anfragen gemäss Art. 14 BÜPF. Für diese ist keine richterliche Genehmigung notwendig und eine tatbeständliche Einschränkung ist auch nicht gegeben.

Die Überwachung umfasst nicht nur die beschuldigte Person, sondern kann auch Dritte erfassen, wenn eine Drittperson den Fernmeldeanschluss (oder das Handy, den Computer, das E-Mail-Account) der beschuldigten Person benutzt oder wenn die Drittperson für die beschuldigte Person Mitteilungen entgegennimmt. Ebenso kann ein Dritter bei der Rastersuche mit Antennensuchlauf betroffen sein. Beim Antennensuchlauf werden einem Pseudonym zugeordnete Daten in einem Suchvorgang der wahren Identität zugeführt.

Daten aus nicht genehmigten Überwachungen müssen sofort vernichtet werden und dürfen nicht verwertet werden (Art. 277 StPO). Die Überwachung von Personen, die durch ein Berufs- oder Amtsgeheimnis[30] privilegiert werden, ist unter der Leitung des Gerichts vorzunehmen. Den Strafverfolgungsbehörden dürfen keine Berufsgeheimnisse zur Kenntnis gebracht werden. Informationen, für die das Zeugnisverweigerungsrecht gilt, müssen ausgesondert und sofort vernichtet werden.

b) Überwachung mit technischen Überwachungsgeräten

Die Staatsanwaltschaft kann zudem technische Überwachungsgeräte zur Überwachung von nicht öffentlichen Gesprächen in einem Raum einsetzen (Art. 280 lit. a StPO). Voraussetzung dafür ist, dass der Einsatz der technischen Überwachung nur gegenüber der beschuldigten Person angeordnet wird und überdies die zuvor unter Ziff. a) hiervor genannten Voraussetzungen erfüllt sind.

---

[30] Siehe Art. 170–173 StPO, namentlich sind dies: Beamte, Geistliche, Rechtsanwältinnen und Rechtsanwälte, Verteidigerinnen und Verteidiger, Notarinnen und Notare, Patentanwältinnen und Patentanwälte, Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte, Apothekerinnen und Apotheker, Hebammen sowie ihre Hilfspersonen, Quellen von Medienschaffenden und Personen, die einem Berufsgeheimnis unterliegen. Bei Letzteren gibt es allerdings Einschränkungen.

Nach herrschender Lehre fällt unter die Überwachung gemäss Art. 280 lit. a StPO nicht der Einsatz der sogenannten GovWare, insoweit als die GovWare mehr als nur Kommunikation zwischen zwei Teilnehmern abhören kann (siehe dazu Ziff. IV.4).

3. Datenschutz im Fernmeldegesetz

Kapitel 7 des Fernmeldegesetzes widmet sich dem Fernmeldegeheimnis und dem Datenschutz. Grundsätzlich darf, wer mit fernmeldedienstlichen Aufgaben betraut ist oder betraut war, Dritten keine Angaben über den Fernmeldeverkehr von Teilnehmerinnen und Teilnehmern machen und niemandem Gelegenheit geben, solche Angaben weiterzugeben (Art. 43 FMG).

Die Fernmeldedienstanbieterinnen müssen aber ihren Kunden Auskünfte über die für die Rechnung verwendeten Daten bereithalten können (Art. 45 FMG) und sie dürfen Standortdaten von Kundinnen und Kunden nur für die Fernmeldedienste und ihre Abrechnung bearbeiten, es sei denn, sie hätten die Einwilligung der Kunden (Art. 45b FMG). Ebenfalls mit Einwilligung ist das Bearbeiten von Daten auf fremden Geräten durch fernmeldetechnische Übertragung, sprich das Setzen eines Cookies durch die Fernmeldedienstanbieterin erlaubt (Art. 45c FMG).[31] Die Daten, die gemäss FMG bearbeitet und gespeichert werden dürfen, haben einen Zusammenhang mit der Erbringung einer Dienstleistung an Kunden und dienen dazu, die Einhaltung der vertraglichen Abmachungen nachzuweisen.

Darüber hinaus regelt der Bundesrat in der Verordnung zum Fernmeldegesetz[32] in Art. 80–88 den Umgang mit Datenschutz für Fernmeldedienstanbieter. In Art. 80 FDV wird der Grundsatz festgehalten, dass persönliche Kundendaten von den Fernmeldedienstanbietern nur so lange und so weit bearbeitet werden dürfen, als dies für den Verbindungsaufbau bzw. die Erfüllung der Pflichten gemäss BÜPF notwendig ist. Sodann regeln Art. 81–83 FDV die Fragen der Mitteilung von Daten an Kunden sowie die Möglichkeit des Umgangs mit Massenwerbung durch Fernmeldedienstanbieter. Art. 84–86 FDV enthalten Bestimmungen zur Anzeige von Rufnummern und der Anrufumleitung. Hinsichtlich Datensicherheit verpflichtet der Gesetzgeber die Fernmeldedienstanbieterinnen, ihre Kunden zu in-

---

31 Es fragt sich, ob dies nicht eine Diskriminierung der Fernmeldedienstanbieter ist, wenn nur diese keine Cookies ohne vorherige Aufklärung der Kunden und deren explizite Einwilligung anbringen dürfen. Denn ein allgemeines Cookies-Verbot besteht in der Schweiz derzeit noch nicht. Darüber hinaus ist HTTP(S) verbindungslos und es gibt deshalb auch einen für den Datenschutz unbedenklichen Einsatzbereich für Cookies (siehe z.B. das Geschäftsmodell von adwebster.com).

32 Verordnung vom 9. März 2007 über Fernmeldedienste (FDV, SR 784.101.1).

formieren und ihnen geeignete Hilfsmittel zur Beseitigung von Risiken anzubieten oder zu nennen (Art. 88 FDV). Darüber hinaus verweist die Verordnung auf das Datenschutzgesetz.

4. Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs

a) BÜPF und VÜPF

Im Rahmen der Strafverfolgung sind geheime Ermittlungsmassnahmen in der Strafverfolgung notwendig, wozu die Überwachung des Post- und Fernmeldeverkehrs gehört.[33] Der Bund hat deshalb 1998 – noch mit den 26 verschiedenen kantonalen Strafprozessordnungen – das BÜPF erlassen, welches per 1. Januar 2002 in Kraft trat. Mit der neuen StPO erfuhr es eine erste Anpassung. Derzeit ist das BÜPF in einer Totalrevision. Ein Vorentwurf wurde im Jahre 2010 in die Vernehmlassung geschickt. Es ist damit zu rechnen, dass das revidierte BÜPF im Jahre 2013 ins Parlament kommt.

Seit dem Jahre 2002 hat sich nicht nur die Technologie stark weiterentwickelt (indem auch die Korrelation von grossen Datenmengen machbar ist), auch der sachliche Anwendungsbereich des BÜPF hat sich ausgedehnt. Es geht heute nicht mehr nur um den Kampf gegen das organisierte Verbrechen wie anno 2002, sondern zunehmend auch um Internetkriminalität im Allgemeinen.[34]

Sodann ist per 1. Januar 2012 die revidierte VÜPF in Kraft getreten. Danach sollen denn künftig nicht mehr nur Mobiltelefonie und E-Mail-Verkehr, sondern auch der Internetverkehr abgehört bzw. in Echtzeit überwacht werden können.

Der beauftragte Dienst ÜPF[35] ist nach der heutigen Konzeption Ausführungsorgan der Überwachung.

b) Sachlicher und persönlicher Anwendungsbereich

Das BÜPF gilt in sachlicher Hinsicht für die Überwachung des Post- und Fernmeldeverkehrs, die im Rahmen eines Strafverfahrens des Bundes oder eines Kantons – das heisst im Rahmen der StPO, zum Vollzug eines Rechtshilfeersuchens

33 Siehe StPO, 8. Kapitel, 1. Abschnitt.
34 Wobei gerade die Internetkriminalität oft organisiert begangen wird.
35 Zuvor nannte er sich Dienst für besondere Aufgaben (DBA).

nach dem Rechtshilfegesetz vom 20. März 1981[36] oder im Rahmen der Suche und Rettung vermisster Personen angeordnet und durchgeführt wird.

Der persönliche Anwendungsbereich erstreckt sich auf alle staatlichen, konzessionierten oder meldepflichtigen Anbieterinnen von Post- und Fernmeldedienstleistungen sowie auf Internet-Anbieterinnen.[37] Während unter den Begriff der Internet-Anbieterin auch Internet-Dienste-Anbieterinnen fallen könnten, hat die geltende VÜPF nur die Internetzugangsanbieterinnen verpflichtet. Internetzugangsanbieterinnen sind Fernmeldedienstanbieterinnen oder der Teil einer Fernmeldedienstanbieterin, die der Öffentlichkeit fernmeldetechnische Übertragungen von Informationen auf der Basis der IP-Technologien unter Verwendung von IP-Adressen anbietet.[38] Damit fallen derzeit reine Dienstanbieter wie E-Commerce-Plattformen-Betreiberinnen ausser Betracht. Wer aber auch Internetzugang anbietet, muss denn auch seine Dienste überwachen können.

Ebenfalls zur Duldung einer Überwachung können Betreiberinnen von internen Fernmeldenetzen oder Hauszentralen verpflichtet werden. Dies sind Personen, die über die Beschaffung, die Erstellung und den Betrieb dieser Einrichtungen entscheiden.[39]

c) Datenschutz im Rahmen des BÜPF

Während das FMG den Grundsatz der Datensparsamkeit und der Datenlöschung, mithin das datenschutzrechtliche Verhältnismässigkeitsprinzip postuliert, werden im Rahmen des BÜPF weitere Daten erhoben bzw. länger aufbewahrt, als dies für geschäftliche Zwecke notwendig ist. Damit werden Daten erhoben, die dem ausschliesslichen Zweck der Fernmeldeüberwachung dienen.

Das Verhältnismässigkeitsprinzip ist mithin nicht im BÜPF ausdrücklich geregelt, ergibt sich aber aus Art. 13 Abs. 1 DSG. Das BÜPF enthält einzig Bestimmungen betreffend den Umfang der Daten, die zu speichern sind. Die VÜPF kann insbesondere nicht darüber hinausschiessen, ohne dass nicht eine Anpassung in der BÜPF vorzunehmen wäre.

Im Zusammenhang mit dem Umgang von Personendaten in datenschutzrechtlicher Hinsicht schweigt sich das BÜPF aus. Immerhin gibt es einige wenige Normen zum Datenschutz in Art. 7–9 VÜPF, welche subsidiär gelten könnten, wäre

---

36 Bundesgesetz vom 20. März 1981 über internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz, IRSG, SR 351.1).

37 Art. 1 BÜPF.

38 Anhang zum VÜPF, Ziff. 1.

39 Anhang zum VÜPF, Ziff. 2.

die Anwendung des DSG nicht ausgeschlossen. Art. 7 VÜPF enthält die Legitimation der Personendatenbearbeitung für den Zweck der Kontrolle der Überwachung für die anordnenden Behörden[40] und Art. 8 VÜPF für den Dienst zum Betrieb eines Verarbeitungszentrums. Bemerkenswert ist auch, dass hinsichtlich Datensicherheit in Art. 9 VÜPF auf die Verordnung des Bundesgesetzes über den Datenschutz[41] und die Bestimmungen zur IKT-Sicherheit in der Bundesinformatikverordnung vom 26. September 2003 (BinfV)[42] verwiesen wird. Art. 8 und 9 der BinfV müssen deshalb sinngemäss auf die Richtlinien für die Fernmeldedienstanbieter übertragen werden. Damit gilt auch der Leitfaden des EDÖB zu den technischen und organisatorischen Massnahmen des Datenschutzes.[43] Die BinfV hält zudem ausdrücklich für Bundesorgane in deren Art. 6 fest, dass der Einsatz der Informations- und Kommunikationstechnik den Datenschutz der betroffenen Personen gewährleisten muss.

Dagegen sind die Anbieterinnen von Post- oder Fernmeldediensten bis zum Übergabepunkt der Daten an den Dienst für die Datensicherheit verantwortlich und unterliegen diesbezüglich den Weisungen des Dienstes ÜPF.[44] Dies beinhaltet Sicherheitsaspekte der Auslieferung der Daten und deren Integrität.

Da die Daten im Rahmen einer verdeckten Ermittlung gewonnen werden, dürfte die Klassifizierung der Daten für deren Übermittlung als geheime, besonders schützenswerte Personendaten erfolgen. Eine Übermittlung muss folglich verschlüsselt, geschützt und protokolliert werden. Dies erfolgt heute für den Content of Communication nicht.

III. Daten nach BÜPF und VÜPF

1. Überwachte Daten

Nachfolgend sei aufgezeigt, welche Daten beim Fernmeldeverkehr aufgrund des BÜPF aufzuzeichnen sind. Es ist hier festzuhalten, dass nicht alle Daten der

---

40 Während eine Kontrolle durch die Fernmeldedienstanbieter, wie dies Art. 7 VÜPF ebenfalls erwähnt, aufgrund des Prozesses der Überwachung gar nicht stattfindet. Sehr wohl aber eine Personendatenbearbeitung insbesondere in Hinblick auf die Herausgabe von IP-Adressen.

41 Verordnung vom 9. Dezember 2011 über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV), SR 235.11.

42 BinfV, SR 172.010.58.

43 Abrufbar unter http://www.edoeb.admin.ch/dokumentation/00445/00472/00935/index.html?lang=de (Stand 20.9.2012).

44 Art. 9 Abs. 2 VÜPF.

Telekommunikation auch Personendaten im Sinne von Art. 3 lit. a DSG sind. Allerdings soll ja der Zugriff der Daten gerade die Identifikation von Personen ermöglichen, weshalb die nachfolgenden Daten auch als Personendaten zu qualifizieren sind. Eine detaillierte Untersuchung dieses Themas sprengt allerdings den Rahmen dieses Beitrages.

2. Verkehrs- und Rechnungsdaten/ Interception Related Information

a) Begriffe

Gemäss Art. 15 BÜPF i.V.m. Art. 273 StPO sind die Anbieter von Fernmeldediensten verpflichtet, Verkehrs- und Rechnungsdaten sowie die zur Überwachung notwendigen Informationen dem Dienst ÜPF zuzuleiten. Verkehrs- und Rechnungsdaten sind die Informationen, die von der Anbieterin über den Post- oder Fernmeldeverkehr von Teilnehmerinnen und Teilnehmern aufgezeichnet werden, um die Tatsache der Postsendung oder der Kommunikation und die Rechnungsstellung zu belegen (Anhang 2 Ziff. 7 VÜPF).

Verkehrsdaten sind Informationen, die von einer Anbieterin zu geschäftlichen Zwecken gehalten werden. Welches die geschäftlichen Zwecke sind, muss dem Dienstangebot und dem Vertrag mit dem Kunden entnommen werden. Wenn eine verbrauchsabhängige Verrechnung vereinbart wurde, müssen einzelne Verbindungen nachgewiesen werden. Wenn eine Flat Rate vereinbart wurde, ist dies aus Gründen der Rechnungsstellung nicht der Fall; es stellt sich dann die Frage, ob eine Anbieterin wegen andern vertraglichen Vereinbarungen (z.B. Quality of Service) Verbindungsnachweise erbringen muss. Verkehrsdaten werden für die rückwirkende Überwachung erhoben.

Rechnungsdaten sind dagegen gemäss Art. 81 Abs. 1 FDV einerseits die vollständigen Adressierungselemente[45] der angerufenen Anschlüsse oder die Rufnummern der anrufenden Anschlüsse ohne die letzten vier Ziffern und andererseits das Datum, die Zeit und die Dauer der Verbindung.

Randdaten als Begriff wird im BÜPF/VÜPF nicht definiert, wird aber im Zusammenhang mit der Echtzeitüberwachung verwendet. Die Randdaten sind die Inter-

[45] «Adressierungselemente der angerufenen Anschlüsse» gemäss Art. 81 Abs. 1 FDV sind eine Untermenge der «Adressierungselemente» gemäss Art. 3 lit. f und g (siehe nachfolgend Ziff. d) des FMG. «Adressierungselemente der angerufenen Anschlüsse» sind Netzadressen, wie z.B. eine Telefonnummer im E.164-Format.

cept Related Information (IRI[46]). Damit sind die Randdaten ein Oberbegriff für alle Daten, die mit der Verkehrssteuerung verbunden sind (im Gegensatz zum Inhalt der Kommunikation, dem Content of Communication, CC oder auch Nutzinformation).

Verbindungsdaten sind eine Untermenge der Randdaten, die der Signalisierung entnommen werden, ebenso wie die Verkehrsranddaten, welche die Header-Information einer E-Mail bezeichnen.

Die Begrifflichkeiten basieren teilweise auf ETSI-Standards und teilweise wird davon abgewichen. Dies führt zu einem Begriff-Wirrwarr. Erst die «organisatorischen und administrativen Anforderungen» und die «technischen Anforderungen für die Überwachung des Fernmeldeverkehrs» geben Aufschluss darüber, welche Daten dies im Detail betrifft, weil eine eigene Definition aufgeführt wird oder ein ETSI-Verweis vorgenommen wird.[47]

b) Adressierungselemente (Art. 16 lit. c VÜPF)

Im Rahmen einer Überwachung (Echtzeit und rückwirkend) müssen die Adressierungselemente[48] gemäss Art. 3 lit. f FMG bekannt gegeben werden.[49] Adressierungselemente sind Nummerierungselemente wie Kennzahlen, Rufnummern und Kurznummern (Telefonnummern) und Kommunikationsparameter. Letztere sind Elemente zur Identifikation von Personen, Computerprozessen, Maschinen, Geräten oder Fernmeldeanlagen, die an einem fernmeldetechnischen Kommunikationsvorgang beteiligt sind. Darunter fallen IMSI-Nummern[50],

46 Gem. ETSI TS 101 671 V2.15.1 (2006-11), Art. 3 ist IRI: collection of information or data associated with telecommunication services involving the target identity, specifically communication associated information or data (including unsuccessful communication attempts), service associated information or data (e.g. service profile management by subscriber) and location information.

47 Organisational and Administrative Requirements (OAR) v2.13, Technical Requirements for Telecommunication Surveillance (TR TS) v3.0, beide abrufbar unter https://www.li.admin.ch/de/documentation/downloads/trts_oar.html (Stand 20.9.2012).

48 Im FMG wird ein veritables Definitionschaos angerichtet, da im Widerspruch zu ITU-T behauptet wird, z.B. IMEI wäre als Kommunikationsparameter (ist eigentlich ein eindeutiger Device Identifier) ein «Adressierungselement».

49 Art. 14 Abs. 1 lit. b BÜPF i.V.m. Art. 16 lit. c Ziff. 1 VÜPF und rückwirkend Art. 16 lit. d Ziff. 1 VÜPF.

50 International Mobile Subscriber Identity.

IMEI-Nummern[51], IP-Adressen[52], MAC-Adressen[53] und Domain-Namen (und damit auch E-Mail).

E-Mail ist die häufigste genutzte Anwendung im Rahmen des Internets. Eine E-Mail besteht aus einem Header (Kopf) und einem Body (Inhalt). Der Header, die Kopfzeile, beinhalten in seiner vollen Version (full Header) den Weg, den eine E-Mail genommen hat, sowie den Absender, den Empfänger, das Datum der Erstellung und das Format des Inhaltes. Normalerweise sieht der Benutzer nur den komprimierten Header. Die Header-Informationen sind die Verkehrsranddaten[54], der Body Inhalt der E-Mail, die Nutzinformation.

Ebenfalls bekannt zu geben ist nebst der Rufnummer des Verdächtigen die Zielnummer und allenfalls dazwischengeschaltete Nummern. Hinzu kommen die erzeugten Signale, einschliesslich der Signalisierung für den Bereitschaftszustand, die Parameter der Fernmeldeanlagen (z.B. IMEI-Nummer) und die erzeugten Signale für die Aktivierung der Konferenzschaltung oder der Anrufumleitung.

c) Bei Mobiltelefonie

Bei der Mobiltelefonie soll die Bestimmung und die simultane oder periodische Übertragung des Zell-Identifikators (Cell ID), des Standortes und der Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person verbunden ist, in Echtzeit-Überwachung abgefragt werden. Dies gilt unabhängig davon, ob es zu einem Verbindungsaufbau einer Kommunikation gekommen ist oder nicht.[55] Ein in regelmässigen Intervallen durchgeführter Location Update bei keinem Verbindungsaufbau führt zu einer erheblichen Mehrbelastung der Telekommunikationsnetze.

---

51 International Mobile Equipment Identity.

52 Gemäss Anhang der Verordnung für Adressierungselemente im Fernmeldebereich vom 6. Oktober 1997 (AEFV, SR 784.104): Internet- oder IP-Adresse (Internet Protocol Address): Numerischer Kommunikationsparameter, der die Identifikation einer insbesondere aus Netzrechnern oder -servern bestehenden Internet-Domain sowie der Benutzerrechner, die an den Verbindungen in diesem Netz beteiligt sind, ermöglicht.

53 Media-Access-Control-Adresse ist die Hardware-Adresse jedes einzelnen Gerätes, die zur eindeutigen Identifizierung des Geräts dient.

54 Der Ausdruck Verkehrsranddaten definiert Verkehrsdaten als Untermenge der Randdaten.

55 Art. 16 lit. b und lit. c Ziff. 4 VÜPF.

d) Datum und Uhrzeit

Ebenfalls notwendig sind bei der Erhebung der Daten des Fernmeldeverkehrs Datum und Uhrzeit. Bei der rückwirkenden Überwachung ist zudem noch die Dauer der Verbindung von Interesse.

3. Überwachung des Fernmeldeverkehrs/Call Content

Unter der Echtzeit-Überwachung wird das Abfangen in Echtzeit und die simultane, leicht verzögerte oder periodische Übertragung der Post- oder Fernmelderanddaten (Intercept Related Information, IRI), inklusive der Nutzinformationen (Content of Communication, CC) verstanden. Die Nutzinformationen sind dabei der Anteil des zu überwachenden Fernmeldeverkehrs, der die zwischen Benutzenden bzw. zwischen deren Endeinrichtungen ausgetauschten Informationen (z.B. Laute, Telefax, E-Mails und Daten) enthält, also das Gespräch oder der Inhalt eines E-Mails[56] und seiner Anhänge. Die rückwirkende Überwachung beschränkt sich auf die technischen Daten ohne die Nutzinformationen.[57] Die verschiedenen Überwachungsmöglichkeiten werden als Überwachungstypen beschrieben[58].

4. Teilnehmeridentifikation/Auskünfte über Fernmeldeanschlüsse

Zu den Auskünften über Fernmeldeanschlüsse gehören u.a. Namen, Adressen und Berufe der tatverdächtigen Personen und der allenfalls zu überwachenden weiteren Personen.[59] Auch Personen, die einem Berufsgeheimnis nach Art. 271 Abs. 1 StPO unterstehen, können überwacht werden. Allerdings werden deren Daten gesondert behandelt (vgl. dazu Ziff. II.2.a). Zudem werden Adressierungselemente und die Art der Anschlüsse erhoben.

5. Antennensuchlauf im Besonderen

Der Antennensuchlauf dient dem Zweck der rückwirkenden Eruierung aller an einem bestimmten Standort angefallenen mobilen Kommunikationsvorgänge

[56] Die Bodyinformationen eines E-Mails.
[57] Art. 16 lit. d VÜPF.
[58] Siehe Art. 16 VÜPF.
[59] Art. 14 BÜPF.

während eines bestimmten Zeitraumes, sofern es zum Aufbau einer Kommunikation gekommen ist.

Das Bundesgericht hatte in einem Fall betreffend eine rückwirkende Überwachung von Mobilfunk-Verkehrsdaten über Antennensuchlauf[60] zu untersuchen, ob diese nicht ausdrücklich im BÜPF geregelte Erhebung von Verkehrsdaten per Rasterfahndung noch unter der noch bis 31. Dezember 2011 gültigen VÜPF zulässig ist. Nebst den noch nicht bekannten Verdächtigten werden dabei etliche Daten von unbeteiligten Personen erfasst. Bei Antennensuchläufen im Rahmen von Rasterfahndungen gegen noch eine unbekannte Täterschaft werden Telefonieverkehrsdaten von zunächst noch unbestimmt vielen Teilnehmern erfasst und vorerst pseudonymisiert miteinander abgeglichen, um aus Verkehrsdaten verschiedener Tatorte oder Tatzeiten die Schnittmenge von konkret Verdächtigen zu ermitteln. Das Bundesgericht erachtete ein solches Vorgehen als zulässig, sofern ein dringender Verdacht eines Verbrechens vorliegt, die gesuchte Täterschaft grundsätzlich individualisierbar sei und dies als ultima ratio im Sinne des Subsidiaritätsprinzips eingesetzt wird. Nicht zulässig sei jedoch die Erhebung des Gesprächsinhaltes. Es müsse sich zudem auf einige wenige Verdächtige beschränken und die angepeilte verdächtige Schnittmenge der abgeglichenen Verkehrs- und Rechnungsdaten müsse klein sein.

Mit dem Entscheid des Bundesgerichts können damit nicht nur Geolokalisationsdaten[61] erhoben werden, sondern vice versa können die Geolokalisationsdaten – nämlich der Antennensuchläufe – dazu verwendet werden, Täter zu identifizieren. Entsprechend wurde dies in Art. 16 lit. e VÜPF, gültig ab 1.1.2012 aufgenommen.

6. Vermischung und Korrelation der Daten der Telekommunikation und des Internetverkehrs

Bereits heute und in Zukunft noch viel mehr vermischen sich die Daten der Telekommunikation und des Internetverkehrs. Über IP lässt sich z.B. ein SMS Ping für die Standortidentifikation machen. Dies ist heute technisch möglich. Aufgrund der fehlenden Aufzählung im BÜPF bzw. im VÜPF ist eine solche Datenabfrage mittels SMS Ping zur Standortidentifikation nur mit einer konkreten Überwachungsanordnung zulässig.

Ebenfalls denkbar wäre z.B. mit dem Internet of Things und der Vernetzung jedes Stromschalters bei einem Beschuldigten via vernetztem Stromschalter zu überwa-

[60] BGE 137 IV 340, E. 6.1 kommentiert in: Jurius, Raster-Suche nach Mobiltelefon-Nummern erlaubt, in: Jusletter 9. Januar 2012.

[61] Geolokationsdaten sind Abbildungen von Zellen auf geografische Koordinaten.

chen, wann er das Licht löscht und schlafen geht. Auch hierzu bedürfte es einer Überwachungsanordnung, deren gesetzliche Grundlage aber in der VÜPF noch fehlt, da der sogenannte Target Identifier derzeit eine Person und kein Ding ist. Relevant dürfte sein, ab welchem Layer man generell nicht mehr von Telekommunikation (und damit auch nicht von Internet) sprechen kann. Dort ist die Grenze des BÜPF.

Die geltende VÜPF hat aufgrund dieser Entwicklung und Verschmelzung m.E. zu Recht den sachlichen Anwendungsbereich auf den Internetverkehr ausgedehnt.[62] Allerdings wäre es wünschenswert, diese Ausdehnung auf Gesetzesstufe zu vollziehen.

Darüber hinaus besteht eine noch viel grössere Gefahr aus dem Fortschritt der Technik. Aufgrund der Rechenleistung, die heute zur Verfügung steht, ist eine Korrelation von Daten, d.h. das Zusammenführen von Daten aus unterschiedlichen Quellen, einfach zu bewerkstelligen. Deshalb können schon wenige Informationen aus zwei verschiedenen Quellen über uns ein umfassendes Bild ergeben.

IV. Ausblick und Kritik

1. De lege ferenda

Im Jahre 2010 hat der Bundesrat den Vorentwurf vom 30. April 2010[63] (VE BÜPF) und den Bericht[64] zur Totalrevision des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) in ein Vernehmlassungsverfahren geschickt. Dieses berücksichtigt diverse Postulate.[65]

Derzeit sollen Anpassungen am Vorentwurf in Überarbeitung sein und die Vorlage soll voraussichtlich im Jahre 2013 ins Parlament gelangen.

---

62 So z.B. Voice-over-IP, der Internettelefonie. Wird verschlüsselt zwischen zwei Computern telefoniert, so kann ohne Entschlüsselung das Gespräch nicht abgehört werden. Die einzige Möglichkeit, ein solches Gespräch aufzuzeichnen, ist diejenige, auf dem Computer eines Benutzers eine entsprechende Software zu installieren. siehe nachfolgend GovWare/Staatstrojaner unter Ziff. 4.

63 Abrufbar unter http://www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/entw-d.pdf (Stand 20.9.2012).

64 Abrufbar unter http://www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/vn-ber-d.pdf (Stand 20.9.2012).

65 Siehe dazu bei Rolf H. Weber, Christoph A. Wolf, Ulrike I. Heinrich, Neue Brennpunkte im Verhältnis von Informationstechnologien, Datensammlungen und flexibilisierter Rechtsordnung, in Jusletter, 12. März 2012, Ziff. 3.1.

Nachfolgend soll sowohl auf die geltende und allenfalls problematische gesetzliche Regelung wie auch de lege ferenda auf den Vorentwurf eingegangen werden.

2. Rangordnung

Ein neues BÜPF wird einerseits als neueres Recht vor dem alten sowie als lex specialis Vorrang vor einer lex generalis haben. Es geniesst gegenüber der Strafprozessordnung, dem Fernmeldegesetz und dem Datenschutzgesetz damit auch in Zukunft Vorrang.

Es ist deshalb darauf zu achten, dass die Bestimmungen des Datenschutzgesetzes und des Fernmeldegesetzes[66] nicht mit dem BÜPF/VÜPF kollidieren oder datenschutzrechtliche Schutzlücken entstehen lassen, sondern sich ergänzen. Datenschutzrechtliche Bestimmungen im BÜPF müssen sich an die Grundsätze im DSG anlehnen und darüber hinaus detaillierte Vorschriften zur Datensicherheit des ISS[67] und der Übertragung der ausgeleiteten Daten zu erlassen.

Ebenso ist zu beachten, dass ein neues BÜPF selbstverständlich auch zu Änderungen an der erst kürzlich angepassten VÜPF führt. Dem ist angemessen zu begegnen, indem genügend lange Übergangsfristen definiert werden.

3. Legalitätsprinzip

Die Bearbeitung von Personendaten im Rahmen der Überwachung ist derzeit auf Verordnungsstufe in Art. 7 ff. VÜPF geregelt. Im Rahmen der Revision des BÜPF soll nun in Art. 4 VE BÜPF festgehalten werden, dass die Behörden, welche die Überwachungen anordnen oder genehmigen, sowie die Personen, die Überwachungen nach dem Gesetz durchführen, diejenigen Personendaten bearbeiten dürfen, die sie benötigen, um die Ausführung der Überwachungsanordnung gewährleisten zu können.

Die Regelung auf Gesetzesstufe statt wie bis anhin auf Verordnungsstufe ist zu begrüssen. Derzeit sind nämlich nur die Fernmeldedienstanbieter durch Art. 43 ff. FMG zum Datenschutz auf Gesetzesstufe verpflichtet, nicht jedoch die Internetzugangsanbieter, was insbesondere bei Einführung einer Strafrechtsnorm relevant ist. Darüber hinaus erscheint diese Generalklausel hinsichtlich «aller benötigter Personendaten» (Art. 4 VE BÜPF) im Lichte der engen Zweckbestimmung, die

66 Siehe dazu Ziff. IV.4 betr. Cookies und Spyware/GovWare/Staatstrojaner.

67 Interception System Schweiz, das System des Dienstes ÜPF zur Verarbeitung der Überwachungsmassnahmen.

der Datenschutz fordert, als zu weit. Er genügt deshalb auch nicht als Grundlage für das anlasslose Speichern von Daten.

Fordert die Staatsanwaltschaft Daten, die nicht im BÜPF enthalten sind und für die keine Informationspflicht seitens des Fernmeldedienstanbieters besteht, können die Daten auch nicht benötigt und rechtmässig bearbeitet werden. Dies führt dazu, dass diese mangels legalen Verwendungszwecks von den Fernmeldedienstanbieterinnen und Internetzugansanbieterinnen nicht herauszugeben sind. Zu Recht verlangt deshalb die Mehrheit der Kritiker bezüglich Art. 4 VE BÜPF, dass neu eine Formulierung gewählt werden soll, die nur die «Ausführung der gerichtlich angeordneten und rechtmässigen Überwachungsanordnungen» umfasst. Ein Rechtsmittel der Fernmeldedienstanbieter und Internet(zugangs)anbieterinnen betreffend den Umfang der Überwachung gewährleistet damit die Rechtsstaatlichkeit.[68]

Als zweiter Punkt kommt hinzu, dass in der Generalklausel noch zusätzliche gesetzliche Grundlagen zu schaffen sind, welche die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen regeln, um dem Gebot der genügenden Bestimmtheit zu entsprechen.[69]

Darüber hinaus ist drittens darauf zu achten, was alles überwacht werden soll. Rechtsstaatlich problematisch ist, dass der Begriff der Verkehrsdaten weder im BÜPF, noch im FMG oder der StPO geregelt ist. Damit wird ein weiter zukünftiger Spielraum für die Strafverfolgungsbehörden geschaffen. So kann z.B. mit der Erweiterung des Adressraumes von IPV4 auf IPv6 zukünftig jedes an das Internet angeschlossene Gerät mit einer eigenen Adresse versehen werden.[70] Diese Befürchtung, geäussert vom Deutschen Datenschutzbeauftragten, ist heute bereits Realität. Und zwar nicht aufgrund der zunehmenden Grösse des Adressraumes der IP-Adressen, sondern aufgrund des Protokolls, welches IPv6 verwendet. Dieses beinhaltet nämlich auch die MAC-Adresse, also die Identifikations-Nummer für jedes Stück Hardware. Zusammen mit den Verkehrs- und Rechnungsdaten kann der Fernmeldedienstanbieter den Benutzer identifizieren. Zudem kann er noch viel mehr. Er kann so auch Informationen darüber liefern, ob der Benutzer nun sein Licht löscht oder noch brennen lässt.

---

68 Andreas Heiniger, Schrankenlose Fernmeldeüberwachung aufgrund eines konzeptionellen Fehlers im BÜPF?, in: Jusletter 17. September 2012.

69 Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens über den Bericht und den Vorentwurf zur Änderung des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), abrufbar unter http://www.ejpd.admin.ch/content/ejpd/de/home/themen/sicherheit/ueberwachung_des_post-/revision_buepf_undvuepf.html (Stand 20.9.2012).

70 BfDI-Tagungsband zum Symposium Internetprotokoll Version 6 (IPv6), Wo bleibt der Datenschutz?, abrufbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/TagungsbandSymposiumIPv6.pdf?_blob=publicationFile, (Stand 20.9.2012).

Ebenfalls ausgedehnt wurde im Rahmen des Vorentwurfes die rückwirkende Überwachung, die generell bei jedem Verbrechen und Vergehen angeordnet werden kann. Eine Beschränkung auf einen eingeschränkten Deliktskatalog ist bei der letzten VÜPF-Revision dahingefallen.

Zu bedenken ist zudem, dass durch Hardware-Identifiers (wie IMEI, MAC-Adressen) Strafverfolger den Benutzer durch Korrelation identifizieren können. Wenn der Benutzer die Hardware weitergibt, entstehen falsche Identifikationen, was den technischen Möglichkeiten Grenzen setzt und zudem zu Verdächtigungen Unbeteiligter führen kann.

4. Verhältnismässigkeit

Das derzeit gültige BÜPF entspricht einer austarierten Regelung, die den Anliegen der persönlichen Freiheit, der Wahrung des Fernmeldegeheimnisses und des Datenschutzes auf der einen Seite und den Interessen der Strafverfolgungsbehörden auf der anderen Seite angemessen Rechnung trägt.

Wird nun in diesem austarierten System noch mehr in die Waagschale der Interessen der Strafverfolgungsbehörden gelegt, so droht das Gleichgewicht zu kippen[71]. Anlass dazu könnten folgende Punkte sein, die Einlass in den Vorentwurf zur Revision des BÜPF gefunden haben.

Zum einen darf natürlich nicht jedes Bagatelldelikt dazu führen, dass eine Überwachung, sei es eine rückwirkende oder eine Echtzeitüberwachung, angeordnet wird. Nur bei schweren Delikten ist nach Auffassung des Bundesgerichtes an die Verhältnismässigkeit bzw. die Subsidiarität kein hoher Massstab anzulegen.[72]

Zum Zweiten hat bereits im Rahmen des Vorentwurfes der Staatstrojaner (auch GovWare[73]) in der Presse und der Lehre zu heftigen Diskussionen geführt, insbesondere in Hinblick auf die Legalität der getroffenen Massnahmen.[74] Aber auch

---

71 Gleicher Ansicht hinsichtlich der Austarierung bzw. des fairen Ausgleichs ist Heiniger, FN 68, Ziff. 6. Der faire Ausgleich bezieht sich bei Heiniger aber v.a. auch auf die Fernmeldedienstanbieter, die einer Möglichkeit bedürfen, ein Rechtmittel bei einer nicht zulässigen Überwachung ergreifen zu können.

72 Thomas Hansjakob, in: Donatsch et al. (Hrsg.); Kommentar zur Schweizerischen Strafprozessordnung, 2010, NN. 25 zu Art. 269 StPO; kürzlich bestätigt in BGE 1B-265/2012 vom 21. August 2012.

73 Während der Begriff Trojaner für die schädliche und bösartige Malware verwendet wird, soll der Begriff GovWare den legitimen Einsatz von Malware ausdrücken.

74 Siehe dazu Olivier Jotterand / Jérémie Müller / Jean Treccani, L'utilisation du cheval de Troie comme mesure de surveillance secrète, in: Jusletter, 21. Mai 2012, welche den Einsatz von Staatstrojanern unter den geltenden Art. 280 StPO dem Legalitätsprinzip entspre-

unter dem Gesichtspunkt der Verhältnismässigkeit lässt sich der Einsatz von Software, die den Rechner von Beschuldigten ausspioniert und weit über das Abhören von verschlüsselter Kommunikation gehen kann, nicht rechtfertigen. Es darf nicht dem Richter obliegen, Software einzusetzen, die alles herausfinden kann. Es braucht dazu gesetzliche Schranken, da die ganze Harddisk mit der entsprechenden GovWare gelesen werden kann.

Gleiches gilt für den Einsatz von Cookies durch die Strafverfolgungsbehörden. Zumindest ist das Setzen von Cookies zur Gewinnung von Personendaten ohne Zustimmung des Betroffenen in der EU klar unzulässig.[75] Auch in der Schweiz besteht diese Auffassung.[76] Jedoch gilt das Verbot des Setzens von Cookies, Spyware etc. ohne die Einwilligung des Nutzers derzeit erst für Fernmeldedienstanbieter (Art. 45c FDV). Der derzeitige Vorentwurf BÜPF steht dazu in Art. 21 Abs. 4 VE BÜPF in Widerspruch. Danach soll der Fernmeldedienstanbieter die Strafverfolgungsbehörden unterstützen, indem er GovWare, Spyware oder Staatstrojaner beim Benutzer platziert, quasi mit der GovWare infiziert.[77]

Ebenfalls beanstandet wurde in den Stellungnahmen zum VE BÜPF, dass eine flächendeckende Identifikation (wie sie z.B. Italien kennt) unverhältnismässig sei und umgangen werden könne. Die Umgehungsmöglichkeiten sind tatsächlich vielfältig. So gibt es etliche Ratgeber und Dienste zum anonymen Surfen.

Hinsichtlich der Erweiterung der Datenaufbewahrungspflicht von 6 auf 12 Monate (gem. Art. 20 Abs. 2 VE BÜPF) fragt sich, ob dies noch dem Verhältnismässigkeitsprinzip entspricht. Diese wird zum einen gefordert, da die Strafverfolgung meist länger dauert. Zum anderen kommen Delikte nicht immer gleich ans Tageslicht. M.W. wird aber mit der Verlängerung der Aufbewahrungsfrist der Hebel an einem falschen Ort angesetzt. Eigentlich müsste das Strafverfahren effizienter und straffer gestaltet werden.

---

chend betrachten, anders dagegen Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, in: Jusletter, 5. Dezember 2011, und Ciril Riss/Nicole Beranek Zanon, Art. 280 StPO genügt nicht als gesetzliche Grundlage für den Einsatz von Staatstrojanern, in: Jusletter, 9. Juli 2012.

75 Siehe dazu: e-Privacy-Richtlinie der EU 2002/58/EG; Gruppe Artikel 29, Bewährtes Vorgehen bei OBA (Englisch).

76 Die Meinung des EDÖB zu Cookies, abrufbar unter http://www.edoeb.admin.ch/themen/00794/01609/01763/index.html?lang=de (Stand 20.9.2012).

77 M.E. braucht es sowohl für die Verpflichtung von Fernmeldedienstanbieterinnen für die Strafverfolgungsbehörden Cookies bei Kunden einzusetzen, um Benutzerprofile zu erstellen und diese den Strafverfolgungsbehörden weiterzuleiten, wie auch für die Platzierung von Third Party Cookies durch die Strafverfolgungsbehörden oder für den Betrieb einer Webseite durch die Strafverfolgungsbehörden zur Distribution von GovWare/GovCookies spezifische gesetzliche Grundlagen, die verhältnismässig sind und eine genügende Bestimmtheit aufweisen.

Zu guter Letzt kann der Bundesrat gemäss der Formulierung von Art. 20 Abs. 4 VE BÜPF den Behörden nach Art. 14 BÜPF den Zugriff auf bestehende nicht öffentliche Verzeichnisse gestatten. Denkbar wäre z.B. das Tätigkeitsjournal für Domain-Namen unter .ch. Im Zusammenhang mit Anfragen von Strafverfolgungsbehörden sowie anderen Behörden wird die Registerbetreiberin für die .ch-Domain derzeit ca. 10-mal jährlich beauftragt, Daten über gewisse Domain-Namen-Inhaber offenzulegen. Ein ganzes Zugänglichmachen des Tätigkeitsjournals wäre damit unverhältnismässig und verletzt den Datenschutz von vielen anderen Domain-Namen-Haltern.

Diese und weitere Kritikpunkte zusammen kumuliert dürften dazu führen, dass das Gleichgewicht zwischen den Interessen kippt.

5. Schutzlücken ohne BÜPF?

Ohne das BÜPF dürfte der Staat den Fernmelde- und Internetverkehr von Verdächtigen nicht überwachen, da eine gesetzliche Grundlage fehlen würde. Dass die Echtzeitüberwachung zum Zwecke der Strafverfolgung notwendig ist, wird nicht bestritten. Die Frage aber, ob es einer Vorratsdatenspeicherung bedarf oder ob es Schutzlücken gäbe, hätten wir keine rückwirkende Überwachung, ist berechtigt. Denn heute müssen alle Fernmeldedienstanbieter für 6 Monate Verkehrs- und Randdaten speichern (und bald gemäss Art. 19 Abs. 2 VE BÜPF 12 Monate bzw. Art. 20 Abs. 2 VE BÜPF).

In Deutschland entschied im Jahre 2010 das Bundesverfassungsgericht[78], dass die dannzumal vorliegenden gesetzlichen Grundlagen nicht genügten, um den Eingriff ins Fernmeldegeheimnis zu rechtfertigen. Das Bundesverfassungsgericht gab aber klare Anweisungen an den Gesetzgeber, wie denn eine rechtskonforme, mithin verfassungskonforme Vorratsdatenspeicherung aussehen müsse.

Die Vorratsdatenspeicherung ist nur unter engen Auflagen zulässig. So müssen die Daten bei den Providern verbleiben. Es darf unter anderem kein unmittelbarer Zugriff auf sämtliche Daten durch den Staat geben und es braucht eine konkrete gesetzliche Regelung für eine besonders hohe Datensicherheit. So muss auch der Zugriff für die Strafverfolgung abschliessend geregelt werden, d.h., es muss definiert werden, für welche Straftaten und welche Gefahrenabwehr dies gilt. Sodann sei das Verfahren über die Auswertung der Daten nach Übermittlung an die Behörden zu regeln und nach der Art der abzufragenden Daten zu unterscheiden. Es sollen wie in der Schweiz besondere Regeln für Personen gelten, die einer ge-

[78] Urteil des deutschen Bundesverfassungsgerichts vom 2.3.2010 (1BvR 205/08, 1 BvR 263/08, 1BvR 586/08).

setzlichen Schweigepflicht unterworfen sind. Die betroffenen Personen sind sodann zu benachrichtigen, es sei denn, das Gericht hätte etwas anderes angeordnet. Ebenso gilt ein Richtervorbehalt für die Übermittlung und Nutzung der Daten. Zudem bedürfe es eines Rechtsschutzverfahrens zur nachträglichen Überprüfung der Datenübermittlung. Für IP-Adressabfragen macht das deutsche Bundesverfassungsgericht aber eine Ausnahme; an diese dürfen keine so hohen Anforderungen gestellt werden. Hinzu kommt, dass eine Abfrage der Verkehrsdaten nur subsidiär erfolgen kann. Allerdings darf an die Subsidiarität keine grossen Anforderungen gestellt werden, wie erst kürzlich das Schweizerische Bundesgericht feststellte.[79] Sind andere Untersuchungshandlungen ausgeschöpft – wie z.B. die Einsicht in die Rechnungsbelege – so dürfen die Strafverfolgungsbehörden die rückwirkende Überwachung, also den Zugriff auf die gespeicherten Verkehrsdaten anordnen.

Diese Regelungen sind insbesondere deshalb notwendig, weil die «vorsorglich anlasslose Speicherung aller Telekommunikationsverkehrsdaten über sechs Monate unter anderem deshalb ein so schwerwiegender Eingriff [ist], weil sie ein Gefühl des ständigen Überwachtwerdens hervorrufen kann; sie erlaubt in unvorhersehbarer Weise tiefe Einblicke in das Privatleben, ohne dass der Rückgriff auf die Daten für den Bürger unmittelbar spürbar oder ersichtlich ist. Der Einzelne weiß nicht, was welche staatliche Behörde über ihn weiß, weiß aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können.»[80]

Während das BÜPF viele dieser Vorgaben bereits regelt, besteht betreffend Datenschutz und insbesondere Datensicherheit für die Revision des BÜPF m.E. Handlungsbedarf. Es müssen Lücken geschlossen werden und Abgrenzungen klar definiert werden.

Eine weitere Frage ist, ob wir überhaupt Schutzlücken bei der Gefahrenabwehr und bei der Strafverfolgung hätten, wenn keine rückwirkende Überwachung bestände. Ein Gutachten des Max-Planck-Instituts kommt hierzu zum Schluss, dass es keine Auswirkungen auf die Aufklärungsquoten hätte, insbesondere auch im Vergleich zur Schweiz, welche eine Vorratsdatenspeicherung besitzt.[81]

---

79 Entscheid des Bundesgerichts 1B_265/2012 vom 21. August 2012.

80 Urteil des Bundesverfassungsgerichts vom 2. März 2010 (1 BvR 256/08; 1 BvR 263/08; 1 BvR 586/08), Rn. 241.

81 Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten, Max-Planck-Institut, Gutachten, Juli 2011, S. 219 N. 11 ff., abrufbar unter: http://vds.brauchts.net/MPI_VDS_Studie.pdf (Stand 20.9.2012); das Gutachten wurde aber im Nachgang kritisiert, da es durch Beeinflussung durch das Justizministerium entstanden sei. Zudem basiert die Studie auf Zahlen aus dem Jahre 2009.

6. Datensicherheit

Wie auch schon das Urteil des deutschen Bundesgerichtshofs zur Vorratsdatenspeicherung erörtert hatte, braucht es strenge Anforderungen an die Datensicherheit im Bereich der Überwachungsmassnahmen im Fernmeldeverkehr.[82] Im Rahmen des Vorentwurfes zum neuen BÜPF hat man dem Rechnung getragen und in Art. 4 VE BÜPF den Verweis auf die datenschutzrechtlichen Bestimmungen und damit auf Art. 7 DSG hinsichtlich Datensicherheit aufgenommen. Gemäss Art. 12 VE BÜPF ist der Dienst ÜPF für die Sicherheit des Verarbeitungssystems verantwortlich. Der Bundesrat erlässt Vorschriften über technische und organisatorische Schutzmassnahmen, insbesondere gegen den Zugang, die Änderung, die unbefugte Verbreitung und die ungewollte oder unbefugte Vernichtung der Daten. Personen, die Überwachungen nach dem BÜPF durchführen, müssen bei der Übertragung der Daten aus der Überwachung den entsprechenden Anweisungen des Dienstes für die Datensicherheit folgen.

Bei der konkreten Umsetzung, insbesondere im Rahmen der TSTR und der OAR, sollte der Datensicherheit erhöhte Rechnung getragen werden. Dies bedeutet, dass die Datenübertragung wenn immer möglich verschlüsselt erfolgen sollte und mit einer Punkt-zu-Punkt-Verbindung oder einem Virtual Private Network (VPN) zu erfolgen hat.

7. Begehrlichkeiten

Die vorhandenen Daten schaffen weitere Begehrlichkeiten. So soll gemäss Art. 20 Abs. 4 2. Satz VE BÜPF ein direkter Zugriff auf nicht öffentliche Verzeichnisse durch Behörden möglich werden. Dies ist zugegebenermassen interessant für all diejenigen Bundesämter, welche die Einhaltung gesetzlicher Verpflichtungen prüfen müssen wie z.B. die FINMA betreffend dem Erfordernis, dass eine Online-Bank auch über eine Bankenlizenz verfügt, die Swissmedic, dass rezeptpflichtige Medikamente nicht online ohne Rezept verkauft werden oder die Eidgenössische Spielbankenkommission ESBK, dass keine Wetten und Lotterien ohne eine Bewilligung online erfolgen.

Spinnt man das Ganze weiter, so sieht man, wo diese Begehrlichkeiten enden könnten. Der Zugriff auf Daten von Single-Sign-On-Anbieterinnen, die ihre Authentifikation auf biometrische Verfahren abstützen und dazu das Internet benötigen, könnte dazu führen, dass nebst den Fernmeldedaten auch auf Daten wie

[82] Vgl. FN 50.

Stimme, Iris und Ohr und Fotografien von Benutzern zukünftig zurückgegriffen werden kann.

8. Vollstreckung

Ein letztes Problem liegt in der Technik. Das System des Dienstes ÜPF ist noch nicht genügend in der Lage, alle möglichen Daten auch entgegenzunehmen, auszuwerten und den Strafverfolgungsbehörden zur Verfügung zu stellen. Dies zum einen wegen der Datenmenge und zum anderen bedingt durch die technisch eingeschränkten Übermittlungsmethoden.

Das geltende Recht sieht damit einige Überwachungsarten vor, die mangels sogenanntem Target Identifier derzeit technisch nicht überwacht werden können. Entsprechend ist ein Seilziehen zwischen Fernmeldedienstanbietern, dem Dienst ÜPF und den Staatsanwaltschaften im Gange. Die Fernmeldedienstanbieter möchten im Gesetz und in der Verordnung nur das festhalten, was derzeit technisch möglich ist. Der Dienst ÜPF und die Staatsanwaltschaften möchten möglichst Generalklauseln, damit Gesetz und Verordnung nicht schon bald revidiert werden müssen und neue Technologien keine Hindernisse für die Strafverfolgungsbehörden mehr darstellen.

V. Fazit

Als Schlussfolgerung kann festgehalten werden, dass eine grundsätzliche Kollision der Konzeption von DSG und BÜPF besteht. Der Gesetzgeber ist in der anstehenden Revision des BÜPF gefordert, eine Wertung vorzunehmen und klare gesetzliche Grundlagen zu schaffen, die den Grundrechtseingriff ins Fernmeldegeheimnis und den Datenschutz i.A. rechtfertigen und ein austariertes Modell ergeben. Dabei ist das Augenmerk darauf zu richten, dass das Gleichgewicht der Interessen zwischen der Wahrung der Grundrechte und den Interessen der Strafverfolgung gewahrt bleibt.