Prof. Sabine Gless
Basel

Strafverfolgung im Internet

Nicht im Handel

Sonderdruck aus
«Schweizerische Zeitschrift für Strafrecht»
Band 130 · 2012 · Heft 1

Stämpfli Verlag AG Bern

Sabine Gless, Basel

Strafverfolgung im Internet

Inhaltsübersicht

I. Einleitung

Ist Strafverfolgung im Internet zulässig? Die Antwort auf diese Frage scheint den meisten heute selbstverständlich – die Diskussion geht nicht mehr um das Ob, sondern nur noch um das Wie der Strafverfolgung. Frühe Protagonisten des Internets hatten jedoch durchaus die Vision eines weltweiten Kommunikationsraumes ohne jegliche staatliche Regulierung. In diesem Sinne erklärte etwa John Barlow[1] im Jahr 1996 am World Economic Forum (WEF) in Davos die Unabhängigkeit des Internets:

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. ..."[2]

Bekanntlich hat die Staaten diese Unabhängigkeitserklärung der neuen, künstlich geschaffenen Welt wenig interessiert. Sie formulieren vielmehr ihre Ansprüche an das Verhalten im World Wide Web und kontrollieren die Einhaltung

1 Ehemaliger Liedtexter der Grateful Dead, später Sprecher der Internetbewegung Electronic Frontier Foundation.

2 Siehe [https://projects.eff.org/~barlow/Declaration-Final.html]. In deutscher Übersetzung (bei Telepolis): «Regierungen der industriellen Welt, ihr müden Riesen aus Fleisch und Stahl, ich komme aus dem Cyberspace, dem neuen Zuhause des Geistes. Als Vertreter der Zukunft bitte ich euch aus der Vergangenheit, uns in Ruhe zu lassen. Ihr seid nicht willkommen unter uns. Ihr habt keine Souveränität, wo wir uns versammeln.»

der Verhaltensanforderungen durch Strafverfolgung und andere Massnahmen im virtuellen Raum. Die damit einhergehenden Probleme der Rechtsdurchsetzung im Internet werfen viele praktische und rechtliche Fragen auf. Sie reichen von der Auseinandersetzung über die Strafbarkeit bestimmter Handlungen und Inhalte im Netz[3] über Probleme bei verdeckten Ermittlungen in Internetchats[4] bis zur praktischen Umsetzung und rechtlichen Zulässigkeit von Online-Überwachungen oder der geheimen Durchsuchung von Computern und anderen Datensystemen.[5]

Staatliche Behörden tun heute also genau das, wovor Barlow vor fünfzehn Jahren gewarnt hat: Sie stellen ihre Wachposten an den Grenzen des Cyberspace auf, sie spionieren die Bewohner des weltweiten Netzes aus. Massnahmen wie die heimliche E-Mail-Überwachung oder den Einsatz sog. Staatstrojaner rechtfertigen sie unter anderem mit dem Bedürfnis nach Strafverfolgung. Die Verteidiger eines von staatlichen Eingriffen unabhängigen Internets sichern zwar unter Zuhilfenahme technischer Vorrichtungen immer wieder ein Stück Netz-Freiheit ausserhalb staatlicher Überwachung, etwa durch Verschlüsselungsprogramme, den Einsatz von Proxy-Servern, Fire-walls resp. Antitrojanern etc.[6] Doch die staatlichen Behörden sind ihnen auf den Fersen. Diese setzen im Gegenzug auch auf technische Massnahmen wie etwa die Sperrung von Internetseiten[7] oder den Einsatz von Spionagesoftware (Spy-ware).[8]

Vor allem aber können Hoheitsträger in der realen Welt – auch mit dem Ziel der Strafverfolgung in der virtuellen Welt – spürbare Massnahmen ergreifen. Da die Akteure des Internets mit den Strafverfolgungsbehörden die reale Welt teilen,

3 *J. Achermann,* Besitz an verbotenen pornographischen Dateien im Cache-Speicher, Jusletter 15.8.2011; *M. A. Niggli/Ch. Schwarzenegger,* Strafbare Handlungen im Internet, SJZ 2002, 61–73; *A. Popp,* Von «Datendieben» und «Betrügern» – zur Strafbarkeit des so genannten «phishing», NJW 2004, 3517–3518; *Ch. Schwarzenegger,* Die Internationalisierung des Wirtschaftsstrafrechts und die schweizerische Kriminalpolitik, ZSR 2008 II, 399–503; *U. Sieber,* Rechtliche Ordnung in einer globalen Welt, Rechtstheorie 41 (2010), 151 ff.

4 *P. Bischoff/M. Lanter,* Verdeckte polizeiliche Ermittlungshandlungen in Chatrooms, Jusletter 14.1.2008; *P. Studer,* Die vorbeugende Ermittlung von Pädophilen in Kinderchatrooms – ein Opfer der neuen Strafprozessordnung?, Jusletter v. 15.11.2010.

5 *U. Buermeyer,* Die «Online-Durchsuchung». Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, 154 ff.; *T. Hansjakob,* Einsatz von GovWare – zulässig oder nicht?, Jusletter v. 6.12.2011.

6 Vgl. etwa zum Einsatz von Antitrojanern: http://www.pctipp.ch/downloads/sicherheit/5831/archicrypt_anti_bundestrojaner.html oder zu Anonymisierungsprogrammen: *P. Brunst,* Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, Berlin 2009, 46 ff.; *H. Kudlich,* Strafverfolgung im Internet – Bestandsaufnahme und aktuelle Probleme, GA 2011, 204 f.

7 [http://www.nzz.ch/nachrichten/politik/schweiz/switch_sperrt_boesartige_websites_1.8464050.html].

8 Vgl. Presseerklärung des EJDP, zitiert am 13. Oktober 2011 in NZZ Online, sowie [http://www.nzz.ch/nachrichten/politik/wahlen2011_smartvotedb/auch_in_der_schweiz_haben_die_behoerden_spionage-software_eingesetzt_1.12977775.html].

in der ihr Computer beschlagnahmt und sie verhaftet werden können, sind sie letztendlich immer staatlicher Strafverfolgung unterworfen. Damit sie bestraft werden können, müssen die inkriminierten Handlungen jedoch vor Gericht bewiesen werden. In diesem Zusammenhang stellen sich immer wieder alte und auch neue Fragen nach der Zulässigkeit strafprozessualer Beweissammlung im Internet. Die Aktualität der Fragestellungen zeigen nicht nur Debatten zwischen Wissenschaftlern, wie etwa auf dem Strafrechtslehrertag 2011 in Leipzig,[9] sondern verschiedenste Meldungen in der Tagespresse.[10] Im Zentrum des ersten Teils der folgenden Überlegungen (II) stehen die einschlägigen, bereits bestehenden Ermächtigungsgrundlagen der Strafprozessordnung (StPO). Weitere Fragen, etwa nach der Zulässigkeit präventiv-polizeilicher Massnahmen oder grenzüberschreitender Ermittlungen,[11] müssen eigenständigen Untersuchungen vorbehalten bleiben.

Der zweite Teil der vorliegenden Untersuchung (III) analysiert kritisch Entwicklungslinien der Strafverfolgung im Internet. Insbesondere der Einsatz sog. Staatstrojaner hat wieder eine Diskussion über die Zulässigkeit und Grenzen technisch-invasiver Ermittlungen ausgelöst. Denn einerseits ist der Einsatz neuer Techniken notwendig, um die virtuelle Welt kontrollierbar oder kontrollierbarer zu machen, andererseits sind Strafverfolgungsbehörden als Hoheitsträger im weltweiten Netz weiter an ihre nationale Rechtsordnung, an die für sie einschlägigen, demokratisch legitimierten Normen gebunden.[12] Gerade der Einsatz von Spy-ware durch die Behörden hat wieder einmal deutlich gemacht, dass nicht alles, was technisch möglich ist, rechtlich zulässig sein muss, aber auch nicht alles, was rechtlich noch zulässig erscheint, in gleicher Weise zuverlässig technisch umsetzbar ist[13]. Hier stellt sich für die Strafverfolgung die – aus anderen Gebieten der Rechtswissenschaft bereits bekannte – Frage nach der Vorherrschaft des Rechts oder dem Primat der Technik (s. u. III).

9 «Fragmentarisches Strafrecht in einer global vernetzten Welt», 34. Strafrechtslehrertagung (Leipzig, 23.–26. 6. 2011); *G. Schmölzer,* Straftaten im Internet – eine materiell-rechtliche Betrachtung, 34. Strafrechtslehrertagung (Leipzig, 23.–26. 6. 2011); *D. Klesczewski,* Straftataufklärung im Internet: technische Möglichkeiten und rechtliche Grenzen von strafprozessualen Ermittlungseingriffen im Internet, 34. Strafrechtslehrertagung (Leipzig, 23.–26. 6. 2011).

10 Zuletzt etwa zum Einsatz sog. Staatstrojaner durch Schweizer Behörden, vgl. Basler Zeitung vom 15.10.2011, 5; NZZ vom 15.10.2011, 13.

11 Vgl. dazu etwa: *D. Bär,* Transnationaler Zugriff auf Computerdaten, ZIS 2011, 53 ff.; *S. Heimgartner,* Strafprozessuale Beschlagnahme, Zürich et al. 2011, 93 und 267; *B. Gercke,* Zur Zulässigkeit sog. Transborder Searches, StraFo 2009, 271 ff.; *H. Kudlich,* Strafprozessuale Probleme des Internet, JA 2000, 227 ff.; *Bischoff/Lanter* (Fn. 4); *K. Gaede,* Der grundrechtliche Schutz gespeicherter E-Mails beim Provider und ihre weltweite strafprozessuale Überwachung, StV 2009, 101 f.

12 *Heimgartner* (Fn. 11), 267; *H. Kudlich* (Fn. 6), 195 f.

13 *S. Métille,* Les mesures de surveillance prévues de CPP, Jusletter v. 19.12.2011.

II. Beweissammlung im Internet – ausgewählte Fallkonstellationen

Die am 1. Januar 2011 in Kraft getretene Strafprozessordnung (StPO) hält verschiedene Ermächtigungsgrundlagen bereit, die eine Beweissammlung im Internet durch Schweizer Strafverfolgungsbehörden ermöglichen. Von Interesse sind dabei vor allem die Beschlagnahme und Durchsuchung von Datenträgern (Art. 246 ff. und 263 ff. StPO), die Überwachung des Post- und Fernmeldeverkehrs (Art. 269 ff. StPO), die Observation (Art. 282 f. StPO), der Abruf von Verkehrsdaten (Art. 273 StPO) sowie Regelungen über verdeckte Ermittlungen (Art. 286 ff. StPO). Teilweise wird das Strafprozessrecht durch flankierende Regelungen im BÜPF[14] oder in anderen Bundesgesetzen ergänzt.

Keine der Normen der StPO bezieht sich ausdrücklich auf die Beweissammlung im Internet. Einige der Regelungen bieten jedoch spezifische Anknüpfungspunkte bezüglich der dafür notwendigen Technik und Geräte (Computer, Datenträger, Fernmeldeverkehr etc.) oder sind so allgemein gehalten, dass sie im Prinzip überall angewendet werden können. Für jede technisch mögliche Ermittlungsmassnahme, die einen Eingriff in die grundrechtlich geschützte Kommunikation darstellt, ist zu prüfen, ob de lege lata eine adäquate Ermächtigungsgrundlage besteht, ansonsten ist die Beweissammlung unzulässig.[15]

1. Kontrolle von E-Mail-Kommunikation

Die derzeit wohl prominenteste internetspezifische Kommunikationsform ist der E-Mail-Verkehr. Voraussetzung dafür sind die Einrichtung eines sog. Mailaccounts bei einem (Host-)Provider (etwa gmail, unibas, bluewin) und der Zugang über einen (Access-)Provider (etwa Swisscom, cablecom, Universitätsrechenzentren).

Strafverfolgungsbehörden können vom Inhalt einer E-Mail-Kommunikation in Echtzeit oder durch nachträgliches Lesen Kenntnis nehmen. Welches Vorgehen sie wählen, hängt davon ab, ob zum jeweiligen Zeitpunkt eines Verfahrens eine heimliche Überwachung oder eine (nachträgliche) Sicherung von gespeicherten E-Mails zu Beweiszwecken erforderlich ist. Manchmal fliessen in die Entscheidung aber auch pragmatische Überlegungen ein, z. B. ob und wie die Behörden in verschiedenen Phasen einer E-Mail-Kommunikation am einfachsten Zugriff auf die Mails nehmen können, etwa nur über den Nutzer oder auch über einen der Provider.

14 Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, SR 780.1.

15 *S. Gless*, in: Basler Kommentar Strafprozessordnung, hrsg. von M. A. Niggli/M. Heer/H. Wiprächtiger, Basel 2011, Art. 141 StPO N 1.
W. Wohlers, in: Kommentar zur Schweizerischen Strafprozessordnung, hrsg. von A. Donatsch/Th. Hansjakob/J. Lieber, Zürich/Basel/Genf 2010, Art. 141 N 1.

a) Durchsuchung und Beschlagnahme von E-Mails

Suchen die Strafverfolgungsbehörden nach abgespeicherten E-Mails auf einem Datenträger der verdächtigen Person, damit diese zu Beweiszwecken gesichert werden können, so greifen die allgemeinen Vorschriften:[16] Gemäss Art. 246 ff. StPO können die Strafverfolgungsbehörden Aufzeichnungen und Datenträger durchsuchen. Dazu gehören etwa CDs, USB-Sticks, Festplatten etc.[17] Werden die Strafbehörden fündig, so beschlagnahmen sie nach Art. 263 ff. StPO.[18] Eine Beschlagnahme ist grundsätzlich auch bei einer Drittperson, etwa dem Provider, möglich. Es müssen dann sowohl die für den Datenträger verantwortliche Person und der Datenberechtigte über die Massnahme informiert werden.[19]

Die Nutzung des Internets spielt bei einem abgeschlossenen Kommunikationsvorgang, wenn ein «elektronisches Schriftstück» vorhanden ist, allenfalls dann noch eine Rolle, wenn gespeicherte E-Mails nur mithilfe des Internets abgerufen werden können. Das ist etwa dann der Fall, wenn kein festplattengestützter Speicherplatz, sondern «Cloud Computing» zur Datensicherung genutzt wird.[20] Diese «Clouds» sind von Hardware (Rechenzentrum, Server, Festplatte) abstrahierte IT-Infrastrukturen (Rechenkapazität, Datenspeicher, Netzwerkkapazitäten etc.), über die – dynamisch an den Bedarf angepasst – Daten verarbeitet werden können. Ein Teil der Datenverarbeitung geschieht gewissermassen in einer «Wolke» und liegt (technisch) nicht mehr im Verantwortungsbereich des Nutzers, sondern in dem des Anbieters der «Cloud».[21] Der Zugriff des Benutzers auf den gemieteten Datenraum in der Cloud erfolgt zwar zumeist über das Internet, also im virtuellen Raum. Die Rechnerwolke selbst ist jedoch auf einem örtlich lokalisierten Server gespeichert, auf den auch die jeweils vor Ort zuständigen Strafverfolgungsbehör-

16 *M. Jean-Richard-dit-Bressel,* Die Mailbox – Ziel oder Weg?, ZStrR 2007, 159 f.; aus deutscher Sicht: *H. Kudlich* (Fn. 11), 228 f.

17 Zur Durchsuchung und Beschlagnahme elektronischer Datenträger vgl. *M. Aepli,* Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, unter besonderer Berücksichtigung der Beweismittelbeschlagnahme am Beispiel des Kantons Zürich, Zürich 2004, 89 ff., 118 ff.; *Bär* (Fn. 11), 53 f.

18 BSK StPO-*M. Jean-Richard-dit-Bressel* (Fn. 15), Art. 269 N 24.

19 *Jean-Richard-dit-Bressel* (Fn. 16), 171 ff.

20 Zum Cloud Computing und zu dessen rechtlichen Konsequenzen vgl. etwa: *M. Bedner,* Rechtmässigkeit der «Deep Packet Inspection», 26. November 2009: [http://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis: 34-2009113031192/5/BednerDeepPacketInspection.pdf].

21 *B. Gercke,* Praxishandbuch Internetstrafrecht, hrsg. von B. Gercke/P. Brunst, Stuttgart 2009, 232 ff.; *D. Brodowski/F. Freiling,* Cyberkriminalität – Computerstrafrecht und die digitale Schattenwirtschaft, Schriftenreihe Forschungsforum Öffentliche Sicherheit 2011, 172; *N. Obenaus,* Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, NJW 2012, 651 f.

den zugreifen können.[22] Ebenso können die Betreiber es technisch bewerkstelligen, dass «Cloud Computing» nur innerhalb bestimmter territorialer Räume genutzt werden kann.[23] Mit der wachsenden Beliebtheit des «Cloud Computings» wird der Zugriff auf den virtuellen Kommunikationsraum einer Person zwar schwieriger, jedoch nicht unmöglich. Es gelten deshalb die allgemeinen Regeln.

Bei einer Durchsuchung und Beschlagnahme von gespeicherten E-Mails ergeben sich in der Praxis deshalb im Wesentlichen nur die bekannten Probleme, etwa wenn Inhaberinnen von Aufzeichnungen und Gegenständen ein Zeugnisverweigerungsrecht geltend machen[24] oder Datenträger aus anderen Gründen nicht durchsucht oder beschlagnahmt werden dürfen.[25] Dann müssen die Datenträger vorerst versiegelt werden; allenfalls muss das für eine Entsiegelung im Vorverfahren zuständige Zwangsmassnahmengericht oder das in der gerichtlichen Phase zuständige Sachgericht über das weitere Vorgehen entscheiden.

b) Heimliche Überwachung von E-Mail-Kommunikation

Anders ist die rechtliche Situation, wenn eine E-Mail-Kommunikation zeitgleich und heimlich überwacht werden soll. Hier werden – wie bei der Telefonüberwachung – die Äusserungen eines Verdächtigen ohne dessen Wissen zu Zwecken der strafprozessualen Beweissammlung im Kommunikationsvorgang dokumentiert.

Ein Ermittlungseingriff in eine laufende Kommunikation ist nach h. M. stets nach den Vorgaben für die Überwachung des Post- und Fernmeldeverkehrs durchzuführen. Diese sind in Art. 269 ff. StPO – im Anschluss an die frühere Regelung im BÜPF[26] – niedergelegt. Die gesetzlichen Schranken dafür erscheinen hoch: Die Überwachung der Telekommunikation wird durch die Staatsanwaltschaft angeordnet (Art. 269 Abs. 1 StPO), die jedoch innerhalb von 24 Stunden dem Zwangsmassnahmengericht einen begründeten Genehmigungsantrag unterbreiten muss. Dieses entscheidet dann über die Zulässigkeit der Massnahme (Art. 274 StPO). Da der Überwachte (zunächst) nichts von der Massnahme erfährt, muss das Gericht

22 *P. Brunst,* Praxishandbuch Internetstrafrecht, hrsg. von B. Gercke/P. Brunst, Stuttgart 2009, 262 ff.; *Brodowski/Freiling* (Fn. 21), 172.

23 Internetunternehmen haben auf einschlägige Bedenken ihrer Kunden bereits insofern reagiert, als sie ihr Cloud Computing mithilfe technischer Vorrichtungen auf bestimmte Rechtsräume begrenzen, vgl. dazu: *M. Armbrust* et al., Above the Clouds: A Berkeley View of Cloud Computing, 15–16 [http://radlab.cs.berkeley.edu].

24 *Obenaus* (Fn. 21), 652 ff.; zu den einschlägigen strafprozessualen Problemen: Botschaft zur Vereinheitlichung des Strafprozessrechts vom 21.12.2005, BBl 2005, 1085 ff., 1239.

25 Vgl. Art. 264 StPO.

26 Prozessrechtliche Vorgaben finden sich heute in der StPO, während technische Fragen, etwa betreffend Provider, weiterhin in BÜPF/VÜPF geregelt sind, vgl. a. Botschaft StPO (Fn. 24), 1085 ff., 1248.

als Kontrollinstanz seine und auch die Interessen Drittbetroffener berücksichtigen.[27] Welche einschränkende Wirkung diese gesetzlichen Hürden in der Praxis haben werden, bleibt abzuwarten.

Das Gesetz differenziert hinsichtlich der Voraussetzungen der Überwachung zwischen verschiedenen Betroffenen: Der Anschluss eines Verdächtigen darf bei dringendem Tatverdacht (Art. 269 Abs. 1 lit. a StPO) auf Begehung einer Katalogtat nach Art. 269 Abs. 2 StPO und unter einem Verhältnismässigkeits- und Subsidiaritätsvorbehalt (Art. 269 Abs. 1 lit. c StPO) überwacht werden.[28] Die geheime Überwachung des Anschlusses einer Drittperson ist nur ausnahmsweise dann zulässig, wenn angenommen werden muss, dass der Beschuldigte deren Anschluss benutzt oder dass die Drittperson Mitteilungen entgegennimmt oder weiterleitet (Art. 270 lit. b StPO).

Bei der Überwachung des Anschlusses eines mutmasslich Zeugnisverweigerungsberechtigten schützt Art. 271 die Berufsgeheimnisträger.[29] Aus Sicht des Gesetzgebers ist die beruflich bedingte Geheimsphäre (etwa das Vertrauensverhältnis zum Strafverteidiger, zu einem Geistlichen oder einem Journalisten) auch bei heimlichen Ermittlungsmethoden absolut geschützt.

Das Vertrauensverhältnis zwischen einem Verdächtigten und einer ihm nahestehenden Person bleibt bei heimlichen Ermittlungsmassnahmen de lege lata jedoch ungeschützt. Hier bewahrt das Zeugnisverweigerungsrecht nur vor einem Gewissenskonflikt bei Aussagezwang; es existiert aber kein besonderer Schutz, wenn Strafverfolgungsbehörden geheim tätig werden. Das bedeutet in der Praxis, dass die Behörden die E-Mail-Kommunikation zwischen Eheleuten überwachen und so belastende Informationen erlangen können, auch wenn ein Ehegatte in einer Vernehmung von einem Zeugnisverweigerungsrecht nach Art. 168 StPO Gebrauch macht. Nach Ansicht des Gesetzgebers sollen die Zeugnisverweigerungsrechte nahestehender Personen – wie beispielsweise auch der Eltern – eben ausschliesslich vor dem Konflikt bei der *zwangsweisen* Informationsbeschaffung durch staatliche Hoheitsträger schützen, nicht aber eine unfreiwillige Preisgabe von belastender Information im Rahmen einer privaten Kommunikation verhindern.[30] Diese Ansicht gründet offensichtlich auf der Überzeugung, dass die Privatsphäre,

27 BSK StPO-*Jean-Richard-dit-Bressel* (Fn. 15), Art. 269 N 21; *N. Schmid,* Handbuch des schweizerischen Strafprozessrechts, Zürich/St. Gallen 2009, N 1136.

28 Vgl. dazu *N. Oberholzer,* Grundzüge des Strafprozessrechts, 2. Aufl., Bern 2005, 549; *M. Pieth,* Schweizerisches Strafprozessrecht, Grundriss für Studium und Praxis, Basel 2009, 128; *N. Ruckstuhl,* Fehlende Parteirechte bei verdeckter Ermittlung, plädoyer 2005, 34–37.

29 Die sie betreffenden Informationen sind auszusondern, es sei denn, sie selbst seien tatverdächtig.

30 Botschaft StPO (Fn. 24), 1085 ff., 1249; *F. Bommer/P. Goldschmid,* Die Auswirkungen von Aussagefreiheit und Zeugnisverweigerungsrechten auf Beschlagnahme und Herausgabe, ZBJV 1997, 345 ff.

etwa auch in der Familie, Schutz vor einem staatlichen Eingriff nur bei einer Willensbeugung der Betroffenen verdient. Mit Blick auf den Ausbau heimlicher Ermittlungsmassnahmen spricht jedoch vieles für eine Ausdehnung des Verwertungsverbots, etwa um die vertrauliche Sphäre im engsten Privatbereich zu schützen, die es erlaubt das Gewissen zu erleichtern, ohne eine Sanktion befürchten zu müssen.

Heute erachtet der Gesetzgeber die Interessen der Betroffenen, insbesondere die Rechte von Beschuldigten, durch die Anforderungen an die Anordnung einer Telekommunikationsüberwachung als gewahrt. Einigkeit herrscht deshalb darüber, dass diese Regeln immer anwendbar sind, wenn die Strafverfolgungsbehörden private Kommunikation ohne Wissen der Betroffenen zur Kenntnis nehmen.[31] Jenseits der prinzipiellen Anwendbarkeit der Grundregeln der Telekommunikationsüberwachung bleiben Einzelfragen offen, weil die aktuellen Rechtsgrundlagen nicht primär für die Strafverfolgung im Internet konzipiert wurden:

Bereits die äusseren Umstände einer E-Mail-Kommunikation über das Internet unterscheiden sich von jenen der Telefonie, weil E-Mails als *schriftliche* Nachrichten – anders als das flüchtige Wort – stets in digitaler Form gespeichert, also auch ohne einen Abhörvorgang manifest und nicht notwendigerweise vom Empfänger direkt abgerufen werden. Seit den Anfängen des internetgestützten E-Mail-Verkehrs diskutiert man deshalb die Frage, wie lange dieser Kommunikationsvorgang als fliessender Verkehr und wann er als abgeschlossen anzusehen ist resp. wie lange ein heimliches Mitlesen und wann eine Beschlagnahme der elektronischen Post angebracht erscheint.[32] Die Zäsur hat die Strafrechtswissenschaft teilweise als entscheidend dafür angesehen, ob eine technisch mögliche Herausgabe von E-Mails durch Dritte – in der Regel durch einen Provider in Form einer Sicherungskopie – noch während des Kommunikationsvorganges ohne Information des Mailboxinhabers zulässig wäre. Eine solche «heimliche Beschlagnahme» würde jedoch die klare Trennlinie der StPO zwischen geheimer Überwachung der am Kommunikationsvorgang Beteiligten einerseits und (offener) Beschlagnahme andererseits verletzen, die auch für elektronische Post gilt. Das technisch Mögliche ist deshalb rechtlich unzulässig. Nach heute herrschender Ansicht ist jede Inhaltskontrolle einer E-Mail-Kommunikation, die den Kommunizierenden gegenüber nicht offengelegt wird, stets als heimliche Telekommunikationsüberwachung nach Art. 269 ff. StPO einzustufen.

31 *E. Jaggi,* Geheime Überwachungsmassnahmen, ZBJV 2011, 1; *I. Zerbes,* Das Urteil des deutschen Bundesverfassungsgerichtes zur Online-Durchsuchung, ÖJZ 2008, 834–846; a. A. BSK StPO-*Jean-Richard-dit-Bressel* (Fn. 15), Art. 269 N 21; *D. Jositsch,* Grundriss des schweizerischen Strafprozessrechts, Zürich 2009, N 429.

32 Dazu etwa: *A. Donatsch/A. Schmid,* Der Zugriff auf E-Mails im Strafverfahren – Überwachung (BÜPF) oder Beschlagnahme, hrsg. von C. Schwarzenegger/O. Arter /F. S. Jörg, Internet-Recht und Strafrecht, Bern 2005, 151 ff.

Das entscheidende Merkmal ist die Heimlichkeit der Massnahme,[33] nicht die faktische Möglichkeit des Zugriffs resp. «Datenherrschaft».[34] Denn sonst hinge es mehr oder weniger vom Stand der Technik oder der Zufälligkeit des Speicherplatzes ab, ob eine Kommunikationsüberwachung als – unzulässige heimliche – Beschlagnahme durchgeführt werden könnte. Der blosse Umstand, dass ein Provider eine Sicherungskopie hergestellt hat, auf welche zurückgegriffen werden könnte,[35] ändert nichts an dem Charakter der Massnahme als heimliche Überwachung, denn den Teilnehmern der E-Mail-Kommunikation bleibt verborgen, dass die elektronische Post von den Strafverfolgungsbehörden mitgelesen wird.[36]

2. Überwachung von Internettelefonie

Neben dem E-Mail-Versand hat die Internettelefonie – als preisgünstige Alternative zu klassischer Telefonie – in kurzer Zeit grosse Bedeutung erlangt. Noch vor 15 Jahren führte man Telefongespräche regelmässig von einem Festnetzanschluss aus, der vergleichsweise einfach einer bestimmten Person oder einem bestimmten Personenkreis zugeordnet werden konnte, was die Kontrolle einer Telefonkommunikation vereinfachte. Bereits die Einführung und schnelle Verbreitung von Mobiltelefonen hat die Überwachung erschwert. Die Internettelefonie birgt nun noch einmal neue Herausforderungen.

Wie bereits erläutert, regeln die Art. 269 ff. StPO die materiellen Voraussetzungen und formellen Anforderungen an eine geheime Überwachung von Post- und Telekommunikation, wozu allgemein neue Kommunikationsformen, wie Internettelefonie oder IP-Telefonie, gezählt werden. Alle diese Regelungen, bei welchen der Gesetzgeber die Interessen der betroffenen Individuen gegenüber dem Strafverfolgungsinteresse abgewogen und die Voraussetzungen für eine Überwachung festgelegt hat, gelten grundsätzlich auch für das Telefonieren über das Internet. Allerdings unterscheidet sich die Technik von Internettelefonie in verschiedener Hinsicht von der klassischen Telefonie mit der Konsequenz, dass ein Provider des überwachten Kunden den Strafverfolgungsbehörden Zugang zum Inhalt eines Telefonats über das Netz nicht in gleicher Weise wie ein normaler Telefonanbieter den Strafverfolgungsbehörden liefern kann.

33 Vgl. a.: *Hansjakob,* in: Kommentar StPO (Fn. 15), Art. 269, Rn. 9, sowie *Heimgartner,* in: Kommentar StPO (Fn. 15), Art. 263, Rn. 5; *ders.* (Fn. 11), s. insbesondere 38 f., vgl. auch 177.

34 BSK StPO-*Jean-Richard-dit-Bressel* (Fn. 15), Art. 269 N 22 f.; *Aepli* (Fn. 17), 17; *Donatsch/Schmid* (Fn. 32), 157; *Th. Hansjakob,* Erste Erfahrungen mit dem BÜPF, ZStrR 2002, 266; *Jean-Richard-dit-Bressel* (Fn. 16), 171; *Schmid,* Handbuch (Fn. 27), N 1139.

35 Vgl. etwa: *Heimgartner* (Fn. 11), 177 f.

36 So auch die h. M., vgl. BSK StPO-*Jean-Richard-dit-Bressel* (Fn. 15), Art. 269, N 24.

Spezielle Probleme ergeben sich etwa dann, wenn eine Überwachung eines bestimmten Anschlusses aus technischen Gründen nicht wie bei der klassischen Telefonie durch ein Mithören oder eine Aufzeichnung der Gespräche in der Leitung möglich ist. Das Problem ergibt sich bei den in der Praxis häufigen sog. nutzerorientierten oder user-based P2P-Internet-Telefonangeboten wie Skype, die nicht zentralisiert (oder computer-based) und mit Verschlüsselungstechnik funktionieren. Sie nutzen das weltweite Netz in der Weise, dass alle Computer, die Skype benutzen, gleichzeitig in einer «Client and Server»-Funktion eingesetzt werden. Das Telefongespräch wird verschlüsselt und dann – wie etwa auch die E-Mail-Kommunikation – in Datenpaketen durchs Netz geschickt. Da der Inhalt grundsätzlich erst wieder am Endgerät des Nutzers entschlüsselt und zu einem sinnvollen Kommunikationsvorgang zusammengefügt wird, kann das Gespräch nicht in der Leitung, sondern muss möglichst nahe oder allenfalls direkt an den zu überwachenden Endanschlüssen zu Beweiszwecken aufgezeichnet werden.[37]

Technisch funktioniert dies, indem entweder ein Provider kooperiert oder die Strafverfolgungsbehörden Spy-ware einsetzen, welche entschlüsseln oder direkt ein Mikrofon am Computer eines Verdächtigten manipulieren kann, einsetzen. Die Installation solcher Programme auf einem Computer öffnet aber eben nicht nur die Tür zur Telefonüberwachung, sondern bedeutet je nach technischer Machart eines Trojaners, dass vielfältige weitere Massnahmen möglich sind, etwa auch eine Aktivierung der an einem Computer angebrachten Kamera zur Wohnraumüberwachung oder eine Durchsuchung aller auf dem Computer gespeicherten Dateien.[38] Über sog. Malware könnten ferner neben den für eine Überwachungsaktion notwendigen Datenprogrammen auch noch andere Datensätze auf einen Computer geschleust werden.[39]

Der Umstand, dass die derzeit benutzte Spy-ware nach Aussage von Experten technisch nicht auf bestimmte Überwachungsmöglichkeiten begrenzt werden kann, ist ein Grund dafür, dass der Einsatz von «GovWare» aus strafprozessualer Sicht als sehr fragwürdig erscheint.[40] Denn selbst wenn Spy-ware – wie in der hier geschilderten Fallkonstellation – im Rahmen einer an sich zulässigen Telefonüberwachung eingesetzt würde, so eröffneten sich aufgrund der technischen Struktur der Datenprogramme, die als Spy-ware funktionieren, unzulässige Manipulationsmöglichkeiten am infiltrierten Computer. Für ein solches Vorgehen fehlt derzeit eine Ermächtigungsgrundlage. Lausch- und Spähangriffe nach Art. 280 oder

37 *Brunst* (Fn. 22), N 855 ff.; *Brodowski/Freiling* (Fn. 21), 143 ff. sowie 194 ff.

38 *Hansjakob*, in: Kommentar StPO (Fn. 15), Art. 269, N 14.

39 Zu den verschiedenen Funktionen von «malicious software» (malware) s. [http://en.wikipedia.org/wiki/Malware].

40 Solche Bedenken wurden offensichtlich auch im Vernehmlassungsverfahren zu dem geplanten Art. 270bis StPO geäussert, vgl. Medienmitteilung des EJDP zur Revision von BÜPF und VÜPF vom 26. 8. 2011.

Art. 282 f. StPO, die ein breites Spektrum von Massnahmen eröffnen, erlauben gleichwohl keine aktiv durch die Behörden durchgeführte heimliche Durchsuchung eines Datensystems. Das gilt umso mehr, wenn diese mithilfe einer Manipulation im System zudem eine fortgesetzte Überwachung in der virtuellen resp. unter gewissen Umständen sogar in der realen Welt (heimliche Wohnraumüberwachung) ermöglicht.[41] Die durch den Ermittlungseingriff erlangten Informationen erscheinen darüber hinaus in ihrem Beweiswert fragwürdig, wenn mithilfe von Spy- oder Malware etwa auch Daten auf einen Computer geschleust werden können.[42]

3. Abruf sog. Randdaten/Vorratsdatenspeicherung

Bei dem Abruf sog. Randdaten geht es nicht um eine staatliche Kontrolle des *Inhalts* einer Kommunikation, sondern um eine Registrierung des Kommunikationsvorganges an sich. Als Randdaten werden die Informationen über einen elektronischen Kommunikationsvorgang bezeichnet, die nicht den Inhalt betreffen. Sie umfassen die Nummer des Anrufers oder des Angerufenen, den Zeitpunkt und die Dauer des Gesprächs, die IMEI-Nummern (International Mobile Equipment Identity, eindeutige Identifikation des Geräts), die IMSI-Nummern (International Mobile Subscriber Identity, eindeutige Identifikation der SIM-Karte) sowie bei Mobiltelefonen zusätzlich den Standort des Gesprächsteilnehmers oder bei Zugang zum Internet das Einloggen über eine IP-Adresse.[43] Randdaten geben ganz unterschiedliche Informationen über den Kommunikationsvorgang. Die Verbindungsranddaten verraten unter anderem, welcher Anschluss wann und wie lange mit welchem anderen Anschluss verbunden war – und wo ein Mobiltelefon zu einem bestimmten Zeitpunkt benutzt wurde.

Der nachträgliche Abruf der Randdaten bei den Telefondienstanbietern, die als Internet-Accessprovider fungieren,[44] ist heute unter den Vorgaben des Art. 273 StPO zulässig. Der Inhalt einer Kommunikation darf aber, selbst wenn dieser inklusive Randdaten regelmässig ebenfalls beim Dienstanbieter gespeichert

41 *Pieth* (Fn. 28), 132; *Jaggi* (Fn. 31), 10, Anm. 58; *Hansjakob* (Fn. 5), Rz. 17 f.; ebenso aus österreichischer Sicht: *Zerbes* (Fn. 31), 834 ff.

42 Vgl. a. deutsches Bundesverfassungsgericht, Entscheidung, Band 120, 274, 320 f., sowie zur Möglichkeit, damit Daten auf fremden Computern zu platzieren: *Brodowski/Freiling* (Fn. 21), 119: Analysebericht des CCC vom 8. 10. 2011, 5 und 15 [http://www.ccc.de/].

43 *S. de Saussure,* Le IMSI-Catcher: fonctions, applications pratiques et légalité, Jusletter v. 30. 11. 2009, Rz 19; *M. Bisges,* Voraussetzungen der Auskunft bei Providern über ihre Kunden anhand von IP-Adressen, wistra 2009, 303 ff.

44 Dazu etwa: *Hansjakob* (Fn. 34), 265–283.

wird, auf der Grundlage dieser Ermächtigungsgrundlage nicht herausgefordert werden.[45]

Die Randdaten selbst können derzeit sechs Monate rückwirkend verlangt werden (Art. 273 Abs. 3 StPO). Deshalb müssen die Anbieterinnen für Telefondienste, wie schon zuvor unter Geltung des BÜPF, die Daten vorrätig halten. Das ist die – in manchen europäischen Staaten sehr umstrittene, mittlerweile aber durch EU-Recht festgelegte – «Vorratsdatenspeicherung».[46] Die vorgeschlagene Revision des BÜPF sieht eine Speicherungsdauer von zwölf Monaten vor (s. u. III.1.).[47]

Aus Sicht des Gesetzgebers greift diese Überwachung in viel geringerem Masse in die Kommunikationsfreiheit ein als die Überwachung der Inhalte nach Art. 269–279 StPO.[48] Deshalb ist der Abruf sog. Randdaten ohne Beschränkung auf bestimmte Katalogtaten nach richterlicher Genehmigung bei allen Verbrechen und Vergehen sowie bei einer Übertretung gemäss Art. 279^{septies} StGB zugelassen, allerdings nur, wenn dringender Tatverdacht besteht.[49]

Ob der Grundrechtseingriff bei einer Erhebung von Randdaten tatsächlich erheblich geringer ist als bei einer Inhaltsüberwachung, hängt zum einen davon ab, was zu den Randdaten gezählt wird. Wenn zu ihnen beispielsweise die Betreffzeile einer E-Mail gezählt würde,[50] so kommt dies substanziell einer Kommunikationsüberwachung gleich.[51] Zum anderen ist von Bedeutung, wie die rückwirkende Erhebung von Daten strafprozessual verwendet wird: Wird die Randdatenerhebung etwa dafür genutzt, um nachträglich und ohne konkreten Tatverdacht ein Bewegungsbild einer Person zu erstellen, um beispielsweise einem Diebstahlsverdächtigen weitere in den vergangenen Monaten begangene Einbruchdiebstähle anzulasten, dann erlangt diese Datensammlung eine neue Bedeutung. Vor diesem Hintergrund erschliesst sich die Problematik des sog. Antennensuchlaufs, der den Randdatenabruf letztlich zur Fahndungsmethode umfunktioniert.[52]

45 BGer vom 3. 11. 2011 1B_376/2011, E. 5.2; *Hansjakob,* in: Kommentar StPO (Fn. 15), Art. 273, N 7; *Heimgartner* (Fn. 11), 179; *Aepli* (Fn. 17), 19 (zum BÜPF a. F.).

46 Richtlinie 2006/24/EG vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, ABl. L 105 vom 13. 4. 2006, 54; zur Harmonisierungswirkung von EU-Recht vgl. *S. Gless,* Internationales Strafrecht, Grundriss für Studium und Praxis, Basel 2011, Rn. 444 ff.

47 Art. 23 des Vorentwurfes, [http://www.bfm.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/entw-d.pdf].

48 Botschaft StPO (Fn. 24), 1085 ff., 1250.

49 Vgl. dazu ausf. BGer vom 3. 11. 2011, 1B_376/2011, E. 6.

50 BSK StPO-*Jean-Richard-dit-Bressel* (Fn. 15), Art. 273, N 5.

51 Vgl. auch die Botschaft zum BÜPF, BBl 1998 4268.

52 Vgl. dazu BGer vom 3. 11. 2011 1B_376/2011; *Gless,* Heimliche Ermittlungsmassnahmen im Schweizer Recht, ZStR 124 (2012) im Erscheinen.

4. Verdeckte Ermittlungen im Internet

Das Internet bietet viele verschiedene Kommunikationsräume. Das Spektrum reicht von öffentlich zugänglichen Informationen auf Homepages bis hin zu Foren, in denen in Echtzeit Informationen zwischen beliebigen Personen ausgetauscht werden können. Dieser sog. Chat kann über unterschiedliche Plattformen abgewickelt werden: Chaträume bieten – öffentlich zugänglich, mit Registrierung oder geschlossen organisiert, themenbezogen oder thematisch offen – Gelegenheit zur Kommunikation mit Unbekannten. Der Chat ist zumeist anonym resp. pseudonym und flüchtig. Die Teilnehmer treten oft nicht unter ihrem bürgerlichen Namen auf. Anders als etwa bei Facebook, wo sich «Freunde» austauschen und man die Idee der Identität des Gegenübers aufrecht erhält, bieten offene Chats für jedermann die Gelegenheit, die Realität hinter sich zu lassen und als eine andere Person aufzutreten. Diese Möglichkeit haben natürlich auch Personen erkannt, welche die (scheinbare) Anonymität für Straftaten nutzen wollen.

Umstritten ist, ob resp. in welcher Form in den verschiedenen Räumen Strafverfolgungsbehörden oder Polizei ohne besondere Vorkehrungen Informationen zur Strafverfolgung sammeln dürfen.

Nach allgemeiner Meinung sind Streifenfahrten der Polizei durch die öffentliche virtuelle Welt in gleicher Weise erlaubt, wie in der realen Welt eine Observation im Vorbeigehen auf öffentlichem Grund zulässig ist. Dementsprechend dürfte die Polizei öffentliche Kommunikationsräume, wie etwa nicht zugangsgesicherte Homepages, Blogs oder Chatrooms, ohne Weiteres besuchen und dort Daten sichern, jedenfalls solange sie nicht aktiv in die Kommunikation eingreift.[53]

Eine andere Bewertung ergibt sich bei einer Ausdehnung der polizeilichen Beobachtung, welche rund um die Uhr, während Wochen und Monaten gezielt stattfindet.[54] Art. 282 StPO gestattet der Polizei, bis zu einem Monat selbstständig zu observieren.[55] Will die Polizei die Massnahme verlängern, benötigt sie die Genehmigung der Staatsanwaltschaft (Abs. 2).

Eine gezielte Kontaktsuche ist ohnehin nicht mehr als Streifenfahrt, sondern als verdeckte Ermittlung zu klassifizieren, die den Vorgaben des Art. 286 ff. StPO genügen muss. Als verdeckte Ermittlung gilt nach BG-Rechtsprechung «jedes Anknüpfen von Kontakten mit einer verdächtigen Person zu Ermittlungszwecken durch einen nicht als solchen erkennbaren Polizeiangehörigen ungeachtet des Täuschungsaufwandes und der Eingriffsintensität».[56] Das Bundesgericht hat damit

53 *Heimgartner* (Fn. 11), 183; *Bischoff/Lanter* (Fn. 4), Rz. 45 ff.

54 Botschaft StPO (Fn. 24), 1085 ff., 1252.

55 Im Entwurf war die Frist noch auf zwei Wochen beschränkt, vgl. Botschaft StPO (Fn. 24), 1085 ff., 1253.

56 BGer 6B.743/2009 und 6B.837/2009 (Urteile vom 8. März 2010), E. 3.1.

der Meinung, die zwischen «weniger qualifizierten» verdeckten Abklärungen und «echten» verdeckten Ermittlungen unterscheiden wollte, eine Absage erteilt.[57] Diese Grundsätze gelten grundsätzlich ebenso für Ermittlungen im Internet. Das Argument, dass im Rahmen einer Kommunikation im Chat ohnehin kein berechtigtes Vertrauen entsteht, dass sich hinter einem Pseudonym (cherry15) die im Profil angegebene Person (Charlène, 15 Jahre, WBS-Schülerin) und nicht ein 40-jähriger Verkäufer oder eben die Polizei verbirgt, greift nicht durch. Denn auch die Pseudonymität eines Profils suggeriert eine bestimmte Identität. Wenn ein Polizist eine nicht offene Ermittlung durch ein Pseudonym verheimlicht und hinter diesem Deckmantel eine Kommunikation aufnimmt, dann ist dies mit Blick auf die Verfahrensstellung des Beschuldigten und für das System der «checks and balances» in der StPO problematisch.[58] Denn der beschuldigten Person bleibt verborgen, dass sie sich in einem «verdeckten Verhör» gegenüber den Verfolgungsbehörden äussert. Sie ist nicht in der Lage, autonom zu entscheiden, wie sie in einem Kontext reagieren will, in dem Fantasie, Virtualität und Realität eng aneinandergrenzen.[59] Hinzu kommt die Gefahr, dass bei der verdeckten Ermittlung die Grenzen zulässiger Einwirkung überschritten werden. Verdeckte Ermittler dürfen weder Straftaten provozieren noch die Tatbereitschaft wecken. Eine nicht offene, unter einem Pseudonym geführte Ermittlung in einem Chat fällt damit unter das Regime der Vorschriften über verdeckte Ermittlungen gemäss Art. 269 ff. StPO.

III. Herrschaft des Rechts oder Primat der Technik?

Obwohl die Schweizer Strafprozessordnung derzeit bereits verschiedenste Ermächtigungsgrundlagen bereithält, die eine Beweissammlung im Internet ermöglichen, stellen sich mit der technischen Weiterentwicklung des Internets immer wieder neue Fragen in Zusammenhang mit strafrechtlichen Ermittlungen.

1. Einsatz sog. Staatstrojaner oder GovWare

Vor dem Hintergrund der technischen Weiterentwicklung ist die Initiative des EJDP zu verstehen, die in Zusammenhang mit einer Totalrevision des BÜPF[60]

57 *S. Gless,* Anmerkung zu 6B_837/2009, Urteil vom 8.3.2010, forumpoenale 2011, 30 f., *L. Vetterli,* Gesetzesbindung im Strafprozess, Zürich u.a. 2010, 167 ff.

58 *Bischoff/Lanter* (Fn. 4), Rz 48 ff.

59 Vgl. dazu mit Blick auf die Geltung von *nemo tenetur: Gless* (Fn. 15), Art. 140 StPO, N 8; *P. Albrecht,* Zur rechtlichen Problematik des Einsatzes von V-Leuten, AJP 2002, 633.

60 Vorentwurf zur Änderung des BÜPF vom 30.4.2010, [http://www.bfm.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/entw-d.pdf].

eine Rechtsgrundlage für den Einsatz sog. Trojaner oder (um neutrale Sprache bemüht) sog. GovWare[61] vorschlug. Danach sollte die StPO unter anderem um folgende Regelung ergänzt werden:

> *«Art. 270bis Abfangen und Entschlüsselung von Daten*
>
> *1 Sind bei einer Überwachung des Fernmeldeverkehrs die bisherigen Massnahmen erfolglos geblieben oder wären andere Überwachungsmassnahmen aussichtslos oder würden die Überwachung unverhältnismässig erschweren, so kann die Staatsanwaltschaft auch ohne Wissen der überwachten Person das Einführen von Informatikprogrammen in ein Datensystem anordnen, um die Daten abzufangen und zu lesen. Die Staatsanwaltschaft gibt in der Anordnung der Überwachung an, auf welche Art von Daten sie zugreifen will.*
>
> *2 Die Anordnung bedarf der Genehmigung durch das Zwangsmassnahmengericht.»*

Diese Regelung ist Teil einer Gesamtrevision des BÜPF, welche die Behörden – quasi dynamisch – in die Lage versetzen soll, Kommunikation im Internet zu kontrollieren. Die neuen Regelungen wollen deshalb insgesamt eine sich weiterentwickelnde, dem jeweiligen Stand der Technik angepasste Überwachung von netzbasierten Kommunikationsvorgängen ermöglichen, welche zudem die technische Umsetzung und die Kosten den jeweiligen Dienstanbietern überbürdet.[62] Obwohl das Grundanliegen der Kontrolle des Internets wohl weitgehend Zustimmung findet, traf der konkret vorgelegte Reformvorschlag aus verschiedensten Gründen auf breiten politischen und gesellschaftlichen Widerspruch.[63] Der Bundesrat hat deshalb Ende November 2011 beschlossen, einen neuen Gesetzesvorschlag für den Einsatz von sog. GovWare auszuarbeiten.[64]

Betreffend den Einsatz von «Spy-ware» oder «Malware» ist jedoch ganz unabhängig von der Frage der derzeit noch fehlenden Ermächtigungsgrundlage jedenfalls problematisch, dass – soweit bekannt – die von Behörden eingesetzten

61 Medienmitteilung «Post- und Fernmeldeüberwachung: Klare und restriktive Rechtsgrundlagen» vom 23.11.2011; *Hansjakob* (Fn. 5), Rz. 4 ff.

62 Vgl. Art. 21 ff. des Vorentwurfes sowie den Erläuternden Bericht zur Änderung des BÜPF no. 1.4.6 und no. 2.5 [http://www.admin.ch/ch/d/gg/pc/documents/1719/Bericht.pdf], zur teilweisen Revision dieser Vorschriften vgl. Medienmitteilung vom 23.11.2011 (Fn. 61).

63 Hier treffen unterschiedlichste Interessen aufeinander: wirtschaftliche Interessen der Provider, Freiheitsinteressen von Internetakteuren, Bedenken von liberalen politischen Kreisen gegenüber invasiven Überwachungseingriffen, vgl. *C. De la Cruz/C.-A. Gordon,* Eine Revision durch die Hintertür, und *T. Hansjakob,* Staatsanwälte sind keine Big Brothers, beide NZZ vom 10.8.2011, 9, sowie aus strafprozessualer Sicht den Erläuternden Bericht zur Änderung des BÜPF vom 6.10.2000 no. 2.10; BBl 2000 5128–5141 [http://www.admin.ch/ch/d/gg/pc/documents/1719/Bericht.pdf], besucht am 3.9.2011; aus grundrechtlicher Sicht: *J. P. Müller/M. Schefer,* Grundrechte in der Schweiz – Im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte, 4. Aufl., Bern 2008, 172 f.

64 Medienmitteilung «Post- und Fernmeldeüberwachung: Klare und restriktive Rechtsgrundlagen» vom 23.11.2011.

Datenprogramme derzeit wohl technisch nicht auf die Überwachung eines Kommunikationsvorgangs oder die Überprüfung bestimmter Dateien begrenzt werden können.[65] Die einschlägigen Datenprogramme öffnen je nach technischer Ausgestaltung nicht nur jede auf dem infiltrierten Computer gespeicherte Information für die Behörden, sondern es werden weitere Manipulationen technisch möglich, wie etwa die Aktivierung von Mikrofonen und Kameras oder sogar die Installation von Datenbeständen auf einem Computer.[66] Vorgaben in einer Ermächtigungsgrundlage, etwa eine Durchsuchung auf bestimmte Dateien zu begrenzen, auf welche die Staatsanwaltschaft zugreifen will, wirken nur dann begrenzend, wenn ein solcher Zugriffswille technisch implementiert werden kann. Das ist der Fall, wenn eine «Spy-ware» gezielt zum Auffinden bestimmbarer Dateien oder zur Überwachung bestimmter Kommunikationsvorgänge eingesetzt werden kann. Nur dann ist die Herrschaft des Rechts über die Technik gewährleistet, andernfalls besteht die Gefahr nicht kontrollierbarer Ermittlungseingriffe. Dass der Gesetzgeber angesichts invasiver Überwachungsmöglichkeiten hoheitliche Ermittlungsrechte begrenzen will, kommt etwa in der Botschaft zur StPO in Zusammenhang mit Art. 279 StPO klar zum Ausdruck: Der Einsatz technischer Überwachungsgeräte ist nur bei genauer Festlegung des intendierten Zwecks zulässig.[67]

Insgesamt zeigt die Diskussion um den Einsatz von «Staatstrojanern» oder «GovWare», wie schwierig es ist, angesichts neuer technischer Überwachungsmöglichkeiten in der rechtspolitischen Diskussion darauf zu beharren, dass nicht immer das gerade technisch Mögliche, sondern das Bestreben um das rechtlich Zulässige und das Sinnvolle die Debatte bestimmen sollte.[68]

2. Regelung neuer Ermittlungsmassnahmen im Internet

Auch jenseits des Einsatzes von «Trojanern» stellen sich in Zusammenhang mit der Weiterentwicklung der Strafverfolgungsmassnahmen im Internet immer wieder neue Fragen. Denn das Reservoir technisch möglicher Ermittlungsinstrumente scheint fast unbegrenzt; für die Zukunft wäre etwa ein zuständiges Moni-

65 So jedenfalls die Analyse des Chaos Computer Clubs, dem eine Spy-ware resp. Schadenssoftware zugespielt wurde, die vermutlich von einer deutschen Behörde auf einem privaten Computer installiert wurde [http://www.ccc.de/], Mitteilung vom 8. 10. 2011.

66 Vgl. dazu etwa die Berichterstattung in der «Zeit» vom 12. 10. 2011 [http://www.zeit.de/digital/datenschutz/2011-10/trojaner-software].

67 Botschaft zur Vereinheitlichung des Strafprozessrechts vom 21. 12. 2005, BBl 2005, 1085 ff., 1252; vgl. a. *Müller/Schefer* (Fn. 63), 172 f.

68 Der Weg für eine solche Diskussion scheint bereits jetzt vorgezeichnet, wenn durch die Ausgestaltung der Ermächtigungsgrundlage Einfallstore für das technisch Mögliche geschaffen werden, vgl. dazu *Hansjakob* (Fn. 5), Rz. 23 f.

toring der Internetnutzung durch bestimmte Personen oder Personengruppen denkbar oder eine Speicherung aller Zahlungsvorgänge im Internet mit der Hilfe von Kreditkartenunternehmen.

Damit nicht bei jeder technischen Fortentwicklung ad hoc über Zulässigkeit und Grenzen heimlicher Überwachung entschieden werden muss, bedarf es akkordierter Grundsätze darüber, wie der Einsatz neuer Ermittlungsmassnahmen im Internet künftig zu regeln ist. Folgende Grundsätze sollten bei der Schaffung neuer Vorgaben für Ermittlungsmassnahmen im Internet beachtet werden:

(1) Neue Ermächtigungsgrundlagen sind formal so zu fassen, dass daraus klar hervorgeht, welche konkreten Strafverfolgungsmassnahmen auf dieser Grundlage zulässig sind. Dies fordert bereits der in Art. 36 BV verankerte Bestimmtheitsgrundsatz. Der vorgesehene Art. 270bis StPO würde diesen Anforderungen nicht genügen, da weder konkret festgelegt wird, wann andere Massnahmen erfolglos, aussichtslos oder unverhältnismässig wären, noch definiert ist, welche Daten im Einzelfall abgefangen und gelesen werden dürfen.

(2) Inhaltlich muss der Gesetzgeber bei der Ausgestaltung der Ermächtigungsgrundlagen nicht nur den Sicherheitsanliegen der Allgemeinheit, sondern ebenfalls den Freiheiten und Rechten der Einzelnen Rechnung tragen.[69] Letzteres ist in zweierlei Hinsicht von Bedeutung:

Zum einen dürfen Rechtsgemeinschaft und Beschuldigte grundsätzlich erwarten, dass strafprozessuale Ermittlungen offen und nicht heimlich geführt werden, und zwar auch bei Verdacht auf Straftaten im Internet[70]. Denn nach den Vorgaben der StPO ist das Vorverfahren parteiöffentlich: Beschuldigte sind über die ihnen zur Last gelegten Tatvorwürfe zu orientieren; ihnen muss rechtliches Gehör und Akteneinsichtsrecht gewährt werden.[71] Diese Rechte haben nicht ausschliesslich individualschützenden Charakter, sondern dienen genauso der Zuverlässigkeit der Ermittlungen, denn sie eröffnen die Möglichkeit, dass Verdächtigte eine Ermittlungshypothese der Strafverfolgungsbehörden allenfalls entkräften können.[72] Wenn die Ermittlungen insgesamt heimlich ablaufen, wird diese Möglichkeit vergeben. Diese Gefahr besteht gerade bei Online-Überwachungen, bei der grosse Mengen von Daten kontrolliert werden müssen, ohne dass der Dateninhaber deren Existenz oder Bedeutung gegenüber den Behörden erläutern kann.

69 Etwa mit Blick auf die Einschränkung des Brief- und Fernmeldeverkehrs: *Müller/Schefer* (Fn. 63), 214 ff.

70 Dazu ausf.: *I. Zerbes,* Spitzeln, Spähen, Spionieren. Sprengung strafprozessualer Grenzen durch geheime Zugriffe auf Kommunikation, Wien et al. 2010, 43 ff.

71 *Pieth* (Fn. 28), 74 ff.

72 BSK StPO-*Gless* (Fn. 15), Art. 139 StPO, N 11 und 48.

Zum Zweiten muss der Gesetzgeber bei Ermittlungen im Internet sicherstellen, dass die durch die StPO garantierten Verteidigungsrechte sowie Aussage- und Zeugnisverweigerungsrechte nicht durch heimliche Überwachung faktisch umgangen werden.[73] Die Aushöhlung dieser Verfahrensrechte wird in der Literatur bereits heute angesichts eines immer weiter gehenden Ausbaus von nicht offenen Ermittlungsmethoden moniert.[74]

(3) Ferner ist bei der Formulierung von Ermächtigungsgrundlagen zur Überwachung im weltweiten Netz immer zu beachten, dass für Bürgerinnen und Bürger bei der Computer- oder Internetnutzung eine vor staatlichen Eingriffen geschützte Intimsphäre bestehen bleiben muss.[75] Denn auch als Internetnutzer hat der Einzelne ein Recht, im privaten Bereich alleine gelassen zu werden, wenn nicht eine besondere Berechtigung des Staates existiert, in diese Sphäre einzudringen. Strafprozessuale Ermächtigungsgrundlagen, welche eine unverhältnismässig weit gehende Überwachung erlauben und damit quasi Internetbenutzer unter einen Generalverdacht stellen[76] oder bestimmte Gruppen durch umfassende Überwachung zu gläsernen Menschen machen würden, sind unzulässig.[77] Hier stellt sich eine der schwierigsten Fragen im Zusammenhang mit der Strafverfolgung im Internet allgemein und im Zusammenhang mit der Online-Durchsuchung im Besonderen: Wo genau verläuft im virtuellen Raum die Grenze zwischen einer öffentlichen, einer privaten und einer vor Strafverfolgungseingriffen absolut geschützten intimen Sphäre?

Bisher haben weder die staatlichen Behörden, die Netzaktivisten, noch die Rechtswissenschaftler oder die Akteure des Internets darauf eine befriedigende Antwort gegeben.[78] Eine solche ist aber Voraussetzung für eine adäquate Regelung der Strafverfolgung im Internet. Die Strafrechtswissenschaft hat ihre Bewertung bisher oft an formalen, technischen Abläufen der Kommunikation orientiert und sich wenig mit der Frage einer berechtigten oder unberechtigten Erwartung vertraulicher resp. nicht staatlich überwachter Kommunikation im Internet sowie mit der Frage einer absolut geschützten Intimsphäre auseinandergesetzt. Sie ist sich

73 *Zerbes* (Fn. 70), 99 ff.

74 *Pieth* (Fn. 28), 135; *Albrecht* (Fn. 58), 633.

75 Dogmatisch kann sich diese Forderung unter anderem auf Art. 3 StPO stützen, vgl. dazu BGE 127 I 6, E. 5.b mit Hinweis auf *J. P. Müller,* Grundrechte (3. Aufl.), 4 f.; BSK StPO-*M. Thommen* (Fn. 15), Art. 3, N 11.

76 Zu der in Art. 10 verankerten Unschuldsvermutung: BSK StPO-*E. Tophinke/T. Hofer* (Fn. 15), Art. 10, N 1.

77 Vgl. dazu: *W. Hoffmann-Riem,* Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, 1012 ff.

78 Dazu etwa die Diskussion um einen Anspruch auf Anonymität und dessen Aufhebung und Einschränkung im Internet bei *Brunst* (Fn. 6), 407 ff.; *T. Hoeren,* Anonymität im Web – Grundfragen und aktuelle Entwicklungen , ZRP 2010, 251 ff.; *B. Rudin,* Das Recht auf Anonymität, digma 2008, 6 ff.

aber der Problematik bewusst.[79] Gerade die Diskussion um den Einsatz von Spyware und die Möglichkeit der Online-Durchsuchung zeigt, dass es auch in der virtuellen Welt Grenzen für die Strafverfolgung geben muss, die sich durchaus an einem bereits in der realen Welt gefundenen Konsens orientieren können. So würde beispielsweise niemand eine Ermächtigung der Strafverfolgungsbehörden zum Einbruch in die Wohnung eines Beschuldigten zum Zwecke der heimlichen Durchsuchung mit Installation von Mikrofonen und Kameras gutheissen, über die darüber hinaus noch Material in die Sphäre des Beschuldigten gelangen könnte, sodass die Grenzen zwischen Ermittlungsmassnahme und Ermittlungsergebnis zu verschwimmen drohten.[80]

Die Problematik der Grenzziehung zwischen einer öffentlichen, einer Privat- und einer vom Staat nicht infiltrierten Intimsphäre bestimmt auch in anderen Staaten die Diskussion,[81] beispielsweise im benachbarten Deutschland:[82] Hier bestätigte das Bundesverfassungsgericht[83] in einem Urteil über eine Gesetzgebung zur Online-Durchsuchung, dass das deutsche Grundgesetz die Vertraulichkeit und Integrität informationstechnischer Systeme, insbesondere vor einem heimlichen Zugriff, grundrechtlich schütze.[84] Eine heimliche Infiltration eines informationstechnischen Systems sei nur dann zulässig, wenn tatsächliche Anhaltspunkte für eine konkrete Gefahr im Hinblick auf ein überragend wichtiges Rechtsgut bestünden, etwa für Leib und Leben für Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand der Existenz des Staates berührten.[85] In diesem Falle sei die Überwachung aber immer auf Daten aus einem laufenden Telekommunikationsvorgang zu beschränken, selbst wenn eine weiter gehende Kontrolle durch von den Behörden eingesetzte Trojaner grundsätzlich möglich wäre. Ansonsten sei eine solche staatliche Massnahme nicht zulässig.[86]

79 Vgl. zur Bedeutung der Privatsphäre etwa: *Jaggi* (Fn. 31), 2; *Schmid,* Handbuch (Fn. 27), vor Art. 269–279, Rn. 1.

80 Vgl. dazu: *Müller/Schefer* (Fn. 63), 172 f. und 206, sowie *M. Kutscha,* Verdeckte «Online-Durchsuchung» und Unverletzlichkeit der Wohnung, NJW 2007, 1169 ff.

81 Aus österreichischer Sicht: *Zerbes* (Fn. 70), 43 ff.

82 Vgl. dazu Frankfurter Allgemeine Sonntagszeitung vom 9.10.2011, 41; *M.-T. Tinnefeld,* Online-Durchsuchung – Menschenrechte vs. virtuelle Trojaner, MMR 2007, 137; *Kudlich* (Fn. 6), 195; *W. Beulke/F. Meininghaus,* StPO, §§ 102 ff.; GG Art. 2 Abs. 1, 13 Abs. 2 (Heimliche Online-Durchsuchung eines PC), StV 2007, 60 ff.; *Buermeyer* (Fn. 5), 154 ff.; *Gaede* (Fn. 11), 98; *M. Hofmann,* Die Online-Durchsuchung – staatliches «Hacken» oder zulässige Ermittlungsmassnahme?, NStZ 2005, 121 ff.

83 BVerfG Urteil vom 27.2.2008 (1 BVR 370/07, BVR 597/07); dazu etwa: *M. Jahn/H. Kudlich,* Die strafprozessuale Zulässigkeit der Online-Durchsuchung, JR 2007, 57 ff.

84 BVerfG Urteil vom 27.2.2008 (1 BVR 370/07, BVR 597/07), Leitsatz 1.

85 BVerfG Urteil vom 27.2.2008 (1 BVR 370/07, BVR 597/07), Rn. 251; vgl. auch *Klesczewski* (Fn. 9); *Zerbes* (Fn. 31), 834 ff.

86 BVerfG Urteil vom 27.2.2008 (1 BVR 370/07, BVR 597/07), Rn. 190.

IV. Fazit

Nach dem Verständnis unserer Gesellschaft ist das Internet kein rechtsfreier Raum. Vielmehr sollen dort in gleicher Form strafbewehrte Verhaltensvorgaben gelten wie in der realen Welt. Die Fragen nach der Legitimation der Rechtsetzung und nach der faktischen Möglichkeit der gleichmässigen Rechtsdurchsetzung im World Wide Web sind jedoch längst nicht alle beantwortet. Hinzu kommt, dass bestimmten Verhaltensweisen in der virtuellen Welt eine andere Bedeutung zugeschrieben werden als in der realen Welt, so ist etwa das Kommunikationsverhalten im Internet nicht ohne Weiteres mit dem Kommunikationsverhalten in der realen Welt gleichzusetzen. Begegnungen und Austausch im Netz – zum Beispiel in einem Chat – haben eine andere soziale Bedeutung als die Interaktion mit dem körperlich präsenten Gegenüber.

Deshalb herrschen jenseits der Einigkeit über das Ob einer Strafverfolgung im Internet noch viele Zweifel über die Einzelaspekte des Wie. Bei der Lösung der Zweifelsfragen muss sich die Strafrechtswissenschaft den neuen Fragen einer Strafverfolgung im virtuellen Raum stellen. Sie hat die Aufgabe, die Praxis von Behörden, neue Gesetzgebungsvorschläge und vorhandenes Recht in seinen Auswirkungen auf das Strafverfahren zu untersuchen und allenfalls Einwände zu erheben, wenn tradierte Grundsätze des Strafverfahrens schleichend erodiert werden, etwa die grundsätzliche Vorgabe der StPO, dass Strafermittlungen offen und nicht heimlich zu führen sind und dass es für jede Zwangsmassnahme einer gesetzlichen Grundlage bedarf.

Wer das Internet nicht sich selbst überantworten will, kann nicht in Abrede stellen, dass der Einsatz neuer Ermittlungstechniken notwendig ist, damit die virtuelle Welt kontrollierbar oder zumindest kontrollierbarer wird. Wenn Strafverfolgungsbehörden als Hoheitsträger im weltweiten Netz ermitteln, sind sie jedoch weiter an ihre nationale Rechtsordnung, an die für sie einschlägigen, demokratisch legitimierten Normen gebunden und werden von der Rechtsgemeinschaft daran gemessen.

Künftig sollte sich die Strafrechtswissenschaft deshalb für gesetzliche Vorgaben einsetzen, welche notwendige Ermittlungsmassnahmen im Internet auf die Grundlage klar formulierter Ermächtigungsgrundlagen stellen und den Einsatz neuer Ermittlungstechniken zielorientiert begrenzen. Diese gesetzlichen Vorgaben müssen sich an der Richtschnur offener Ermittlungen orientieren und heimliche Kontrollmassnahmen als Ausnahme behandeln sowie die im Strafverfahren verbürgten Verfahrensrechte von Beschuldigten und anderen Betroffenen adäquat berücksichtigen. Darüber hinaus ist es Aufgabe der Strafrechtswissenschaft, darauf hinzuwirken, dass strafprozessuale Ermächtigungsgrundlagen einen unantastbaren Kern der Persönlichkeitssphäre respektieren, und dafür einzustehen, dass das Recht nicht in Wechselwirkung mit dem Internet zum gläsernen Menschen führt.