

Zürich, 20. Februar 2014

Matthias Brunner
Viktor Györfly
Claude Hentz
Kim Mauerhofer
Peter Nideröst
Antigone Schobinger
Lisa Zaugg

Einschreiben

Dienst Überwachung

Post- und Fernmeldeverkehr

Informatik Service Center ISC-EJPD

3003 Bern

Viktor Györfly

Rechtsanwalt

Gartenhofstrasse 15
Postfach 9819
8036 Zürich
Telefon 044 240 20 55
Telefax 044 241 24 02
gyoerffy@advogar.ch
MwSt-Nr. 521 641

D St

Sehr geehrte Damen und Herren

Namens und im Auftrag von stelle ich Ihnen das

Gesuch

mit folgenden

Anträgen:

1. Die sei anzuweisen, die
gemäss Art. 15 Abs. 3 ÜPF gespeicherten Ver-
kehrs- und Rechnungsdaten des Gesuchstellers
zu löschen und deren Speicherung in Zukunft
zu unterlassen, soweit die betroffenen Daten
nicht für die Erbringung der vertraglichen
Leistungen gegenüber dem Gesuchsteller zwin-
gend erforderlich sind.
2. Die sei anzuweisen
bzw. zu verpflichten, keine gemäss Art. 15 Abs.
3 ÜPF gespeicherten Verkehrs- und Rech-
nungsdaten des Gesuchstellers an den Dienst
ÜPF oder an andere Behörden oder an Gerichte
herauszugeben;

unter Kosten- und Entschädigungsfolgen zu
Lasten des Staates.

I. Formelles

1. Der unterzeichnende Rechtsanwalt ist zur Vertretung des Gesuchstellers gehörig bevollmächtigt. Eine Kopie der entsprechenden Vollmacht liegt dem Gesuch bei (s. **Beilage 1**).
2. Wer ein schutzwürdiges Interesse hat, kann gemäss Art. 25a VwVG von der Behörde, die für Handlungen zuständig ist, welche sich auf öffentliches Recht des Bundes stützen und Rechte und Pflichten berühren, verlangen, dass sie (a.) widerrechtliche Handlungen unterlässt, einstellt oder widerruft und (b.) die Folgen widerrechtlicher Handlungen beseitigt.
3. Die Speicherung der Daten beschlägt, wie nachstehend dargelegt wird, Grundrechte, welche durch die Europäische Menschenrechtskonvention (EMRK) geschützt sind. Damit muss – in Verbindung mit diesen Grundrechten – auch das Recht auf effektive Beschwerde gemäss Art. 13 EMRK gewahrt sein. Zur Wahrung des Rechts auf effektive Beschwerde ist das Gesuch damit von der zuständigen Behörde materiell zu behandeln und es ist dabei entweder gutzuheissen oder es dem Gesuchsteller im Falle der Ablehnung die Möglichkeit zu gewähren, ein Rechtsmittel an eine Instanz zu ergreifen, welche die Sache wiederum materiell behandelt.
4. Gemäss Art. 15 Abs. 3 des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (nachfolgend: BÜPF) sind die Anbieterinnen von Fernmeldediensten verpflichtet, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten (nachfolgend: Metadaten) während sechs Monaten aufzubewahren.
5. Der Gesuchsteller ist Kunde der (nachfolgend: Anbieterin). Die Anbieterin speichert demnach gestützt auf Art. 15 Abs. 3 BÜPF, d.h. gestützt auf öffentliches Recht des Bundes, während sechs Monaten die erwähnten Metadaten, die bei der Kommunikation des Gesuchstellers anfallen (s. **Beilage 2**).
6. Die Speicherung der Metadaten stellt einen erheblichen und unrechtmässigen Eingriff in die nachstehend (Ziff. II.B.) genannten Grundrechte dar.
7. Die Speicherung der Metadaten durch die Anbieterin berührt somit ein Grundrecht des Gesuchstellers. Es handelt sich bei der Speicherung der Metadaten mithin um eine Handlung i.S.v. Art. 25a VwVG.
8. Das erforderliche schutzwürdige Interesse des Gesuchstellers ergibt sich vorliegend ohne Weiteres aus dem vorstehend erwähnten schweren Eingriff in das durch die Bundesverfassung und die EMRK geschützte Fernmeldegeheimnis.

9. Welche Behörde für die zu beurteilenden Handlungen – und damit zur Behandlung des vorliegenden Gesuchs – zuständig ist, ergibt sich aus den anwendbaren Sach- und Organisationsgesetzen (vgl. ISABELLE HÄNER in: Praxiskommentar zum VwVG, Zürich 2009, Art. 25a, N 30). Vorliegend wird die Speicherung der Metadaten von der Anbieterin, d.h. von einer juristischen Person des Privatrechts, vorgenommen. Diese ist naturgemäss nicht zum Erlass einer Verfügung gemäss Art. 25a VwVG befugt. Zuständig zum Erlass einer Verfügung ist im Bereich der auf Private ausgelagerten Aufgaben vielmehr der Bund bzw. die zuständige Aufsichtsbehörde (vgl. HÄNER, a.a.O., Art. 25a, N 15). Aufsichtsbehörde ist im Fernmeldewesen gemäss Art. 58 des Fernmeldegesetzes vom 30. April 1997 (nachfolgend: FMG) grundsätzlich das Bundesamt für Kommunikation (BAKOM). Im Bereich der Überwachung des Post- und Fernmeldeverkehrs ist jedoch davon auszugehen, dass die Zuständigkeit beim Dienst Überwachung Post- und Fernmeldeverkehr (nachfolgend: Dienst ÜPF) liegt, da diesem gemäss Art. 13 Abs. 1 BÜPF insbesondere die Aufgabe zukommt, Überwachungen anzuordnen und diese bei Wegfall der Rechtmässigkeit einzustellen. Der ÜPF ist somit sachlich und funktionell zur Behandlung des vorliegenden Gesuchs zuständig.
10. Sofern der Dienst ÜPF der Auffassung ist, er sei nicht für die Behandlung des Gesuches zuständig, wird er gestützt auf Art. 8 VwVG ersucht, das Gesuch an die zuständige Behörde weiterzuleiten und den Gesuchsteller darüber zu informieren.

II. Begründung

A. *Regelung und Praxis der Vorratsdatenspeicherung, gespeicherte Daten*

1. Art. 273 StPO sowie die im BÜPF und der entsprechenden Ausführungsgesetzgebung enthaltene Regelung verpflichten verschiedene Anbieter von Kommunikationsdienstleistungen, Daten im Zusammenhang mit den erbrachten Dienstleistungen während 6 Monaten zu speichern (Vorratsdatenspeicherung). Unter den in Art. 273 StPO genannten Voraussetzungen sind diese Daten an die Strafverfolgungsbehörden herauszugeben, gemäss Praxis des Bundesgerichts u.U. auch dann, wenn die Daten länger als sechs Monate aufbewahrt worden sind (BGE 139 IV 98 [1B_481/2012]).
2. Erfasst werden Daten im Zusammenhang mit schriftlicher und mündlicher Kommunikation, in erster Linie bei der Kommunikation in elektronischer Form, aber auch im herkömmlichen Verkehr via Post. Erfasst werden insbesondere Daten, die aus der Kommunikation via Telefon, Mail, Internet und in Briefpostsendungen anfallen.

3. Welche Daten von welchen Anbietern zu speichern sind, erschliesst sich nicht ohne Weiteres. Auf Gesetzesstufe (Gesetz im formellen Sinn) sind die Regelungen in der StPO und im BÜPF festgelegt. Aus dem Studium der entsprechenden Gesetzesartikel wird aber nicht klar, welche Daten von welchen Providern genau erfasst werden müssen. Weitere Regelungen finden sich in der VÜPF, also auf Verordnungsstufe. Die dort enthaltenen Vorschriften machen allerdings auch nicht hinreichend deutlich, was zu erfassen ist. Zudem sind die gesetzlichen Regelungen, einschliesslich jener auf Verordnungsstufe, insgesamt bereits derart abstrakt, dass sich für den Laien nicht erschliesst, was diese im Einzelnen bedeuten. Details sind in Richtlinien geregelt, die im Wesentlichen den ETSI-Standard Lawful Interception umsetzen (vgl. Art. 17 und Art. 25 VÜPF; https://www.li.admin.ch/de/documentation/downloads/trts_oar.html). Diese Richtlinien sind in ihren technischen Details nur für Spezialisten, die entsprechend technisch bewandert sind verständlich, für Laien hingegen nicht. Dazu kommt, dass in der Praxis nicht möglich ist, unter Berufung auf die Auskunftspflicht gemäss Datenschutzgesetz von der Anbieterin entsprechende detaillierte Auskünfte zu erhalten. Den Rechtsunterworfenen ist damit in ganz wesentlichen Aspekten nicht klar, welche Daten überhaupt erfasst werden.
4. Erfasst werden offenbar insbesondere folgende Daten:
 - a) Grunddaten des betreffenden Kunden:
 - Name, Adresse
 - Geburtsdatum
 - Ausweis/Ausweisnummer
 - Beruf
 - Telefonnummer(n)
 - Mail-Adresse(n)
 - Bei Firmen: Firma, Firmennummer (Zefix)
 - Kontaktperson
 - Kunde seit bzw. von/bis
 - b) Telefon:
 - Telefonnummer
 - Telefonnummer der Gegenseite
 - Telefon-Anbieter
 - Telefon-Abo
 - Dauer des Abos
 - Art des Anschlusses
 - Angaben zum Anschlussinhaber, einschliesslich Adresse(n)/ Mail-Adresse(n)
 - Details zu Zahlungen für den Anschluss (Art der Zahlung, Inhaber, Bank, Kontonummern)
 - Details zu Kosten/Zahlung des Gesprächs

- in den Richtlinien wird darauf verwiesen, dass gewisse zusätzliche Informationen, die nicht Bestandteil der Vorratsdatenspeicherung sind, über die strafprozessuale Editionsspflicht erhältlich gemacht werden können, insb. weitere Zahlungsinformationen und gewählte Extensions während des Telefongesprächs (DTMF)
- Zeiten, insb. Beginn und Ende Anruf
- Art der Verbindung/Kommunikation
- Allfällig Umleitungen/Weiterleitungen bei der Kommunikation

zusätzlich bei Anrufen via Festnetz:

- Adresse des Anschlusses
- verwendetes Gerät

zusätzlich bei Anrufen via Mobiltelefon:

- IMSI (auf SIM gespeicherte, eindeutige Nummer)
- IMEI (eindeutige Nummer des Telefongerätes)
- pUK- und pUK2-Code (Codes zum Entsperren der SIM)
- Zeiten, insb. Beginn und Ende der Verbindung zu den im Gespräch genutzten Antennen
- benutzte Antennen einschliesslich Adresse, Nummer und Koordinaten der Antenne, Hauptstrahlrichtung

zusätzlich bei SMS oder MMS:

- Angaben zu Art, Status, Übertragung der SMS bzw. MMS
- Mail-Adresse bei Übertragung via Mail-Gateway

c) Mail:

- Mail-Adressen, inkl. Aliases
- Mail-Konto-Inhaber, einschliesslich Adresse und Mail
- Dauer des Mail-Kontos
- Details zu Zahlungen für das Mail-Konto (Art der Zahlung, Inhaber, Bank, Kontonummern)
- Mail-Adresse Absender
- Mail-Adresse Empfänger
- Zeitangaben zur Übertragung des Mails
- Übertragungsprotokoll, Übertragungsart des Mails (POP, IMAP, Webmail)
- Übertragungsstatus des Mails
- IP-Adressen der kommunizierenden Stellen (z.B. Absender und Mailserver)
- Message ID
- Verbindungsaufnahmen zum Mail-Server

d) Internet:

- Provider

- Internet-Abo
 - IP-Adresse
 - MAC-Adresse (eindeutige Nummer des Gerätes), Lokalisation, Art und weitere Eigenschaften des Modems bzw. Routers und der Auswahl
 - Angaben zum Kunden, einschliesslich Adresse(n)/Mail-Adresse(n)
 - Details zu Zahlungen für das Internet-Abo (Art der Zahlung, Inhaber, Bank, Kontonummern)
 - zusätzlich bei Internet-Verbindungen über Mobilfunk: benutzte Antennen einschliesslich Adresse, Nummer und Koordinaten der Antenne, Hauptstrahlrichtung, benutzter Port
- e) Multimedia (Voice over IP (VoIP)-Telefonie, Videotelefonie, etc.):
- Provider der Multimedia-Kommunikation
 - Telefonnummer, SIP-URI (sofern vorhanden)
 - IMSI (sofern vorhanden)
 - Multimedia-Service-Typ
 - Beginn, Ende und Dauer der Kommunikation
 - Rolle in der Kommunikation
 - Adresse
 - Details zu Zahlungen (Art der Zahlung, Inhaber, Bank, Kontonummern)
 - IP-Adresse, ausgehender Port, Port auf der Gegenseite (auch bei Kommunikation über Mobilfunknetz)
- e) Brief- und Paketpost:
- Angaben zu Absender und Empfänger von Postsendungen (soweit vorhanden)
5. Damit werden in den betroffenen Bereichen systematisch Daten darüber gespeichert, wer mit wem wann kommuniziert, wo sich die in die Kommunikation involvierten Personen aufhalten, teilweise werden auch inhaltliche Daten der Kommunikation erfasst. Je nach Kommunikationsart bzw. -kanal werden aus Anlass eines Kommunikationsvorgangs zahlreiche Daten gleichzeitig erfasst, etwa bei der Nutzung des Internets mit Hilfe eines Mobiltelefons.
6. Sehr viel Kommunikation spielt sich über Kanäle ab, die von der Vorratsdatenspeicherung tangiert sind. Zudem fallen ständig Daten an, die Aufschluss über den Aufenthalt einer Person erlauben. Damit wird von der Vorratsdatenspeicherung sehr viel und viel Aussagekräftiges erfasst, auch wenn dabei kein oder kaum Kommunikationsinhalt gespeichert wird.

B. Grundrechtseingriffe, welche aus der Vorratsdatenspeicherung resultieren

1. Die Vorratsdatenspeicherung greift in verschiedene Grundrechte ein. Die Vorratsdatenspeicherung ist damit nur rechtmässig, wenn sie sich über eine genügende gesetzliche Grundlage verfügt, sich auf ein öffentliches Interesse stützen kann und verhältnismässig ist, sie muss also geeignet und erforderlich sein, um den beabsichtigten Zweck zu erreichen, und das öffentliche Interesse muss gegenüber den Interessen der betroffenen Person überwiegen (Art. 36 BV).
2. Die Vorratsdatenspeicherung tangiert das Recht auf Achtung des Intim-, Privat- und Familienlebens, auf Schutz der Privatsphäre, einschliesslich Achtung des Brief-, Post- und Fernmeldeverkehrs, auf Schutz vor Missbrauch der persönlichen Daten und die informationelle Selbstbestimmung (Art. 13 BV, Art. 8 EMRK, Art. 17 UNO-Pakt II, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Konvention Nr. 108 des Europarates, SR 0.235.1]). Diese Normen verleihen jeder Person das Recht, frei von staatlicher Überwachung mit anderen Personen zu kommunizieren. Dies betrifft jede Form von Kommunikation, unabhängig davon, wo und mit welchen Mitteln die Kommunikation geführt wird. Geschützt ist sowohl der Inhalt der Kommunikation als auch die Tatsache an sich, dass die Kommunikation stattfindet, namentlich Ort und Zeit der Kommunikation sowie die Identität der daran teilnehmenden Personen. Diese Grundrechte sind damit immer dann tangiert, wenn der Staat Daten im Zusammenhang mit der Kommunikation von Personen erfasst und speichert, und zwar sowohl, wenn der Inhalt der Daten gespeichert wird, als auch bei der Speicherung sogenannter Metadaten (vgl. JÖRG PAUL MÜLLER/MARKUS SCHEFER, Grundrechte in der Schweiz, 4. Aufl., Bern 2008, S. 203 ff).
3. Die Vorratsdatenspeicherung tangiert weiter die Freiheit der Meinungsäusserung, die Meinungs- und Informations- sowie die Medienfreiheit (Art. 16 BV, Art. 10 EMRK) und die Versammlungsfreiheit (Art. 22 BV, Art. 11 EMRK). Diese Normen verleihen jeder Person das Recht, ihre Meinung frei von staatlichen Eingriffen zu bilden und zu äussern, Medien und weitere Informationsquellen selbst und frei von staatlichen Eingriffen zu konsultieren, ihre Meinung mit anderen Menschen auszutauschen und sich friedlich mit anderen Personen zu versammeln (vgl. MÜLLER/SCHEFER, a.a.O., S. 347 ff., S. 437 ff., S. 517 ff., S. 571 ff.).
4. Sodann sind die persönliche Freiheit und die Bewegungsfreiheit garantiert (Art. 10 Abs. 2 BV, Art. 8 EMRK). Diese Grundrechte schützen das Recht, die Persönlichkeit frei von staatlichen Eingriffen zu entfalten, die wesentlichen Aspekte seines Lebens selber zu gestalten, persönliche Beziehungen zu knüpfen, allein gelassen zu werden und sich frei zu bewegen (vgl. MÜLLER/SCHEFER, a.a.O., S. 139 ff., S. 83 ff.).

5. Schliesslich ist Unschuldsvermutung tangiert (Art. 6 EMRK, Art. 32 BV). Jeder Mensch gilt als unschuldig, so lange er nicht in einem rechtmässig geführten Verfahren für schuldig befunden wurde, einen gesetzlich umschriebenen Tatbestand erfüllt zu haben. Eine angeschuldigte Person hat das Recht auf Aussageverweigerung, sie muss sich nicht selbst belasten (nemo-tenetur-Grundsatz). Die Unschuldsvermutung ist auch im Rahmen des Datenschutzes zu beachten (vgl. MÜLLER/SCHEFER, a.a.O., S. 981 ff.).
6. Die Vorratsdatenspeicherung stützt sich auf eine gesetzliche Grundlage, welche sich über mehrere Bundesgesetze und Verordnungen verteilt. Betrachtet man allerdings, welche Daten effektiv gespeichert werden bzw. praxisgemäss gespeichert werden dürfen und was mit Hilfe dieser Daten an Informationen über die betroffenen Personen gesammelt werden kann, so muss man feststellen, dass die gesetzliche Regelung die Praxis nur rudimentär wiedergibt. Das Ganze ist überdies sehr technisch. Die eigentliche Praxis ist kaum fassbar, zumal die betroffene Person von den Behörden und den involvierten Kommunikationsanbietern keine erschöpfenden und anschaulichen Informationen darüber erhalten kann, welche Daten über sie gespeichert werden und welche Informationen im Einzelnen durch diese Daten gewonnen werden können. So weit ersichtlich weigern sich alle Anbieter, Einsicht alle im Rahmen der Vorratsdatenspeicherung erfassten Daten eines Kunden zu gewähren. Die Anbieterin des Gesuchstellers ist nicht bereit, die gespeicherten Vorratsdaten des Gesuchstellers gesamthaft herauszugeben, so dass der Gesuchsteller bis dato nicht im Einzelnen weiss, was für Daten über ihn gespeichert sind und was sich aus diesen Daten im Einzelnen für Informationen gewinnen lassen (vgl. dazu nachstehend Ziff. II.B.22.). Die technische Komplexität wird namentlich aus den technischen Richtlinien zur Vorratsdatenspeicherung (ETSI-Standard Lawful Interception) deutlich (vgl. vorstehend Ziff. II.A.3. ff.). Mit durchschnittlichen Kenntnissen ist es einer Person nicht ansatzweise möglich, die technischen Richtlinien zu verstehen. Nur wer über sehr gute fachliche Kenntnisse verfügt, kann ermitteln, was alles gespeichert wird und welche Erkenntnisse die Behörden mit den gespeicherten Daten gewinnen können.
7. Die Vorratsdatenspeicherung stellt insgesamt einen schweren Eingriff in die Grundrechte dar, zumal sie sich nicht auf Daten beschränkt, welche notwendigerweise mit der Kommunikationsdienstleistung verbunden sind, wie etwa die Aufzeichnung der Zeitdauer eines Telefongesprächs zum Zwecke der Rechnungsstellung (MÜLLER/SCHEFER, a.a.O., S. 204 m.w.H.). Im Rahmen der bestehenden Praxis werden weit mehr Daten gespeichert (vgl. vorstehend Ziff. II. A. 3. ff.). Bei einem Anruf mit einem Mobiltelefon werden beispielsweise nebst der Gesprächsdauer und der Telefonnummer der angerufenen Person zahlreiche weitere Daten gespeichert wie die IMEI des verwendeten Telefongeräts, Angaben zu den benutzten Antennen (und damit der ungefähre Standort des Anrufers). Bei Versand eines Mails müsste rein für die Rechnungsstellung in aller Regel nichts gespeichert werden, nachdem die Nutzung hier nicht pro Mail, sondern pauschal ver-

rechnet wird. Dennoch ist bei jedem Versand eines Mails eine ganze Reihe von Daten zu speichern. Damit müsste die Regelung der Vorratsdatenspeicherung präzise in einem Gesetz im formellen Sinn festgelegt sein. Voraussetzungen und Umfang der Überwachung müssten für den Einzelnen klar aus dem Gesetz ersichtlich sein (MÜLLER/SCHEFER, a.a.O., S. 210). Auf Gesetzesstufe findet sich aber nur eine rudimentäre Regelung. Aus dem Gesetz selbst wird nicht hinreichend klar, welche Daten erfasst werden und welche Informationen sich daraus insgesamt gewinnen lassen.

8. Nicht als grundrechtskompatibel kann in diesem Zusammenhang die bisherige Gerichtspraxis erachtet werden, welche u.a. markante Ausweitungen der Vorratsdatenspeicherung auf Verordnungsstufe zugelassen hat (beispielsweise die Rasterfahndung in gespeicherten Antennenstandorten samt Hauptstrahlrichtung von Mobiltelefonen, dazu sogleich) sowie die Verwertung von gespeicherten Daten nach Ablauf von sechs Monaten zulässt, wenn diese beim Anbieter vorhanden sind (dazu vorstehend Ziff. II.A.1.). Das Bundesgericht lässt ausser acht, dass die Vorratsdatenspeicherung einen schweren Eingriff in die Grundrechte darstellt, weswegen die damit verbundenen Einschränkungen im Einzelnen in einem Gesetz im formellen Sinn enthalten sein müssten.
9. Zu beachten ist in diesem Zusammenhang, dass aus einer vagen gesetzlichen Grundlage ein «chilling effect» resultieren kann, da für die rechtsanwendenden Behörden ein grosser Spielraum bleibt und die Tragweite der Regelung für die Rechtsunterworfenen kaum erkennbar ist. Dies daraus resultierende Tendenz, sich bei der Äusserung von Meinungen zurückzuhalten, beeinträchtigt die Meinungsfreiheit (zum «chilling effect» der Vorratsdatenspeicherung vgl. nachstehend Ziff. B.II.38.). An die Bestimmtheit der gesetzlichen Grundlage sind insoweit aus dem Gedanken des grundrechtlichen Schutzes freier Kommunikation und der Gefahr unerwünschter «chilling effects» besonders strenge Anforderungen zu stellen (MÜLLER/SCHEFER, a.a.O., S. 375 ff.)
10. Als Beispiel dafür, dass die Tragweite der gespeicherten Daten für die betroffenen Personen kaum zu ermessen ist, kann die Rasterfahndung in gespeicherten Antennenstandorten erwähnt werden (sog. Antennensuchlauf, vgl. 1B_376/2011 sowie SIMON SCHLAURI, Fernmeldeüberwachung à discrétion?, in: sic! 2012, S. 238, S. 240 f.). Eine Person mag sich allenfalls bewusst sein, dass jedes Mal, wenn sie ihr Mobiltelefon verwendet (bzw. das Mobiltelefon für gewisse, vom Benutzer u.U. nicht einmal wahrgenommene Funktionen aktiviert wird), der Antennenstandort samt Hauptstrahlrichtung gespeichert wird, und dass ihr effektiver Standort damit sehr genau, u.U. auf wenige Meter genau, erfasst wird. Sie wird sich aber kaum darüber im klaren sein, dass diese Daten dafür verwendet werden können, sie in eine Rasterfahndung einzubeziehen, wenn die Strafverfolgungsbehörde im Rahmen einer entsprechenden Strafuntersuchung wissen möchte, wer sich in den letzten sechs Monaten in einem bestimmten Zeitpunkt an einem bestimmten Ort aufgehalten hat. Die Rasterfahndung in

gespeicherten Antennenstandorten vermag sich zudem nur auf eine Verordnungsbestimmung zu stützen (Art. 16 lit. e VÜPF). Ein Gesetz im formellen Sinn, das diese Massnahme im Einzelnen regeln würde, besteht nicht. Sie verfügt damit nicht über eine genügende gesetzliche Grundlage, zumal sie einen schweren Eingriff in die Grundrechte darstellt.

11. Insgesamt ist damit zu konstatieren, dass zwar eine gesetzliche Grundlage für die Vorratsdatenspeicherung existiert, diese aber als ungenügend zu erachten ist. Wesentliche Details der Praxis erschliessen sich aus keinem Gesetz im formellen Sinn, sondern sind nur auf Verordnungsstufe (VÜPF) bzw. gar nur in den ETSI-Standards Lawful Interception festgehalten. Zum Einen kann die betroffene Person effektiv nicht ermitteln, was alles über sie gespeichert wird und welche Informationen damit gewonnen werden können. Zum Anderen begrenzt die gesetzliche Regelung nur ungenügend, welche Informationen zu welchem Zweck gesammelt werden dürfen.
12. Als öffentliches Interesse für die Vorratsdatenspeicherung kann das Interesse an der Aufklärung von Verbrechen, Vergehen und Übertretungen nach Artikel 179^{septies} StGB (Missbrauch einer Fernmeldeanlage) angeführt werden. Unter den in Art. 273 StPO genannten Voraussetzungen kann die Staatsanwaltschaft gespeicherte Vorratsdaten herausverlangen und als Beweismittel in der entsprechenden Strafuntersuchung verwenden. Art. 273 StPO verweist sodann auf die Voraussetzungen von Art. 269 Abs. 1 lit. b (genügende Schwere der Straftat) und c (Subsidiarität: Erfolglosigkeit der bisherigen Ermittlungen, Aussichtslosigkeit oder unverhältnismässige Erschwerung der Ermittlungen) StPO. Hervorzuheben ist dazu, dass nicht etwa ein Katalog von Delikten besteht, der die Nutzung der gespeicherten Daten im Strafverfahren erlaubt, sondern dass grundsätzlich jeder dringende Verdacht auf ein Verbrechen oder Vergehen ausreicht, im Fall von Artikel 179^{septies} StGB sogar der Verdacht auf eine Übertretung. Die Verwendung von Vorratsdaten beschränkt sich also grundsätzlich nicht auf Fälle schwerer Kriminalität. Die Schwelle liegt insofern sehr tief. Die Voraussetzungen der genügenden Schwere der Tat und der Subsidiarität haben im Übrigen in der Praxis der Genehmigung der Verwendung von Vorratsdaten kaum eine Relevanz und bilden somit keine effektive Schwelle gegen entsprechende Anordnungen.
13. Es kann nicht nur die Herausgabe der Daten der verdächtigten Person verlangt werden, sondern auch jene eines Anschlussüberlassers i.S.v. Art. 270 lit. b Ziff. 1 StPO sowie gemäss eines Teils der Lehre die Daten eines Nachrichtenmittlers i.S.v. Art. 270 lit. b Ziff. 2 StPO (vgl. THOMAS HANSJAKOB, StPO-Kommentar, Zürich 2010, Art. 273 StPO N 11; NIKLAUS SCHMID, Praxiskommentar StPO, Zürich/St. Gallen 2009, Art. 273 N 6). Es müssen sich damit u.U. auch nicht verdächtige Personen die Nutzung ihrer Vorratsdaten gefallen lassen.

14. Wird eine Straftat über das Internet begangen, so ist die Internet-Anbieterin gemäss Art. 14 Abs. 4 BÜPF verpflichtet, der zuständigen Behörde alle Angaben zu machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen. Eine über das Internet begangene Straftat liegt vor, wenn irgend eine Tathandlung über das Internet abgewickelt wird, beispielsweise die Anstiftung. Eine Beschränkung in Bezug auf die Art der Straftat besteht nicht. Die Auskunftspflicht umfasst alle Angaben, die eine Identifikation des Urhebers ermöglichen, namentlich Auskunft darüber, wer eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt benützt hat, nach Möglichkeit mit weiteren Daten zur entsprechenden Person, etwa der Telefonnummer. Die Auskunftspflicht greift auch, wenn es um die konkrete Zuordnung dynamischer IP-Adressen geht (THOMAS HANSJAKOB, Kommentar BÜPF/VÜPF, Art. 14 N 24 ff.).

15. Das Gewicht des öffentlichen Interesses wird stark durch den Umstand relativiert, dass sich die Effektivität der Vorratsdatenspeicherung kaum belegen lässt. Empirische Untersuchungen dazu zeigen keinen signifikanten Einfluss auf die Aufklärungsrate, eine abschreckende Wirkung durch ein höheres Nachweisrisiko ist ebenfalls nicht nachweisbar. Aufschlussreich sind hier insbesondere die diesbezüglichen Gutachten und Untersuchungen des Max-Planck-Instituts für ausländisches und internationales Strafrecht. Nachdem die Vorratsdatenspeicherung in Deutschland eingeführt und später aufgrund eines Urteils des Bundesverfassungsgerichts wieder ausser Kraft gesetzt wurde, wäre zu erwarten, dass sich signifikante Unterschiede zwischen der Zeit, in der Vorratsdatenspeicherung zur Verfügung stand, und der Zeit davor und danach zeigen würden. Auch ein Vergleich mit der Schweiz, die die Vorratsdatenspeicherung schon seit langem kennt, bietet sich an. Das Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht hat diese Zusammenhänge untersucht, stellte aber insgesamt kaum signifikante Veränderungen bzw. Unterschiede fest. In der Schweiz existieren offenbar keinerlei Statistiken und Untersuchungen zur Effektivität der Vorratsdatenspeicherung, obschon die Vorratsdatenspeicherung hierzulande schon seit 2002 zur Verfügung steht (Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Freiburg i. Br., 2011, Schutzlücken durch Wegfall der Vorratsdatenspeicherung? [<http://www.mpicc.de/ww/de/pub/forschung/forschungsarbeit/kriminologie/vorratsdatenspeicherung.htm>]). Derartige Untersuchungen können nicht dadurch ersetzt werden, dass einzelne Fälle anekdotisch als Beleg für den Nutzen der Vorratsdatenspeicherung angeführt werden, zumal einzelne Beispiele keinen allgemein bestehenden Effekt belegen können. Im Einzelnen wird regelmässig schwerlich festzustellen sein, ob die Vorratsdaten für die Aufklärung des Delikts unerlässlich waren, zumal diese nicht die einzigen Beweismittel sind und der effektive Ursprung eines Tatverdachts zuweilen nicht klar zutage liegt. Nicht selten finden sich dazu keine oder nur nebulöse Hinweise in den Akten (*«Polizeiliche Ermittlungen haben ergeben...»*), und es ist offenbar insbesondere im Drogenbereich international gängige Praxis der Strafverfolgungsbehörden, den effektiven Ursprung des Tatverdachts zu verschleiern, etwa durch die

Inszenierung von scheinbar zufälligen Polizeikontrollen (vgl. <http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805>, wo ein Beam-ter der DEA zu diesem als «*parallel construction*» bezeichneten Ansatz wie folgt zitiert wird: «*Parallel construction is a law enforcement technique we use every day, It's decades old, a bedrock concept.*»).

Die Effektivität der Vorratsdatenspeicherung muss damit insgesamt stark angezweifelt werden. Es kann nicht davon ausgegangen werden, dass sich die Aufklärungsquote mit Hilfe der Vorratsdatenspeicherung markant steigern lässt.

16. Zur Verhältnismässigkeit, namentlich zur Erforderlichkeit, finden sich zwar die Bestimmungen von Art. 269 Abs. 1 lit. b. und c. StPO, welche aufgrund des Verweises gemäss 273 Abs. 1 StPO auch bei der Vorratsdatenspeicherung zur Anwendung gelangen. Diese Voraussetzungen bilden in der Praxis aber keine effektive Schwelle gegen die Anordnung entsprechender Massnahmen (vgl. vorstehend Ziff. II.B.12.). Zu beachten ist zudem, dass sich dies nur auf die Verwendung der gespeicherten Daten im Strafverfahren bezieht, nicht auf die Speicherung an sich. Zu prüfen ist also vorab und in erster Linie einmal, ob die Speicherung an sich verhältnismässig ist.
17. Verlangt die Staatsanwaltschaft in einem konkreten Fall Auskunft über gespeicherte Daten, so können diese in der Strafuntersuchung als Beweismittel verwendet werden, können also im Prinzip einen Beitrag zur Aufklärung der begangenen Straftat leisten. Die Vorratsdatenspeicherung ist damit grundsätzlich geeignet, das damit anvisierte öffentliche Interesse zu erfüllen.
18. Zu prüfen ist sodann, ob es für die Erreichung des Zwecks als notwendig erscheint, die Daten im vorgesehenen Umfang zu speichern. Über die vorgesehene Zeit hinweg fallen über die betroffene Person in grossem Umfang Daten an. Dies erscheint – jedenfalls in diesem Umfang, also für so viele Daten so vieler Personen über so lange Zeit – nicht als erforderlich. Nachdem die allermeisten der gesammelten Daten nie für eine Strafuntersuchung relevant werden, und nachdem die anfallenden Daten für die Aufklärung von Straftaten weitgehend ineffektiv sind, erscheint es als geboten, sich auf eine sehr viel weniger weit gehende Erfassung von Daten zu beschränken. So weit man die Auffassung vertreten will, dass Daten, die in Echtzeit nach Eröffnung des Strafverfahrens erfasst werden können, nicht genügen, kann – und muss – sich die Verwendung von Metadaten jedenfalls auf solche beschränken, die in engem zeitlichen und sachlichen Zusammenhang mit der zu untersuchenden Straftat angefallen sind. Es gibt verschiedene Prozeduren, die dies gewährleisten, etwa das in Deutschland als «quick freeze» bezeichnete Verfahren. Dabei werden vorhandene Metadaten bei aufkommendem dringendem Tatverdacht sofort gesichert. Kurze Zeit später kann entschieden werden, in wie weit ein

Anfangsverdacht Anlass gibt, die gesicherten Daten in einem konkreten Strafverfahren zu verwenden. Der grosse Unterschied ist hierbei, dass – wie bei anderen Zwangsmassnahmen auch – erst der dringende Tatverdacht überhaupt Anlass für den Grundrechtseingriff gibt. Dagegen erleiden bei der Vorratsdatenspeicherung alle an der Kommunikation mit Post und Fernmeldeverkehr teilnehmenden Personen einen Eingriff in die Grundrechte. Der Eingriff wird so, was die davon betroffenen Personen betrifft, flächendeckend. Dies erscheint nicht als notwendig. Die erhobenen Daten reichen auch nicht bis zu sechs Monate zurück, was einen kleineren Grundrechtseingriff darstellt und als ausreichend erscheint, zumal aus den vom Dienst ÜPF geführten Statistiken ersichtlich ist, dass die Strafverfolgungsbehörden in den meisten Fällen nur zeitnah angefallene Daten benötigen (vgl. Medienmitteilung der SwiNOG Federation vom 16. Juni 2013).

19. Das Interesse des Staats an der Vorratsdatenspeicherung verfügt über kein grosses Gewicht, nachdem die gespeicherten Daten die Aufklärung von Straftaten nicht oder nur unwesentlich zu verbessern vermögen. Im Arsenal der Untersuchungsmittel und Zwangsmassnahmen nimmt die Vorratsdatenspeicherung insgesamt nur einen bescheidenen Platz ein. Dagegen fällt die permanente und weit reichende Überwachung der betroffenen Personen stark ins Gewicht.
20. Die Bedeutung der Kommunikation über Kanäle, die der Vorratsdatenspeicherung unterliegen, namentlich Telefon, Mail und Internet, ist sehr gross und nimmt in Zukunft noch zu. Die Daten, die bei der Vorratsdatenspeicherung anfallen, lassen weit reichende Schlüsse auf das Kommunikationsverhalten zu, auch auf den Inhalt, sei es, dass inhaltliche Daten erfasst werden, sei es, dass die erfassten Daten Rückschlüsse auf den Inhalt erlauben. Erfasst werden zudem weitere Daten, namentlich Standortdaten, Daten zur Person, insb. Adressen, Bankdaten, Daten zu den verwendeten Geräten und Daten mit Bezug auf den Provider. Bei der heute verbreiteten Nutzung namentlich von Mobiltelefonen fallen die entsprechenden Daten fast ständig an, was u.a. extrem detaillierte Bewegungsprofile erlaubt. Hinzu kommt, dass die im Rahmen der Vorratsdatenspeicherung erfassten Daten mit weiteren Daten kombiniert werden können, was zu noch tiefgreifenderen Grundrechtseingriffen führt (vgl. dazu auch Ziff. II.B.33.).
21. Die Vorratsdatenspeicherung verletzt eine Reihe von datenschutzrechtlichen Grundsätzen, namentlich das Verbot des Datensammelns auf Vorrat, den Grundsatz der Zweckbindung der Daten und den Grundsatz der Verhältnismässigkeit der Datenbearbeitung (vgl. dazu Art. 4 ff. DSGVO; URS MAURER-LAMBROU/ANDREA STEINER, Balser Kommentar DSGVO, 2. Aufl., Basel 2006, Art. 4 N 9 ff.; ASTRID EPINEY, in: BELSER/EPINEY/WALDMANN, Datenschutzrecht, Bern 2011, § 9 N 23 ff.). Es werden sehr viele Daten aller betroffenen Personen auf Vorrat gesammelt. Die Daten entstehen als Nebenprodukt von Kommunikationsvorgängen und dienen eigentlich dazu, dass die gewünschte Kommunikation stattfinden kann. Indem die

Daten dabei systematisch aufgezeichnet und gespeichert werden, um allenfalls in einem späteren Strafverfahren verwendet werden zu können, ändern sie ihren Zweck grundlegend. Es wäre erforderlich, dass die betroffene Person der Sammlung der Daten freiwillig zustimmt, nachdem sie angemessen informiert worden ist. Dies ist bei der Vorratsdatenspeicherung nicht der Fall. Als betroffene Person ist man nicht in der Lage, Inhalt und Tragweite der Vorratsdatenspeicherung zu erkennen, auch nicht, wenn man sich darum bemüht, die entsprechenden Informationen zu beschaffen. Die gesetzlichen Grundlagen und die technischen Details sind für Laien unverständlich (vgl. vorstehend Ziff. II.A.3. ff.). Auch hat die betroffene Person nicht die Möglichkeit, der Sammlung und Verwendung der Daten zuzustimmen oder diese zu verhindern, indem sie ihre Zustimmung verweigert. Schliesslich gibt es nicht einmal griffige Bestimmungen, die sicherstellen würden, dass die Daten nach der gesetzlich vorgesehenen Frist von sechs Monaten gelöscht werden (wie dargelegt lässt das Bundesgericht die Verwendung der Daten auch nach Ablauf von sechs Monaten zu, vgl. vorstehend Ziff. II.A.1.). Die Verletzung datenschutzrechtlicher Grundsätze durch einen Anbieter hat in aller Regel keine verwaltungsrechtlichen oder strafrechtlichen Folgen.

22. Eine Anfrage beim Provider oder beim Dienst ÜPF würde der betroffenen Person auch nicht zu einem befriedigenden Informationsstand verhelfen. Auf allgemeiner Ebene sind keine griffigen Informationen vorhanden, mittels derer sich ein Laie ein konkretes Bild über die gespeicherten Daten machen kann. Gesuche an den eigenen Anbieter, die über sich gespeicherten Daten zu erhalten, werden – so weit ersichtlich – von keinem Provider bewilligt. Die Anbieter sind höchstens bereit, einige wenige Daten herauszugeben, verweigern aber durchwegs die Einsicht in alle gespeicherten Daten. Damit kann sich die betroffene Person kein Bild darüber machen, welche Daten von ihr gespeichert sind und wie gravierend der Eingriff in ihre Grundrechte konkret ist, welcher damit verbunden ist. Dieser Aspekt der Heimlichkeit der Vorratsdatenspeicherung verstärkt den damit verbundenen Eingriff zusätzlich.
23. Schliesslich ist nicht sichergestellt, dass die Daten nicht ins Ausland gelangen, etwa im Rahmen internationaler Rechtshilfe in Strafsachen, polizeilicher und geheimdienstlicher Zusammenarbeit, aber auch aufgrund von mangelnder Datensicherheit. Wenn sie ins Ausland gelangen ist die Einhaltung der in der Schweiz geltenden Garantien bezüglich Grundrechte, Datenschutz und Datensicherheit nicht gewährleistet.
24. Die grosse Menge an Daten, die bei diversen Anbietern anfallen, werfen beträchtliche Probleme bezüglich der Datensicherheit auf. Die Daten werden nicht vom Dienst ÜPF oder von den Strafverfolgungsbehörden gesammelt, sondern müssen von den Anbietern gespeichert werden. Dies schützt zwar die Daten vor dem unmittelbaren staatlichen Zugriff, wirft aber dafür andere Probleme bezüglich Datenschutz und Datensicherheit auf: Die Daten müssen von den Anbietern vor unbefugten Zugriffen

geschützt werden. Art. 9 VÜPF überträgt den Anbietern, für die Datensicherheit besorgt zu sein, und verweist zudem auf die VDSG, welche für die Anbieter ohnehin gelten würde, und die BinfV, welche inhaltlich nichts Wesentliches zum Problem beiträgt. Dies genügt nicht. Damit stellt der Staat nicht sicher, dass die Daten sicher gehandhabt werden. Es fehlen griffige Vorschriften zur Datensicherheit, und es fehlt an einer Durchsetzung und Kontrolle der Datensicherheit von staatlicher Seite. Der Dienst ÜPF selbst wird im Übrigen auch nicht zureichend kontrolliert. Zwar besteht u.a. eine parlamentarische Kontrolle der Tätigkeit des Dienstes ÜPF, diese kann aber nur von Zeit zu Zeit einzelne Aspekte der Tätigkeit des Dienstes ÜPF kontrollieren und erstreckt sich offenbar nicht auf die im ISC-EJPD angesiedelte Informatik, auf der die Praxis der Vorratsdatenspeicherung Seitens des Dienstes ÜPF beruht.

25. Effektiv ist die Datensicherheit offensichtlich nicht gewährleistet. Konkrete Vorfälle, die bekannt geworden sind, zeigen, dass dies kein hypothetisches Problem darstellt, sondern ein reales. Angestellte von Swisscom, Orange und Sunrise haben offenbar vertrauliche Daten verkauft (<http://www.handelszeitung.ch/unternehmen/illegaler-datenverkauf-orange-und-sunrise-bestrafen-mitarbeiter>; <http://www.it-markt.ch/de-CH/News/2012/05/21/Verkauf-von-vertraulichen-Daten.aspx>). Bei der Swisscom sind Daten, die geschreddert werden sollten, verschwunden. Dies ist bekannt geworden, nachdem entsprechende Datenträger der NZZ zugespielt worden sind. Darauf befinden sich offenbar 60 Millionen Datensätze, in denen sich Geheimnummern von 979 Prominenten sowie 14'500 interne Mails, Verträge, Projektbeschreibungen und Sitzungsprotokolle befinden. Die Swisscom hat keine Erklärung dafür, wie die Daten abhanden gekommen sein könnten. Bei einem Hackerangriff auf den Mobilfunkanbieter Vodafone in Deutschland sind die Daten von zwei Millionen Kunden – darunter Kontonummern – gestohlen worden (<http://www.nzz.ch/aktuell/schweiz/entwendete-baender-bringen-die-swisscom-in-noete-1.18151998>; <http://www.nzz.ch/aktuell/schweiz/brisante-prominenten-liste-auf-gestohlenem-band-1.18208255>). Dass die genannten Anbieter, einschliesslich der Swisscom, die Datensicherheit nicht durchwegs gewährleisten können, weist darauf hin, dass hier ein grundsätzliches Problem besteht. Der Staat verlangt von privaten Anbietern, die Daten zu sammeln, ohne die Sicherheit der aufgezeichneten Daten zu gewährleisten. Darin liegt ein weiterer Aspekt, der den Eingriff in die Grundrechte als gravierend erscheinen lässt. Die betroffenen Grundrechte und namentlich auch das Fernmeldegeheimnis sind auf diese Weise nicht gewahrt (vgl. Entscheidung Nr. 1258 des rumänischen Verfassungsgerichtshofes).
26. Auf welcher Software und Hardware die Speicherung und Nutzung der Vorratsdaten seitens der Anbieter und seitens des Dienstes ÜPF beruht, ist nicht bekannt. Es kann ohne genauere Kenntnis diesbezüglich nicht angenommen werden, dass die gespeicherten Daten damit hinreichend geschützt sind. Angesichts der grossen Menge und der hohen Sensibilität der Daten müsste der Schutz der Daten auf technischer Seite sehr hohen

Ansprüchen genügen. Das Risiko, dass ausländische staatliche Stellen oder nichtstaatliche Hacker versuchen, an diese Daten heranzukommen, ist nicht zu unterschätzen. Es sei hier auf die ungeheuren Aktivitäten der NSA und mit ihr verbundener Dienste verwiesen (vgl. nachstehend Ziff. II.B.28.). Es ist überdies stets damit zu rechnen, dass ein Anbieter von Soft- und Hardware für Belange der Vorratsdatenspeicherung mit der NSA oder anderen Diensten verknüpft ist, indem er auch der NSA oder anderen Diensten Soft- und Hardware liefert oder indem er sonstwie auf freiwilliger oder unfreiwilliger Basis mit den entsprechenden Diensten zusammenarbeitet, u.a., indem er ihm Kenntnisse über Sicherheitslücken weitergibt (dazu nachstehend Ziff. II.B.28.). Im Zusammenhang mit der NSA sind einige derartige Vorkommnisse bekannt geworden. Dies kann aber genauso auch irgendwelche andere Software und irgendwelche andere Dienste der USA oder anderer Staaten betreffen. Unter diesen Umständen besteht die nicht unbeträchtliche Gefahr, dass in der verwendeten Soft- und Hardware Hintertüren versteckt sind, welche von der NSA oder von anderen Diensten, aber auch von nichtstaatlichen Hackern, genutzt werden können, um an die gespeicherten Daten heranzukommen. Der Bund lässt die Öffentlichkeit nicht wissen, welches der Lieferant der vom Dienst ÜPF verwendeten Software ist. Den Medien ist zu entnehmen, dass es sich um Verint handelt, eine amerikanische Firma mit israelischen Wurzeln, der enge Kontakte zum israelischen Geheimdienst und zur NSA nachgesagt werden (<http://www.tagesanzeiger.ch/schweiz/standard/Abgehoerte-Leitungen-ein-Schweizer-Flop-und-die-Einheit-8200-/story/27811395>).

27. Die mangelnde Datensicherheit und die fehlende Zweckbindung der Daten beinhalten ein weiteres Risiko: Wenn Daten gespeichert werden müssen, deren Datensicherheit aber nicht gewährleistet ist, kann dies auch dazu führen, dass die Daten mit irgendwelchen anderen Absichten zweckentfremdet werden. Die Daten können u.a. auch dafür verwendet werden, betroffene Personen zu kompromittieren oder zu erpressen. Beispiele aus dem amerikanischen Geheimdienst zeigen, dass dies nicht nur ein theoretisches, sondern ein reales Risiko ist (vgl. <http://www.thedailybeast.com/articles/2011/08/02/fbi-director-hoover-s-dirty-files-excerpt-from-ronald-kessler-s-the-secrets-of-the-fbi.html>; <https://www.aclu.org/blog/national-security-technology-and-liberty/prospect-blackmail-nsa>).
28. Ein Schlaglicht auf die gesamte Problematik werfen die Vorgänge, die im Zusammenhang mit der NSA und anderen Diensten bekannt geworden sind (vgl. <http://www.theguardian.com/world/edward-snowden>). Die Tätigkeit der NSA geht so weit, dass sie die Integrität und Sicherheit des Datenverkehrs auf praktisch jeder Ebene nachhaltig untergraben hat. Die NSA lässt sich offenbar Daten von vielen grossen IT-Firmen liefern oder greift diese ohne deren Wissen oder Zustimmung ab. Die Sicherheit von Verschlüsselungstechnologien und dabei vergebenen Zertifikaten ist gezielt ausgehebelt worden. Die NSA und ihre in- und ausländischen Partnerdienste schaffen es so, verschlüsselte Kommunikation im Internet zu

knacken. Die amerikanische Sicherheitsfirma RSA beispielsweise hat ihre Verschlüsselungs-Software offenbar mit einer NSA-Hintertüre ausgestattet. Werden solche Hintertüren und Schwächen eingebaut, besteht das Risiko, dass diese in der auch von (weiteren) Hackern ausgenützt werden (<http://www.tagesanzeiger.ch/ausland/amerika/Auf-die-Spione-folgen-die-Kriminellen/story/17283716>; <http://www.tagesanzeiger.ch/ausland/amerika/Die-Zeche-fuer-die-globale-Spionage-der-NSA/story/19784722>; <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>). Eine Zusammenarbeit zwischen NSA und IT-Firmen besteht offenbar auch insoweit, als IT-Firmen der NSA Informationen über Sicherheitslücken gibt, bevor diese geschlossen werden, so dass die NSA diese Lücken ausnützen kann (<http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html>). Die Enthüllungen über die NSA und ihre Partnerdienste machen klar, dass die Sicherheit der Kommunikation über Telefon, Internet und weitere elektronische Kanäle stark kompromittiert ist. Sie zeigen aber auch die Bedeutung Schwere der Auswertung gesammelter Daten und der Folgen für die Grundrechte der Betroffenen. Beides – die Datensicherheit und die Möglichkeiten der computergestützten Datenauswertung – betrifft auch die Vorratsdatenspeicherung.

29. Die Vorratsdatenspeicherung betrifft alle Personen gleichermassen, nicht nur Personen, die eine Straftat begangen haben oder der Begehung einer Straftat verdächtigt werden. Jede natürliche und juristische Person nutzt die von der Vorratsdatenspeicherung betroffenen Kommunikationsdienste und Kommunikationsnetze und ist damit Subjekt der damit verbundenen Überwachung. Die Unschuldsvermutung und die betroffenen Grundrechte sind unter diesen Umständen nicht gewährleistet (vgl. Entscheidung Nr. 1258 des rumänischen Verfassungsgerichtshofes, S. 12). Problematisch ist hierbei insbesondere, dass jede Person, deren Vorratsdaten aufgezeichnet werden, dem Risiko ausgesetzt wird, sich im Nachhinein rechtfertigen zu müssen, wenn aus den Metadaten ein Tatverdacht gegen sie erzeugt oder verstärkt wird. Sie muss sich für die angefallenen Daten erklären und dabei die Interpretation der Strafverfolgungsbehörden, die sie ihr als Beleg für den Tatverdacht entgeghält, zu entkräften versuchen. Die Wahrscheinlichkeit, als unschuldige Person einer Tat verdächtigt zu werden und dadurch in ein Strafverfahren involviert zu werden – mit allen damit verbundenen privaten und beruflichen Nachteilen –, wird durch die Vorratsdatenspeicherung deutlich erhöht. Die Vorratsdatenspeicherung ist geeignet, den Kreis der Verdächtigen (letztendlich unendlich) zu vergrössern, weil die Zahl der auswertbaren Kommunikationsverbindungen grösser und umfassender wird (vgl. dazu den Antrag an den österreichischen Verfassungsgerichtshof zur Richtlinie 2006/24/EG, S. 32 f.).
30. Betrachtet man die gesetzliche Regelung und die Informationspraxis von Behörden und Providern zur Vorratsdatenspeicherung, so muss man feststellen, dass die mangelhafte Information der Betroffenen System hat. Ein gewisses Mass an Heimlichkeit gegenüber allen Personen, die die entspre-

chenden Kommunikationsformen nutzen, ist der Vorratsdatenspeicherung inhärent, und das entspricht durchaus der Absicht der involvierten Behörden und Provider. Auch dieser Aspekt trägt ganz wesentlich zum Schluss bei, dass der Staat mit der Vorratsdatenspeicherung jede Person als potenzielle Straftäter betrachtet, indem er von allen Personen Metadaten ihrer Kommunikation mitschneidet. Dies kollidiert mit der Unschuldsvermutung und mit den betroffenen Grundrechten.

31. Die Vorratsdatenspeicherung besteht aus der fortlaufenden Aufzeichnung von Daten, welche zu grossen Datensätzen kumuliert, systematisch durchsucht und verknüpft werden können (Stichworte: Data Warehousing, Data Mining und Big Data). Durch diese Akkumulation und Verknüpfbarkeit ändern die Daten ihren Charakter grundlegend. Die Daten können zu Profilen verknüpft werden. Mit dem Zusammenzug der Daten sind Rückschlüsse über das Kommunikationsverhalten möglich, die aus den einzelnen Daten für sich besehen nicht gewonnen werden können. Es können Bewegungsprofile angelegt werden, und es wird so sichtbar, wann sich eine Person wo aufgehalten hat. Die Daten können im Rahmen einer Rasterfahndung nach bestimmten Merkmalen durchsucht werden, etwa danach, ob sich eine Person zu einem bestimmten Zeitpunkt in einer bestimmten Gegend aufgehalten hat. Zwar werden im Wesentlichen Metadaten gespeichert, welche sich aus der Kommunikation der betroffenen Person ergeben und kein Inhalt der Kommunikation. Die Daten sagen aber dennoch sehr viel über die betroffene Person aus, namentlich über ihr Kommunikationsverhalten und ihren Aufenthaltsort. Die Auswertung der vorhandenen Daten mittels spezieller Suchfunktionen und komplexer Algorithmen hebt deren Gehalt überdies auf eine andere Ebene. Die diesbezügliche Technologie hat sich in den letzten Jahren rasant entwickelt; ein Ende der Entwicklung ist nicht abzusehen. Einerseits erlauben derartige Auswertungen Aussagen über die Person, die weit über die einzelnen Datensätze hinausgehen. Das Ganze ist so besehen, was die Daten betrifft, weit mehr als alle einzelnen Teile. Andererseits sind die gewonnenen Aussagen bzw. die damit vorgenommenen Interpretationen von anderer Qualität als die herkömmliche Auswertung einzelner Daten. Es wird nach verborgenen Zusammenhängen in den Daten gesucht, wobei diese Zusammenhänge nicht unbedingt real bestehen, sondern letztlich nur eine mittels Datenverarbeitung gewonnene Interpretation der Daten darstellen. Daten, die für sich alleine betrachtet irrelevant erschienen und allenfalls auch gar nie ins Blickfeld kämen, können durch eine derartige Auswertung Relevanz gewinnen.
32. Problematisch ist dabei – nebst der Wucht und Raffinesse der Daten und ihrer Auswertung an sich –, dass die gespeicherten Daten genutzt werden können, um überhaupt einen Tatverdacht bzw. Korrelationen, die zu einem Tatverdacht führen können, zu erzeugen. Die Vorratsdaten können so dazu führen, dass eine Person aufgrund der gespeicherten Daten überhaupt erst in ein Strafverfahren verwickelt wird. Anschaulich ist dies insbesondere bei der Rasterfahndung in gespeicherten Antennendaten, mit der

u.U. ein Tatverdacht generiert wird. Die Daten der Vorratsdatenspeicherung können damit Grundlage für Zwangsmassnahmen bilden, denen kein hinreichender Tatverdacht vorausgeht, sondern bei denen die Zwangsmassnahmen dazu dienen, den Tatverdacht gegen konkrete Personen überhaupt zu generieren. Dies widerspricht dem rechtsstaatlichen Grundsatz, dass Zwangsmassnahmen nur ergriffen werden können, wenn ein hinreichender Tatverdacht vorliegt (vgl. NIKLAUS OBERHOLZER, Grundzüge des Strafprozessrechts, 3. Aufl., Bern 2012, S. 310, Rz. 848). In Art. 197 Abs. 1 lit. b StPO ist dies an sich festgelegt. Dieser Grundsatz ist aber im Rahmen der Nutzung der Daten aus der Vorratsdatenspeicherung nicht gewährleistet. Erschwerend kommt hinzu, dass nicht alle betroffenen Personen, deren Daten in Rasterfahndung einbezogen werden, danach darüber informiert werden. Die Vorratsdatenspeicherung ist auch insoweit grundrechtswidrig. Das Beispiel der Rasterfahndung in Antennendaten zeigt deutlich, dass die Vorratsdatenspeicherung nicht mit der Unschuldsvermutung vereinbar ist. Es zeigt sich hier exemplarisch das Risiko, dass sich eine Person aufgrund aufgezeichneter Metadaten im Nachhinein rechtfertigen muss (vgl. Ziff. II.B.29.).

33. Die Daten können mit Daten anderer Personen verknüpft werden. Weiter ist eine Verknüpfung mit anderen Daten möglich, welche ausserhalb der Vorratsdatenspeicherung anfallen. Diese Daten können durch weitere Untersuchungshandlungen gewonnen werden, namentlich mit anderen strafprozessualen Zwangsmassnahmen, insb. Beschlagnahme oder Edition von Datenträgern bzw. Daten. Dies können weitere Daten sein zu den in der Vorratsdatenspeicherung gehaltenen Daten, namentlich inhaltliche Daten, etwa der Inhalt eines Mails, einer Voicemail-Nachricht, einer Chat-Nachricht. Diese Daten können auf einem verwendeten Gerät anfallen, namentlich auf einem Mobiltelefon, und von dort ausgelesen werden. Für die Kommunikation werden zunehmend Apps auf Computern, Mobiltelefonen und anderen Geräten verwendet. Die Verwendung dieser Apps generieren inhaltliche Daten und Metadaten, die auf den entsprechenden Geräten erzeugt werden und zumindest teilweise gespeichert bleiben. Gleichzeitig werden je nach genutztem Gerät und Kommunikationskanal auch Vorratsdaten generiert. Dies ist dann insbesondere dann der Fall, wenn für die Kommunikation der Datenkanal eines Mobilfunk-Anbieters genutzt wird. Da solche Apps insbesondere auf Mobiltelefonen sehr oft genutzt werden, fallen durch deren Verwendung mitunter enorme Datenspuren an. Andere Daten, die beigezogen werden können, können beispielsweise aus Hausdurchsuchungen, von der Festplatte eines beschlagnahmten Computers, aus einem Mobiltelefon oder aus Videoüberwachungen stammen. Möglich sind auch Editionsbegehren an Dritte, etwa Anbietern von Internet-Diensten, Arbeitgeber, Behörden, Ladenketten, Banken, Kreditkartenunternehmen oder Online-Shops. Gewonnen werden können so etwa Facebook-, Twitter- oder Google+-Einträge, Chat-Beiträge, Mails, Daten zu Einkäufen und Zahlungen.

34. Nachdem die heutigen Möglichkeiten der computergestützten Verarbeitung kumulierter Daten und die damit verbundene komplexe Auswertungen den Charakter der verwendeten Daten grundlegend ändern und auf eine andere Stufe heben, ist eine solche Bearbeitung von Personendaten mit dem Grundsatz der Zweckbindung grundsätzlich nicht vereinbar. Für die betroffene Person kann in der Regel nicht ersichtlich sein, zu welchen Zwecken die neu kreierten Daten verwendet werden können (vgl. zum Ganzen: EPINEY, a.a.O., § 9 N 34; ROLF H. WEBER, in: Jusletter IT, 11. Dezember 2013, Big Data: Sprengkörper des Datenschutzrechts?).
35. Gerade durch das Element der Heimlichkeit verstösst die Vorratsdatenspeicherung auch gegen den Nemo-tenetur-Grundsatz. Spuren, die jede Person durch alltägliche Formen der Kommunikation selbst gesetzt hat, werden ihrem ursprünglichen Zweck, der im Zusammenhang mit eben dieser Kommunikation steht, entrissen, und mutieren zum belastenden Element in einem Strafverfahren.
36. Die Anordnung von Überwachungsmassnahmen bedarf der Genehmigung durch das Zwangsmassnahmengericht (Art. 274 StPO). Zwischen der Anordnung der Massnahme und dem Entscheid können aber gemäss Gesetz bis zu 6 Tagen verstreichen. Dies kann zur Situation führen, dass die Staatsanwaltschaft nach der Anordnung der Massnahme Vorratsdaten erhält (Art. 273 StPO), das Zwangsmassnahmengericht die Massnahme dann aber nicht genehmigt. Ergebnisse aus nicht genehmigten Massnahmen sind sofort zu vernichten und die daraus gewonnenen Ergebnisse sind nicht verwertbar (Art. 277 StPO). Dies ergibt aber keinen zureichenden Schutz vor ungerechtfertigten Massnahmen, da die erlangten Ergebnisse den Fortgang des Verfahrens beeinflussen können, bevor die Nichtgenehmigung der Massnahme feststeht, und da das damit gewonnene Wissen in den Köpfen der Strafverfolgungsbehörden bleibt, auch wenn die entsprechenden Dokumente und Datenträger vernichtet werden. Zudem ist die effektive Löschung bzw. Entfernung der betreffenden Daten nicht ausreichend gewährleistet (vgl. Ziff. II.A.1., Ziff. II.B.21., Ziff. II.B.24.).
37. Aus den gespeicherten Metadaten lassen sich Rückschlüsse auf das Kommunikationsverhalten der betroffenen Person ziehen, insbesondere darauf, mit wem eine Person kommuniziert, wie und wo. Im Rahmen der Vorratsdatenspeicherung werden damit sehr aussagekräftige Daten angehäuft. Aus den Metadaten können auch Schlüsse auf den Inhalt der Kommunikation gezogen werden, verstärkt noch, wenn sie mit anderen Daten kombiniert werden. Die Vorratsdatenspeicherung stellt insofern einen weit reichenden Eingriff in die Meinungsfreiheit dar.
38. Der Umstand, dass bei der Nutzung der von der Vorratsdatenspeicherung erfassten Kommunikationstechnologien in beträchtlichem Umfang Daten gespeichert werden, aus denen weit reichende Schlüsse auf die betreffende Person, ihr Verhalten und weitere Eigenschaften gezogen werden können, ist geeignet, das Kommunikationsverhalten der betroffenen Per-

son nachhaltig zu beeinflussen und sie in ihrer Nutzung der betroffenen Kommunikationstechnologien zu beeinträchtigen. Die Vorratsdatenspeicherung ist geeignet, die betroffene Person von der Nutzung der betroffenen Technologien abzuhalten oder sie in ihrer Nutzung negativ zu beeinflussen. Wenn die betroffene Person weiss oder ahnt, dass Vorratsdaten aufgezeichnet werden, wird sie ihr Kommunikationsverhalten tendenziell dem anpassen und die entsprechenden Technologien nicht oder nicht unbefangen nutzen. Die Vorratsdatenspeicherung beinhaltet insofern einen «chilling effect», welcher wiederum einen Eingriff in die genannten Grundrechte darstellt (vgl. MÜLLER/SCHEFER, a.a.O., S. 375 ff.).

39. Als Journalist ist der Gesuchsteller von der Vorratsdatenspeicherung speziell betroffen. Er ist für die Ausübung seines Berufes verstärkt darauf angewiesen, frei von Überwachung und unter Wahrung des Quellenschutzes recherchieren und andere Personen kontaktieren zu können. Mit den gespeicherten Vorratsdaten wird bei der Anbieterin eine Datenspur gelegt, aus der Rückschlüsse auf seine beruflichen Aktivitäten, seine Recherchen und seine Kontakte zu Drittpersonen gezogen werden können. Namentlich sind mit den gespeicherten Daten Schlüsse auf Kontakte mit journalistischen Quellen möglich. Die vorstehend dargelegten Grundrechtseingriffe wirken damit beim Journalisten noch verstärkt. Dies gilt namentlich auch für die Rechtsunsicherheit und Intransparenz, die aus der ungenügenden gesetzlichen Grundlage der Vorratsdatenspeicherung resultiert (dazu MÜLLER/SCHEFER, a.a.O., S. 377).
40. Art. 17 BV garantiert die Medienfreiheit. Gestützt auf Art. 17 Abs. 3 BV und Art. 10 EMRK anerkennen der EGMR und das Bundesgericht den Schutz journalistischer Quellen als eine der Grundbedingungen der Medienfreiheit. Eine Pflicht zur Preisgabe der anvertrauten Informationen könnte die Informanten abschrecken (MÜLLER/SCHEFER [mit FRANZ ZELLER], a.a.O., S. 472; FROWEIN/PEUKERT, EMRK-Kommentar, 3. Aufl., Kehl am Rhein 2009, Art. 10 Rn. 17; JENS MEYER-LADEWIG, Handkommentar EMRK, 3. Aufl., Baden-Baden 2011, Art. 10 Rn. 39). Art. 28a StGB und Art. 172 StPO verankern den Quellenschutz und postulieren grundsätzlich die Straflosigkeit und ein Verbot strafprozessualer Zwangsmassnahmen für den Fall, dass ein Journalist als Zeuge seine Quelle nicht offen legt.
41. Der Schutz der Medienfreiheit und der Quellenschutz haben damit zwar grundsätzlich Eingang in die Strafprozessordnung gefunden. Dieser Schutz erweist sich aber in mehrerer Hinsicht als ungenügend. Ungeachtet des für Journalisten bestehenden Zeugnisverweigerungsrechts werden Metadaten, die von der Vorratsdatenspeicherung betroffen sind, auch im Verkehr zwischen Journalisten und ihren Kommunikationspartnern, einschliesslich ihrer Quellen, erfasst. Diese Metadaten können Hinweise auf die Quellen des Journalisten erlauben. Dies stellt einen Eingriff in die Medienfreiheit dar, da mit jeder Form von Kommunikation, die der Vorratsdatenspeicherung unterliegt, der Quellenschutz insoweit durchbrochen wird. Angesichts der eminenten Wichtigkeit des Quellenschutzes wiegt dieser Eingriff schwer.

42. Soweit das in Art. 28a StGB enthaltene Verbot von Zwangsmassnahmen greift, ist der Journalist zwar davor geschützt, dass die vorhandenen Metadaten durch Anordnung von Massnahmen gemäss Art. 273 StPO (Auskunft über Verkehr- und Rechnungsdaten Teilnehmeridentifikation) gegen den Journalisten an die Staatsanwaltschaft gelangen. Eine solche Massnahme ist damit unzulässig, soweit sie nur zum Ziel hat, den Quellschutz zu unterlaufen (HANSJAKOB, Kommentar BÜPF/VÜPF, Art. 4 N 31 ff). Dies ändert aber nichts daran, dass die entsprechenden Metadaten, die in der Kommunikation mit Quellen anfallen, im Rahmen der Vorratsdatenspeicherung erfasst werden, was – wie dargelegt – einen schweren Eingriff in die Medienfreiheit darstellt.

43. Art. 271 StPO verankert den Schutz von Berufsgeheimnissen i.S.v. Art. 271 StPO bei Überwachungen. Richtet sich die Überwachung gegen eine Person, die einer Berufsgruppe gemäss Art. 170 - 173 angehört, so sind Informationen, die mit dem Gegenstand der Ermittlungen und dem Grund, aus dem diese Person überwacht wird, nicht in Zusammenhang stehen, unter der Leitung eines Gerichts auszusondern. Dabei dürfen der Strafverfolgungsbehörde keine Berufsgeheimnisse zur Kenntnis gelangen. Art. 271 Abs. 2 StPO schränkt die Zulässigkeit von Direktschaltungen ein in Fällen, in denen sich die Überwachung gegen Berufsgeheimnisträger richtet. Gemäss Art. 271 Abs. 3 sind bei der Überwachung anderer Personen Informationen, über welche eine in den Art. 170 - 173 genannte Person das Zeugnis verweigern könnte, aus den Verfahrensakten auszusondern und sofort zu vernichten; sie dürfen nicht verwendet werden.

44. Zwar bezieht sich Art. 271 StPO auch auf den Quellschutz von Journalisten. Ein effektiver Schutz der Grundrechte des Journalisten in Bezug auf die Verwendung von Daten aus der Vorratsdatenspeicherung resultiert daraus nicht. Vom Wortlaut her ist nicht einmal klar, ob sich Art. 271 StPO auf die Auskunft über Vorratsdaten nach Art. 273 StPO bezieht. Abgesehen schützt Art. 271 StPO den Journalisten bzw. seine Grundrechte nicht zureichend. Gerade bei Vorratsdaten lässt sich nicht vermeiden, dass diese der Strafverfolgungsbehörde zur Kenntnis gelangen, bevor die Mechanismen, wie sie in Art. 271 StPO vorgesehen sind, greifen können.

45. Die Beschränkung der Zulässigkeit von Direktschaltungen lässt sich in der Praxis seit einigen Jahren nicht mehr durchsetzen, da es kurz gesagt technisch gesehen im aktuellen System nur noch Direktschaltungen gibt. Die Ermittlungsbehörden von Bund und Kantonen können jederzeit und unmittelbar auf die aufgezeichneten Gespräche etc. zugreifen (NIKLAUS SCHMID, Handbuch des Schweizerischen Strafprozesses, Zürich/St. Gallen 2009, N 1146; HANSJAKOB, StPO-Kommentar, Art. 271 StPO N 11).

46. Die Vorschrift, bei der Überwachung von Drittpersonen seien Informationen, die dem Zeugnisverweigerungsrecht unterliegen, aus den Akten zu nehmen, und die entsprechenden Informationen würden einem Verwer-

tungsverbot unterliegen, greift zum Schutz des Journalisten bzw. seiner Quelle nicht. Man hat versucht, den Quellenschutz zu gewährleisten, indem man den Journalisten denselben Vorschriften unterstellt hat wie andere Geheimnisträger. Dabei hat der Gesetzgeber übersehen, dass es hier entscheidende Unterschiede gibt. Anders als etwa bei Anwälten, Geistlichen und Ärzten geht es beim Quellenschutz nicht nur um das Gegenüber des Geheimnisträgers, sondern mindestens ebenso um den Geheimnisträger selbst. Während dem der Schutz des Anwaltsgeheimnisses dem Klienten dienen soll, bezieht sich der Quellenschutz als Teil der Medienfreiheit und des Redaktionsgeheimnisses (Art. 17 BV) primär auf den Journalisten.

47. Art. 271 StPO gewährt dem Journalisten keinen wirksamen Schutz seiner Grundrechte. Zum Einen liegt die entscheidende Information, nämlich dass, wo und über welchen Kanal ein Journalist mit einer anderen Person kommuniziert hat, in den eingeholten Vorratsdaten selbst. Soweit es sich beim Kommunikationspartner um eine geschützte Quelle handelt, liegt die entsprechende Information den Strafverfolgungsbehörden mit der Einholung der Auskunft über die Vorratsdaten unmittelbar vor. Die Strafverfolgungsbehörden erlangen damit ohne Weiteres über den Kontakt mit einer anderen Person Kenntnis. Ist diese andere Person eine Quelle des Journalisten, ist der Quellenschutz damit ausgehebelt. Zum Anderen ist der Journalist weniger umfassend geschützt als etwa der Anwalt. Beim Anwalt ist grundsätzlich die gesamte Kommunikation in seiner Berufssphäre durch das Anwaltsgeheimnis geschützt. Beim Journalisten hingegen bezieht sich der Schutz nur auf seine Quelle, nicht auf irgendwelche andere Kontakte, da er nur insoweit über ein Zeugnisverweigerungsrecht verfügt. Absurderweise würde damit die Durchsetzung der Aussonderung und Unverwertbarkeit nach Art. 271 Abs. 3 StPO beim Journalisten voraussetzen, dass der Behörde, welche die Aussonderung vornimmt und sich der Unverwertbarkeit bewusst sein soll, gerade davon Kenntnis hat, dass es sich um eine Quelle handelt. Anders kann sie das – eben nur selektiv auf Quellen bezogene – Zeugnisverweigerungsrecht im konkreten Fall gar nicht berücksichtigen. Wenn es nun aber der Strafverfolgungsbehörden von sich aus oder aufgrund von Angaben der Quelle oder des Journalisten klar wird, dass sich die Kommunikation auf eine geschützte Quelle des Journalisten bezieht, ist der Quellenschutz bereits ausgehebelt und das Zeugnisverweigerungsrecht wertlos. Die Katze beisst sich in den Schwanz. Eine nachherige Entfernung der entsprechenden Daten ändert daran nichts, ebenso wenig ein Verwertungsverbot. Die entsprechenden Daten mögen danach nicht mehr in den Akten sein. Das Wissen, wer die Quelle des Journalisten ist, ist bereits in die Köpfe der damit befassten Strafverfolgungsbehörden gelangt. Gerade am Quellenschutz des Journalisten, bei dem es zentral darum geht, wer mit wem kommuniziert, zeigt sich, wie einschneidend es sein kann, wenn Vorratsdaten an die Strafverfolgungsbehörden gelangen. Anders als etwa beim Anwalt, wo es in der Regel zentral um den Inhalt der Kommunikation gehen wird – etwa zwischen Angeschuldigtem und Verteidiger –, ist es beim journalistischen Quellenschutz primär entscheidend,

dass keine entsprechenden Metadaten bekannt werden, welche Rückschlüsse auf die Kommunikationspartner ermöglichen.

48. Hinzu kommt, dass eine selektive Löschung der dem Zeugnisverweigerungsrecht des Journalisten unterstehenden Daten mitunter gar nicht möglich ist. In der Praxis ist eine teilweise Entfernung von Daten nicht oder nur eingeschränkt möglich. Es bedarf jedenfalls einer Anordnung durch die Staatsanwaltschaft, was wiederum voraussetzt, dass die Staatsanwaltschaft die entsprechenden Daten zuvor zur Kenntnis genommen hat (vgl. HANSJAKOB, StPO-Kommentar, Art. 271 StPO N 15 ff.).
49. Es bestehen damit keine wirksamen Schutzmechanismen gegen die mit der Vorratsdatenspeicherung verbundene Kompromittierung des Quellenschutzes. Der Journalist muss damit rechnen, dass Vorratsdaten, die durch die Kommunikation mit Quellen anfallen, in einem Strafverfahren beigezogen werden und so seine Quellen offen legen. Der Quellenschutz ist damit durch die Vorratsdatenspeicherung beeinträchtigt und kann nicht mehr garantiert werden, sobald der Journalist Kommunikationsmittel verwendet, die der Vorratsdatenspeicherung unterliegen. Die mit der Vorratsdatenspeicherung verbundenen Einschränkungen der Grundrechte wiegen damit für ihn besonders schwer, einschliesslich des darin enthaltenen «chilling effects». Die Vorratsdatenspeicherung beeinträchtigt damit seine Arbeit bzw. seine Arbeitsweise nachhaltig, zumal er als Journalist eigentlich essenziell auf Kommunikation und die Nutzung zeitgemässer Kommunikationskanäle angewiesen ist. Der Journalist steht vor der Wahl, sich bei der Kommunikation, die der Vorratsdatenspeicherung unterliegt, vom Quellenschutz zu verabschieden, oder aber, diese Kommunikationsformen nicht mehr zu nutzen. Die mit der Vorratsdatenspeicherung verbundenen Verletzung der Grundrechte des Journalisten wiegt damit besonders schwer.

C. *Schlussfolgerungen*

1. Von den vorstehenden Grundrechtsverletzungen durch die Vorratsdatenspeicherung ist der Gesuchsteller als Kunde der Anbieterin konkret betroffen. Die Anbieterin muss die entsprechenden, ihn betreffenden Daten während 6 Monaten aufbewahren. Dies ist, wie dargelegt, mit den Grundrechten des Gesuchstellers nicht vereinbar.
2. In seiner journalistischen Tätigkeit hat der Gesuchsteller einen Schwerpunkt im Bereich Recherche. Er publiziert u.a. regelmässig kritische Artikel zur Justiz in der Schweiz. Er ist in seiner journalistischen Tätigkeit essenziell darauf angewiesen, dass der Schutz seiner journalistischen Quellen gewährleistet ist.
3. Zur Wahrung der Grundrechte bzw. zur Wiederherstellung eines grundrechtskonformen Zustands ist die Anbieterin deshalb anzuweisen, die im Rahmen der Vorratsdatenspeicherung aufbewahrten Daten zu löschen, und inskünftig keine Vorratsdaten zu speichern, soweit die betroffenen

Daten nicht für die Erbringung der vertraglichen Leistungen gegenüber dem Gesuchsteller zwingend erforderlich sind. Weiter ist Anbieterin anzuweisen bzw. zu verpflichten, keine Daten im Rahmen des BÜPF an den Dienst ÜPF oder an andere Behörden oder an Gerichte herauszugeben.

Abschliessend ersuche ich Sie um Gutheissung der eingangs gestellten Anträge.

Mit freundlichen Grüssen



Viktor Györffy

Beilagen:

1. Vollmacht in Kopie
2. Vertrag in Kopie