

**Bericht des Bundesrates in Erfüllung des Postulats 14.3672
der Sicherheitspolitischen Kommission des Ständerates
vom 1. September 2014.
Demonstrationen und Grossanlässe. Bekanntgabe von In-
ternetadressen**

vom ...

Übersicht

Der Bundesrat legt diesen Bericht in Erfüllung des Postulats der sicherheitspolitischen Kommission des Ständerates vom 1. September 2014 (14.3672) «Demonstrationen und Grossanlässe. Bekanntgabe von Internetadressen» vor. Mit dem Postulat wurde der Bundesrat beauftragt, bis Mitte 2015 in einem Bericht darzulegen, wie der Inhalt der Standesinitiative des Kantons Bern 14.305 "Fertig mit dem anonymen Aufruf zu Demonstrationen und Grossanlässen ohne Übernahme von Verantwortung" allenfalls umgesetzt werden könnte.

Die Standesinitiative des Kantons Bern fordert gesetzliche Grundlagen für die Bekanntgabe von Internetadressen an die Polizeibehörden, um im Vorfeld von Demonstrationen und Grossanlässen die Anonymität von Organisatoren aufzuheben und mit ihnen verbindliche Abmachungen zu treffen und Haftungsfragen klären zu können.

Der erste Teil des Berichtes enthält eine Analyse des Ist-Zustandes sowie der Möglichkeiten, wie sie sich gemäss den Entwürfen zur Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs und des neuen Nachrichtendienstgesetzes darstellen. In einem weiteren Schritt wird auf die verfassungsmässigen Zuständigkeiten der Kantone im Polizeibereich und die Kompetenzaufteilung zwischen Bund und Kantonen bei der Bekanntgabe von Internetadressen ausserhalb eines Strafverfahrens eingegangen. Zudem wird auch die damit zusammenhängende Grundrechtsproblematik thematisiert.

Ziel des Berichts ist es, eine Gesamtübersicht über die bestehenden kantonalen Zuständigkeiten und Bundeszuständigkeiten zu bieten und dabei den Hauptakzent auf die im Postulat und in der Standesinitiative erläuterten Fragestellungen zu legen.

Der Bundesrat kommt im vorliegenden Bericht zum Schluss, dass für die Bekanntgabe von Internetadressen ausserhalb eines Strafverfahrens sowohl umfassende Kompetenzen der Kantone als auch des Bundes zum Tragen kommen, nämlich die Polizeihoheit der Kantone einerseits und die Kompetenz des Bundes im Bereich des Fernmeldewesens andererseits. Soweit es um die eigentliche polizeiliche (Ermittlungs-) Tätigkeit geht, ist die Zuständigkeit der Kantone gegeben; wo die technische Umsetzung der Teilnehmeridentifikation Platz greift, kann für die Bundeskompetenz Artikel 92 Absatz 1 BV – in Verbindung mit Art. 57 Absatz 2 BV – herangezogen werden. Die Statuierung der Bedingungen für die Nutzung des Instruments obliegt hingegen den Kantonen. Es obliegt demnach in erster Linie den Kantonen, gesetzliche Regelungen zu schaffen, welche dem Verhältnismässigkeitsprinzip angemessen Rechnung tragen. Sofern das Bedürfnis nach einer gewissen Rechtsvereinheitlichung besteht, bleibt es den Kantonen unbenommen, die notwendigen Regelungen mittels interkantonalen Vereinbarungen zu regeln.

Inhaltsverzeichnis

Übersicht	2
Inhaltsverzeichnis	3
Abkürzungsverzeichnis	5
1. Auftrag und Organisation der Arbeiten	6
1.1 Einleitung	6
1.1.1 Ausgangslage	6
1.1.2 Vorgehen	7
1.2 Auftrag	7
1.2.1 Schnittstellen zu anderen Berichten und Projekten	7
1.2.1.1 Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs	8
1.2.1.2 Nachrichtendienstgesetz	8
1.2.2.3 Interdepartementale Arbeitsgruppe zur Providerhaftung	8
2. Bekanntgabe von Internetadressen de lege lata und de lege ferenda	9
2.1 Möglichkeiten gestützt auf StPO und BÜPF	9
2.1.1 Möglichkeiten ausserhalb von Strafverfahren - Suche von vermissten Personen (Art. 1 und Art. 3 BÜPF)	9
2.1.2 Möglichkeiten in Strafverfahren - Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet gemäss Artikel 14 Abs. 4 BÜPF	9
2.1.3 De lege ferenda: Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet (Art. 22 E-BÜPF)	11
2.1.4 De lege ferenda: Notsuche und Fahndung (Art. 35 und Art. 36 E-BÜPF)	12
2.2 Möglichkeiten gestützt auf das BWIS und auf das Nachrichtendienstgesetz	13
2.2.1 Auskünfte über Teilnehmeradressen (Art. 13 Abs. 1 ^{bis} BWIS, Art. 24 Abs. 2 E-NDG)	13
2.2.2 Genehmigungspflichtige Überwachung nach Artikel 25 Absatz 1 Buchstabe a E-NDG	14
3. Verfassungsmässige Zuständigkeiten in Bezug auf die Bekanntgabe von Internetadressen ausserhalb eines Strafverfahrens	15
3.1 Ausgangslage	15
3.2 Verfassungsrechtliche Zuständigkeiten auf dem Gebiet des Polizeiwesens	16
3.3 Kompetenzaufteilung zwischen Bund und Kantonen bei der Bekanntgabe von Internetadressen ausserhalb eines Strafverfahrens	17
4. Regelung zur Aufhebung der Anonymität von aufrufenden Personen	19
4.1 Ausgangslage	19
4.2 Grundrechtsrelevanz der Massnahme (insbes. der Bekanntgabe von Internetadressen)	19

4.3 Öffentliches Interesse	20
4.4 Verhältnismässigkeit	21
5.Schlussfolgerungen	23

Abkürzungsverzeichnis

BBl	Bundesblatt
BJ	Bundesamt für Justiz
BV	Bundesverfassung
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (SR 780.1)
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (SR 120)
E-BÜPF	Entwurf Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
EJPD	Eidgenössisches Justiz- und Polizeidepartement
fedpol	Bundesamt für Polizei
ff.	und folgende Seite(n)
KKJPD	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
KKPKS	Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten
m.a.H	mit anderen Hinweisen
NDB	Nachrichtendienst des Bundes
NDG	Nachrichtendienstgesetz
S.	Seite(n)
SIK-SR	Sicherheitspolitische Kommission des Ständerates
SR	Systematische Sammlung des Bundesrechts
StGB	Strafgesetzbuch (SR 311.0)
StPO	Strafprozessordnung (SR 312.0)
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
vgl.	vergleiche
z.B.	zum Beispiel

Bericht

1. Auftrag und Vorgehen

1.1 Einleitung

1.1.1 Ausgangslage

Mit dem vorliegenden Bericht erfüllt der Bundesrat das Postulat der sicherheitspolitischen Kommission des Ständerates (14.3672) «Demonstrationen und Grossanlässe. Bekanntgabe von Internetadressen» vom 1. September 2014. Das Postulat hat folgenden Wortlaut:

«Der Bundesrat wird beauftragt, bis Mitte 2015 in einem Bericht darzulegen, wie der Inhalt der Standesinitiative des Kantons Bern 14.305 "Fertig mit dem anonymen Aufruf zu Demonstrationen und Grossanlässen ohne Übernahme von Verantwortung" allenfalls umgesetzt werden könnte».

Der Grosse Rat des Kantons Bern hat in der Januarsession 2014 eine Motion überwiesen, mit welcher der Regierungsrat beauftragt wird, beim Bund die Standesinitiative 14.305 "Fertig mit dem anonymen Aufruf zu Demonstrationen und Grossanlässen ohne Übernahme von Verantwortung" einzureichen. Die Standesinitiative fordert gesetzliche Grundlagen für die Bekanntgabe von Internetadressen an die Polizeibehörden, um im Vorfeld von Demonstrationen und Grossanlässen die Organisatoren ausfindig zu machen, mit ihnen verbindliche Abmachungen zu treffen und Haftungsfragen klären zu können.

Am 19. März 2014 hat der Regierungsrat des Kantons Bern die Standesinitiative an die Vereinigte Bundesversammlung eingereicht. In der Folge hat die Sicherheitspolitische Kommission des Ständerates (SIK-SR) anlässlich der Sitzung vom 15. August 2014 beschlossen, der Standesinitiative keine Folge zu geben und ein Kommissionspostulat einzureichen.

Der Bundesrat hat in seiner Antwort vom 29. Oktober 2014 die Ablehnung des Postulats beantragt. Er führte in seiner Stellungnahme im Wesentlichen aus, dass der Grundsatz der Verhältnismässigkeit nicht gewahrt sei, wenn die Identität der anonymen Personen bekannt gegeben werde, und deren Aufruf zu Demonstrationen oder anderen Grossanlässen keine Aufforderung zu Verbrechen oder Gewalttätigkeiten enthalte. Unter anderem könnten bei allfälligen Störungen an einem Anlass die Organisatoren nicht ohne weiteres straf- und zivilrechtlich zur Verantwortung gezogen werden; der Aufruf zu einer nicht bewilligten Demonstration allein ist keine Straftat gemäss Schweizerischem Strafgesetzbuch (StGB; SR 311.0). Die Bekanntgabe dieser Informationen an die Polizeibehörden für rein präventive Zwecke sei demnach nicht zulässig. Ausserdem würde die Regelung gegen die verfassungsrechtlich garantierte Versammlungsfreiheit (Art. 22 Bundesverfassung der Schweizerischen Eidgenossenschaft [BV]; SR 101) verstossen.

Am 10. Dezember 2014 wurde das Postulat vom Ständerat angenommen. Es wurde allerdings für die Ausarbeitung des Berichtes aufgrund des notwendigen Einbezugs der Kantone eine Fristverlängerung von Frühjahr 2015 auf Herbst 2015 gewährt.

1.1.2 Vorgehen

In der Schweiz befassen sich verschiedene Bundesstellen mit Sicherheitsfragen im Zusammenhang mit der Internetüberwachung. Entsprechend war es für die Erfüllung des Postulats unerlässlich, auf deren Fachwissen in Theorie und Praxis zurückzugreifen. Dies umso mehr, als das Postulat der sicherheitspolitischen Kommission des Ständerates nicht nur eine Analyse der kompetenzrechtlichen Problematik, sondern auch eine Darstellung des faktischen Ist-Zustandes im Bereich der Bekanntgabe von Internetadressen ausserhalb eines Strafverfahrens verlangt. Das federführende Bundesamt für Polizei (fedpol) setzte deshalb eine Arbeitsgruppe ein, die sich aus Fachpersonen von fedpol, des Bundesamtes für Justiz (BJ), des Dienstes für die Überwachung des Post- und Fernmeldeverkehrs (ÜPF) und des VBS (Nachrichtendienst des Bundes [NDB]) zusammensetzte.

Die Fragestellung im Postulat der sicherheitspolitischen Kommission des Ständerates berührt Belange der inneren Sicherheit, für welche primär die Kantone zuständig sind. Deshalb wurden die Kantone in einer informellen Konsultation der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren KKJPD begrüsst.

1.2 Auftrag und Inhalt

Mit dem Postulat der sicherheitspolitischen Kommission des Ständerates wird der Bundesrat beauftragt, in einem Bericht darzustellen, wie der Inhalt der Standesinitiative des Kantons Bern allenfalls umgesetzt werden könnte.

Der erste Teil enthält eine Analyse des Ist-Zustandes sowie eine Bestandsaufnahme der diesbezüglichen Aufgabenverteilung zwischen Bund und Kantonen. In einem weiteren Schritt wird auf die Zuständigkeiten der Kantone in Bezug auf die Bekanntgabe von Internetadressen ausserhalb eines Strafverfahrens und auf die damit zusammenhängende Grundrechtsproblematik eingegangen. Zudem wird die Bundeszuständigkeit für die Bewilligung der Überwachung des Fernmeldeverkehrs thematisiert.

Ziel des Berichts ist es, eine Gesamtübersicht über die bestehenden kantonalen und Bundeszuständigkeiten in diesem Bereich zu bieten und dabei den Hauptakzent auf die im Postulat und in der Standesinitiative erläuterten Fragestellungen zu legen.

1.2.1 Schnittstellen zu anderen Berichten und Projekten

Auf Bundesebene haben sich mehrere Projekte und eine interdepartementale Arbeitsgruppe mit Sicherheitsfragen im Zusammenhang mit dem Internet befasst. Die Erkenntnisse dieser Projekte wurden bei der Erarbeitung des vorliegenden Berichts berücksichtigt. Die wichtigsten Projekte und die (vorläufigen) Arbeitsergebnisse der interdepartementalen Arbeitsgruppe werden nachfolgend beschrieben.

1.2.1.1 Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs

Der Bundesrat hat am 27. Februar 2013 die Botschaft und den Entwurf für die Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (im Folgenden: E-BÜPF) vorgelegt.¹ Mit der Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR 780.1) soll sichergestellt werden, dass die notwendigen Überwachungen des Post- und Fernmeldeverkehrs durch die Verwendung neuer Technologien (wie etwa verschlüsselter Internettelefonie) nicht verhindert werden können. Das BÜPF wird deshalb an die technische Entwicklung der letzten Jahre und, im Rahmen des Möglichen, an die absehbaren künftigen technologischen Entwicklungen angepasst. Das Ziel der Revision besteht darin, die Telefonüberwachung besser vollziehen zu können, namentlich die Überwachung von Personen zu ermöglichen, gegen die ein dringender Verdacht auf Begehung einer schweren Straftat besteht. Ein weiteres Ziel besteht darin, Überwachungen ausserhalb von Strafverfahren durchführen zu können, um vermisste Personen zu suchen oder nach geflohenen Personen fahnden zu können. Die Gesetzesvorlage wurde am 27. Februar 2013 vom Bundesrat zur Verabschiedung dem Parlament vorgelegt.

1.2.1.2 Nachrichtendienstgesetz

Das Nachrichtendienstgesetz (NDG) soll die künftige gesetzliche Grundlage für den zivilen Nachrichtendienst der Schweiz bilden. Das NDG regelt Aufgaben, Schranken und Kontrolle des NDB im In- und Ausland. Es schafft die Voraussetzungen für das rechtzeitige Erkennen von Bedrohungen und Gefahren zum Schutz der Schweiz und kann unter bestimmten Voraussetzungen auch zur Wahrung wesentlicher Landesinteressen - wie dem Schutz kritischer Infrastrukturen und des Finanz- und Wirtschaftsplatzes oder bei Entführungen von Schweizer Bürgerinnen und Bürgern im Ausland - eingesetzt werden. Namentlich werden einige Informationsbeschaffungsmassnahmen wie z.B. die Überwachung des Post- und Fernmeldeverkehrs in den Bereichen Terrorismus, verbotener Nachrichtendienst, Proliferation und Angriffe auf kritische Infrastrukturen oder zur Wahrung weiterer wesentlicher Landesinteressen eingeführt. Der Bundesrat hat am 19. Februar 2014 die Botschaft² und den Entwurf zum NDG zuhanden des Parlaments verabschiedet.

1.2.2.3 Interdepartementale Arbeitsgruppe zur Providerhaftung

Eine interdepartementale Arbeitsgruppe zur Providerhaftung untersucht zurzeit aus Sicht des Zivilrechts den gesetzgeberischen Handlungsbedarf und leuchtet dazu die Rechtsgrundlagen zur zivilrechtlichen Verantwortlichkeit von Providern u.a. im Persönlichkeits-, Immaterialgüter- und Wettbewerbsrecht aus. Sie prüft dabei alle Aspekte der zivilrechtlichen Verantwortlichkeit (z.B. Ansprü-

¹ Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, BBl 2013 2683 ff., Entwurf BBl 2013 2789 ff.

² Vgl. BBl 2014 2105 ff.

che auf Beseitigung, Unterlassung oder Schadenersatz) und wird gegebenenfalls bis Ende 2015 eine Vernehmlassungsvorlage erarbeiten.

2. Bekanntgabe von Internetadressen de lege lata und de lege ferenda

2.1 Möglichkeiten gestützt auf StPO und BÜPF

Der Bund regelt die Modalitäten der Überwachung des Post- und Fernmeldeverkehrs im BÜPF. Die Voraussetzungen einer Überwachung im Rahmen eines Strafverfahrens werden in den Artikeln 269 ff. der Schweizerischen Strafprozessordnung (StPO, SR 312.0) geregelt.

2.1.1. Möglichkeiten ausserhalb von Strafverfahren - Suche von vermissten Personen (Art. 1 und Art. 3 BÜPF)

Artikel 3 Absatz 1 BÜPF bietet in Verbindung mit Artikel 1 Absatz 1 Buchstabe c BÜPF die Möglichkeit, auch ausserhalb eines Strafverfahrens eine Überwachungsmassnahme anzuordnen, um den Aufenthaltsort einer Person herauszufinden, wenn angenommen wird, dass eine schwere Gefährdung ihrer Gesundheit oder ihres Lebens besteht. Dabei dürfen auch Daten von unbeteiligten Dritten angefordert werden. Es handelt sich dabei um eine notstandsähnliche Lage, in der das höchste aller strafrechtlich geschützten Rechtsgüter unmittelbar bedroht ist und gerettet werden soll. Die Anordnung einer Echtzeitüberwachung ist ausgeschlossen (d.h. es dürfen keine Kommunikationsinhalte übermittelt werden). De lege lata ist die Anordnung einer solchen Überwachungsmassnahme die einzige Ausnahme vom Grundsatz, dass Überwachungen nur im Rahmen eines Strafverfahrens des Bundes oder der Kantone angeordnet werden können.

2.1.2 Möglichkeiten in Strafverfahren - Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet gemäss Artikel 14 Abs. 4 BÜPF

Bevor der Artikel 14 Absatz 4 BÜPF weiter ausgeführt werden kann, muss auf den persönlichen Geltungsbereich des geltenden BÜPF eingegangen werden.

Der persönliche Geltungsbereich umfasst gemäss Artikel 1 Absatz 2 BÜPF neben den Betreiberinnen von internen Fernmeldenetzen und Hauszentralen nur die Anbieterinnen von Post- und Fernmeldediensten und die Internetzugangsanbieterinnen.

Anbieterinnen abgeleiteter Kommunikationsdienste (so etwa Soziale Netzwerke wie Facebook) fallen nicht in den persönlichen Geltungsbereich des BÜPF und unterliegen auch nicht dessen Pflichten. Sie stellen Dienste bereit, nutzen jedoch für den Datentransport die Infrastruktur der Fernmeldediensteanbieterinnen (im Falle der Dienstleistungsanbietung über das Internet, die Infrastruktur der Internetzugangsanbieterinnen). Es ist für die Internetzugangsanbieterinnen alleine technisch nicht möglich, an die Daten zu gelangen, die etwa einen Urheber eines Postings auf einem Sozialen Netzwerk identifizieren können. Dafür bräuchte man zusätzliche Daten der Anbieterinnen von abgeleiteten

Kommunikationsdiensten.³ Der Zugang zu diesen Daten ist für den Dienst ÜPF jedoch mangels Unterstellung dieser Anbieterinnen unter das BÜPF de lege lata nicht möglich.

Die Bekanntgabe von IP-Adressen zur Identifikation einer unbekanntes Täterschaft bei einer Straftat über das Internet wird im Artikel 14 Absatz 4 BÜPF geregelt.

Die Identifikation erfolgt mittels Anfrage der Strafverfolgungsbehörden bei den Internetzugangsanbieterinnen, welchem Internetzugang sie zu einem bestimmten Zeitpunkt eine bestimmte dynamische IP-Adresse zugewiesen haben.⁴

Dynamische IP-Adressen gehören, im Gegensatz zu statischen IP-Adressen, zu den Randdaten des Internetverkehrs.⁵ Randdaten enthalten keine Kommunikationsinhalte, sondern zeigen auf, wer, wo, mit wem und wie lange kommuniziert hat. Diese Randdaten müssen gemäss Artikel 15 Absatz 3 BÜPF sechs Monate aufbewahrt werden. Grundsätzlich dürfen diese Daten nur herausgegeben und verwertet werden, wenn dies von der Staatsanwaltschaft angeordnet und vom Zwangsmassnahmengericht genehmigt wird. Anordnung und Genehmigung darf nur bei Strafverfahren wegen eines Verbrechens oder Vergehens unter Wahrung des Verhältnismässigkeitsprinzips erfolgen (Art. 273 StPO). Für Strafverfahren wegen einer Übertretung dürfen diese Randdaten nicht erhoben und verwertet werden (einzige Ausnahme bildet der Missbrauch einer Fernmeldeanlage gemäss Art. 179^{septies} StGB).

Artikel 14 Absatz 4 BÜPF durchbricht als *lex specialis* diesen Grundsatz von Artikel 273 StPO.⁶ Zur Identifikation von Urhebern einer Straftat über das Internet dürfen diese Randdaten ohne Anordnung des Staatsanwaltes und ohne Genehmigung eines Zwangsmassnahmengerichts herausgegeben und verwertet werden.⁷ Im Gegensatz zu Artikel 273 StPO schränkt Artikel 14 Absatz 4 die Deliktsart nicht ein. Selbst für eine Übertretung kann eine Teilnehmeridentifikation verlangt werden (allerdings nur bei Begehung einer Straftat über das Internet).⁸

Bei einer öffentlichen Aufforderung zu Verbrechen gemäss Artikel 259 Absatz 1 StGB kann nicht nur eine Teilnehmeridentifikation, sondern sogar eine Echt-

³ Allerdings ist denkbar, dass die Staatsanwaltschaft diese Informationen beschlagnahmt.

⁴ Zur Funktion von dynamischen IP-Adressen vgl. etwa BGE 136 II 508, 514 f.

⁵ Hansjakob, Kommentar BÜPF, Art. 14 BÜPF N 26.

⁶ Vgl. BGE 139 IV 98; dieser Entscheid betrifft v.a. die Frage der zeitlichen Dimension, nicht die Frage des Genehmigungsverfahrens, was vorliegend abgehandelt wird. Diesen Entscheid hat das Bundesgericht später wieder relativiert.

⁷ Entscheid der Rekurskommission des Eidgenössischen Departements für Umwelt, Verkehr, Energie und Kommunikation vom 27. April 2004 im Beschwerdeverfahren J-2003-162 (Fob) E. 6.2.1 ff. (abrufbar unter www.rekoinum.ch/dokumente/114010669724120.pdf) mit Hinweisen zur Entstehungsgeschichte von Art. 14 Abs. 4 BÜPF. A. A. Trechsel/Lieber, StGB Praxiskommentar, Art. 179^{octies} N 5 mit Verweis auf BGE 126 I 60. In Art. 14 Abs. 2 und Abs. 2^{bis} BÜPF sind alle auskunftsberechtigten Stellen aufgeführt. Vgl. aber auch BGE 1B_344/2014 E. 5.1, wo das BG ausgeführt hat, dass wenn den Strafverfolgungsbehörden lediglich strafbare Internet- Kommunikationsaktivitäten bekannt geworden sind (zum Beispiel Postings auf sozialen Netzwerken) und über die Verbindungs-Randdaten der betreffenden Internet-Kommunikation die zugewiesenen IP-Adressen und registrierten Kunden erst eruiert werden sollen (sogenannte "IP-History"), bei Überwachungen die Vorschriften von Art. 273 StPO anwendbar sind (vgl. aber Botschaft BÜPF, BBl 2013 2683, 2743; BGE 126 I 50 E. 5-6 S. 60-67; s.a. unten, Ziff. 2.1.3).

⁸ Hansjakob, Kommentar BÜPF, Art. 14 BÜPF N 23.

zeit- oder Inhaltsüberwachung des Post- und Fernmeldeverkehrs (somit auch des Internetverkehrs) angeordnet werden (siehe Art. 269 Abs. 2 Bst. a StPO⁹). Die Randdaten können gemäss Art. 273 StPO auch eingefordert werden (vgl. jedoch die Ausführungen über den Geltungsbereich von Art. 1 BÜPF). Bei einem Aufruf zu einem Vergehen mit Gewalttätigkeit gegen Menschen oder Sachen gemäss Artikel 259 Absatz 2 StGB können die Randdaten nur eingefordert werden, wenn die Voraussetzungen von Artikel 269 Absatz 1 Buchstaben b und c StPO erfüllt sind.

Der Aufruf zu einer nicht bewilligten Demonstration ohne Aufruf zu Straftaten ist dagegen keine Straftat nach dem Schweizerischen Strafgesetzbuch. Der Aufruf zu einer nicht bewilligten Spontankundgebung kann jedoch eine kantonale Strafnorm oder eine Strafbestimmung in einem Gemeindereglement erfüllen, so etwa gemäss Artikel 8 Absatz 1 Buchstabe b des Reglements über Kundgebungen auf öffentlichem Grund der Stadt Bern. Im Lichte des Verhältnismässigkeitsprinzips erscheint es allerdings ausgeschlossen, dass eine solche Übertretung genügt, um eine Identifikation gemäss Artikel 14 Absatz 4 zu legitimieren, geht es doch um Informationen, die durch das Fernmeldegeheimnis verfassungsmässigen Schutz geniessen.¹⁰

Gemäss Artikel 14 Absatz 2 Buchstabe b BÜPF kann das Gesuch um Identifikation von fedpol und den kantonalen und städtischen Polizeikommandos aussehen. Die Polizeibehörden können diese Anfragen gemäss Artikel 14 Absatz 4 BÜPF für die Erfüllung von Polizeiaufgaben stellen.¹¹

2.1.3 De lege ferenda: Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet (Art. 22 E-BÜPF)

Wie in Ziffer 1.2.2.1 erwähnt, hat der Bundesrat am 27. Februar 2013 die Botschaft und den Entwurf für die Totalrevision des BÜPF dem Parlament vorgelegt. Die Vorlage befindet sich zurzeit in der parlamentarischen Beratung.

Artikel 22 E-BÜPF (Auskünfte zur Identifikation der Täterschaft bei Straftaten über das Internet) wird im Kern aus Artikel 14 Absatz 4 des geltenden BÜPF übernommen. Die Abweichungen von Artikel 22 Absatz 1 E-BÜPF zu Artikel 14 Absatz 4 BÜPF sind vorwiegend redaktioneller Natur; der Entwurf des Bundesrates schafft materiell keine Änderungen. Es wird deshalb auf das vorstehend unter Ziffer 2.1.2 Ausgeführte verwiesen. Es bleibt hervorzuheben, dass diese Teilnehmeridentifikation nur im Rahmen von Strafverfahren möglich ist (Verdacht auf eine Straftat erforderlich).

Neu sind hingegen die Absätze 3 und 4 von Artikel 22 E-BÜPF; sie sind eine Folge des ausgedehnten persönlichen Geltungsbereiches und betreffen sogenannte „Anbieterinnen abgeleiteter Kommunikationsdienste“.¹² Solche Anbieter-

⁹ Bestehen eines dringenden Tatverdachtes gegen eine bestimmbare Person, die Schwere der öffentlichen Aufforderung die Überwachung rechtfertigt, die bisherigen Untersuchungen erfolglos blieben oder die Ermittlungen aussichtslos wären oder unverhältnismässig erschwert würden.

¹⁰ BGE 136 II 508; vgl. hierzu insbesondere auch BGE 1B_344/2014.

¹¹ Hansjakob, Kommentar BÜPF, Art. 14 BÜPF N 18, der hier eine grosszügige Regelung erkennt "... denn Polizeiaufgaben werden natürlich nicht nur im Zusammenhang mit Strafverfahren wahrgenommen".

¹² Vgl. Art. 2 Bst. c E-BÜPF.

rinnen (z. B. reine Email-Provider, Hosting-Provider oder Soziale Netzwerke wie Facebook) erbringen keine klassischen Fernmeldedienste, da sie Daten nicht selber übertragen.¹³ Auch diese Anbieterinnen verfügen über Angaben, die bei der Teilnehmeridentifikation bei Straftaten über das Internet von Nutzen sein können (insb. IP-Adressen). Absatz 3 verlangt, dass sie die ihnen vorliegenden Angaben herausgeben müssen. Das ist im Grundsatz eine strafprozessuale Selbstverständlichkeit. Der Bundesrat kann allerdings zum Schluss gelangen, dass dies für eine effiziente Identifikation von Straftätern, welche ein Delikt über das Internet begangen haben, nicht ausreicht. Deshalb ermöglicht ihm Absatz 4, wichtige Anbieterinnen abgeleiteter Kommunikationsdienste unter ganz bestimmten Bedingungen zur Lieferung von zusätzlichen Angaben zu verpflichten. Als Vorlage dienen dabei die Angaben, die von den klassischen Fernmeldedienstanbieterinnen geliefert werden müssen. Auf diese Weise könnten Anbieterinnen abgeleiteter Kommunikationsdienste verpflichtet werden, gewisse Daten auf Vorrat zu speichern.

Aufgrund des Territorialitätsprinzips können jedoch viele bedeutende Anbieterinnen abgeleiteter Kommunikationsdienste nicht ins schweizerische Recht gefasst werden, wenn sie ihren Sitz und ihre Infrastruktur im Ausland haben.¹⁴

Für Einzelheiten dazu sei auf die Botschaft E-BÜPF verwiesen (BBl 2013 2736).

2.1.4 De lege ferenda: Notsuche und Fahndung (Art. 35 und Art. 36 E-BÜPF)

Artikel 35 E- BÜPF regelt die Notsuche nach vermissten Personen. Anders als das geltende Recht¹⁵ beschränkt Absatz 1 die Mittel für die Notsuche nicht auf die Teilnehmeridentifikation und die Verkehrsdaten (d.h. Randdaten). Neu soll es zulässig sein, auch den Inhalt der Kommunikation zu erhalten.

Die im geltenden Recht¹⁶ vorgesehene Bedingung, dass der Aufenthaltsort der vermissten Person unbekannt ist, wird in Absatz 2 durch eine Alternative ergänzt: Den unverhältnismässig schwer zu ermittelnden Aufenthaltsort.

Für die Notsuche soll gemäss Absatz 3 neu unter bestimmten Voraussetzungen auch der Einsatz von technischen Überwachungsgeräten (insb. IMSI-Catcher) gestützt auf Artikel 269^{bis} StPO zur Identifikation mobiler Kommunikationsgeräte zulässig sein. Mit diesen Geräten lässt sich eine vermisste Person möglicherweise selbst dann auffinden, wenn sich die klassischen Überwachungsmassnahmen als unwirksam erwiesen haben.

Wie bereits im geltenden Recht¹⁷ darf gemäss Absatz 4 unter Berücksichtigung des Verhältnismässigkeitsgrundsatzes nicht nur die Kommunikation der gesuchten Person, sondern gegebenenfalls auch jene einer unbeteiligten Drittperson überwacht werden.

¹³ Vgl. eingehend Botschaft E-BÜPF, 2707 f.

¹⁴ Vgl. Urteil des Bundesgerichts 1B_344/2014 vom 14. Januar 2015, wo das Bundesgericht u.a. entschieden hat, dass für die von der Staatsanwaltschaft beabsichtigten Datenerhebungen (bzw. rückwirkenden Überwachungen) in den USA der Weg der internationalen Rechtshilfe in Strafsachen zu beschreiten ist.

¹⁵ Vgl. Art. 3 Abs. 1 BÜPF.

¹⁶ Vgl. Art. 3 Abs. 2 BÜPF.

¹⁷ Vgl. Art. 3 Abs. 1 BÜPF.

Für Einzelheiten dazu sei auf die Botschaft E-BÜPF verwiesen (BB1 2013 2754 f).

Artikel 36 E-BÜPF regelt die Fahndung nach verurteilten Personen. Diese neue Bestimmung sieht vor, mittels Überwachung des Post- und Fernmeldeverkehrs nach einer Person zu suchen, gegen die in einem rechtskräftigen und vollstreckbaren Entscheid eine Freiheitsstrafe oder eine freiheitsentziehende Massnahme verhängt wurde. Das Strafverfahren ist hier zwar bereits formell abgeschlossen, der direkte Bezug zum Strafrecht aber immer noch gegeben.

Die Überwachung bei einer Fahndung ist gemäss Absatz 1 – wie bei einer Notsuche¹⁸ – subsidiär zu anderen Massnahmen, die geeignet sind, um die flüchtige Person zu finden. Es ist zulässig, nicht nur Randdaten, sondern auch Kommunikationsinhalte auszuwerten, weil diese ebenfalls wichtige Hinweise auf den Aufenthaltsort liefern können. Es wird keine Mindestdauer der Freiheitsstrafe vorgegeben, um eine Überwachung anordnen zu können. Bei ihrem Entscheid über die Anordnung einer Überwachung muss sich die zuständige Behörde jedoch vom Grundsatz der Verhältnismässigkeit leiten lassen. Zu berücksichtigen sind dabei die Dauer der Freiheitsstrafe, die Straftat, die Gefährlichkeit der geflohenen Person und die Kosten der Überwachung.

Für die Fahndung ist gemäss Absatz 2 unter bestimmten Voraussetzungen auch der Einsatz von technischen Überwachungsgeräten (insb. IMSI-Catcher) zulässig.

Wie bei der Notsuche darf gemäss Absatz 3 unter Berücksichtigung des Verhältnismässigkeitsgrundsatzes nicht nur die Kommunikation der geflohenen Person, sondern gegebenenfalls auch jener einer unbeteiligten Drittperson überwacht werden.

Für Einzelheiten dazu sei auf die Botschaft zum E-BÜPF verwiesen (BB1 2013 2755 f).

2.2 Möglichkeiten gestützt auf das BWIS und auf das Nachrichtendienstgesetz

2.2.1 Auskünfte über Teilnehmeradressen (Art. 13 Abs. 1^{bis} BWIS, Art. 24 Abs. 2 E-NDG)

Artikel 13 des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS; SR 120) regelt, welche Behörden und Amtsstellen zu Auskünften an den NDB verpflichtet sind. Absatz 1 listet die zur Auskunft verpflichteten Behörden und Amtsstellen auf (z.B. Grenzschutz- und Zollorgane oder Einwohnerkontrollen). Absatz 1^{bis} ergänzt diese Auflistung mit dem Dienst ÜPF. Diese Ergänzung von Absatz 1 wurde notwendig, weil nach dem seinerzeitigen Transfer der mit nachrichtendienstlichen Aufgaben befassten Organisationseinheiten von fedpol bzw. des EJPD zum VBS für diese keine ausdrückliche Rechtsgrundlage mehr für entsprechende Auskünfte bestand (da nicht mehr fedpol zugehörig) und deshalb neu geschaffen werden musste. Dabei wurde bewusst ein eigenständiger Ansatz gewählt, um die Unterscheidung zwischen

Vgl. Art. 35 Abs. 2 Bst. a E-BÜPF.

den Strafverfolgungsbehörden einerseits und dem NDB als präventiv tätiger Behörde andererseits zu betonen. Zudem ist das Auskunftsrecht auf die Erfüllung nachrichtendienstlicher Aufgaben beschränkt (vgl. die Zusatzbotschaft zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit [„BWIS II reduziert“]; BBl 2010 7870 ff.). Die zur Auskunft verpflichtete Behörde oder Amtsstelle ist der Dienst ÜPF; es besteht keine Auskunftspflicht von Privaten.

Artikel 24 Absatz 2 E-NDG übernimmt die bestehende Regelung von Artikel 13 Absatz 1^{bis} BWIS und geht inhaltlich nicht darüber hinaus. Der Verweis auf Artikel 14 Absatz 2 BÜPF ermöglicht das Einholen von Informationen über Fernmeldeanschlüsse (Adressierungselemente usw.) über den Dienst ÜPF. Es handelt sich dabei um Auskünfte zu Informationen, die nicht dem Fernmeldegeheimnis unterstehen.

2.2.2 Genehmigungspflichtige Überwachung nach Artikel 25 Absatz 1 Buchstabe a E-NDG

Das NDG regelt die Tätigkeit des Nachrichtendienstes im sicherheitspolitischen Bereich und zur Wahrung weiterer wesentlicher Landesinteressen. Artikel 3 E-NDG soll es dem Bundesrat ermöglichen, den NDB unter besonderen Voraussetzungen mit der Informationsbeschaffung und -auswertung sowie gegebenenfalls mit operativen Tätigkeiten zu beauftragen, die über den ordentlichen gesetzlichen Auftrag des NDB hinausgehen. Hierzu ist ein Beschluss des Bundesrates nach Artikel 70 E-NDG notwendig. Der Grundauftrag des Bundesrates (Art. 69 Abs. 1 Bst. a E-NDG) oder die von ihm erlassene Beobachtungsliste (Art. 71 E-NDG) genügen nicht. Der NDB darf also nicht von sich aus oder aufgrund der ordentlichen Führungsinstrumente Grundauftrag und Beobachtungsliste zur Wahrung weiterer wesentlicher Landesinteressen nach Artikel 3 E-NDG tätig werden. Mit dem Beschluss des Bundesrates stehen dem NDB keine besonderen Kompetenzen zu, die über das NDG hinausgehen. Für die Beschaffungstätigkeiten gelten somit die gesetzlichen Regeln, insbesondere für die Anwendung genehmigungspflichtiger Massnahmen (Art. 25 ff. E-NDG), die nach dem normalen Verfahren zu beantragen und zu begründen sind. Daraus ergibt sich, dass im Rahmen eines bundesrätlichen Beschlusses nach Artikel 3 E-NDG keine über die gesetzlich geregelten Überwachungsmöglichkeiten hinausgehenden Beschaffungsmassnahmen angeordnet werden können. Insbesondere die Überwachung des Fernmeldeverkehrs richtet sich auch in diesem Fall nach Massgabe des BÜPF (siehe nachfolgende Ausführungen zu Art. 25 Abs. 1 Buchstabe a E-NDG). Der Bundesrat kann aber Einschränkungen beschliessen und z.B. bestimmte Beschaffungsmassnahmen zur Wahrung weiterer wesentlicher Landesinteressen ausschliessen.

Artikel 25 Absatz 1 Buchstabe a E-NDG ermöglicht es dem NDB, die Überwachung des Post- und Fernmeldeverkehrs gemäss den Bestimmungen des BÜPF anzuordnen. Im Gegensatz zu den Strafverfolgungsbehörden, die solche Überwachungen im Rahmen eines Strafverfahrens zur Überführung eines Täters einsetzen (repressive Zielsetzung), wird der NDB die Post- und Fernmeldeüberwachung ausschliesslich zu präventiven Zwecken anordnen. Ziel ist das frühzeitige Erkennen von Bedrohungen der inneren oder äusseren Sicherheit der Schweiz. Wenn der NDB im Rahmen seiner Abklärungen den Verdacht hat,

dass Officialdelikte vorliegen, ist er verpflichtet, die Strafverfolgungsbehörden zu informieren.

Der Gesetzestext gemäss Botschaft verweist auf die Überwachungsarten nach dem BÜPF. Damit wird die Koordination mit dem sich in Totalrevision befindlichen BÜPF und allfälligen Weiterentwicklungen desselben erleichtert. Die Abwicklung der Überwachungen erfolgt wie bei der Strafverfolgung über den Dienst ÜPF. Der Umfang der rechtlichen Verpflichtungen der Anbieterinnen, bestimmte Massnahmen durchzuführen, insbesondere die hier diskutierte Offenlegung von IP-Adressen im Zusammenhang mit der Kommunikation über soziale Medien, richtet sich nach dem Ergebnis der Totalrevision des BÜPF.

Die Voraussetzungen für die Anordnung von genehmigungspflichtigen Beschaffungsmassnahmen richten sich nach Artikel 26 E-NDG. Im vorliegenden Zusammenhang ist dabei von Bedeutung, dass solche Massnahmen nur zulässig sind, wenn kumulativ eine konkrete Bedrohung entweder durch Terrorismus, Spionage, Proliferation von Massenvernichtungswaffen, illegalen Handel mit radioaktiven Substanzen, Kriegsmaterial und anderen Rüstungsgütern oder Angriffe auf kritische Infrastrukturen vorliegt oder ein Auftrag zur Wahrung weiterer wesentlicher Landesinteressen erteilt wurde sowie die Schwere der Bedrohung die Massnahme rechtfertigt und die nachrichtendienstlichen Abklärungen bisher erfolglos waren, sonst aussichtslos wären oder unverhältnismässig erschwert würden. Zur blossen Verhinderung oder Aufklärung von Störungen der öffentlichen Ordnung und Sicherheit bietet das NDG keine Grundlage.

Zusammenfassend ist festzuhalten, dass sich die im NDG vorgesehenen Überwachungs- bzw. Auskunftsöglichkeiten im Bereich des Fernmeldewesen nach dem BÜPF richten werden, ungeachtet des Umstands, ob die Totalrevision dereinst in Kraft treten wird. Entweder sind Anpassungen des bestehenden BÜPF oder Anpassungen des nach dem allfälligen Inkrafttreten geltenden BÜPF erforderlich (vgl. Botschaft zum NDG, Ausführungen zu Änderungen anderer Erlasse, S. 2221 bis 2223), um die nach dem NDG erweiterten Befugnisse umzusetzen. Da sich auch die erweiterten Fernmeldeüberwachungsmöglichkeiten des NDB nach Massgabe des BÜPF richten, ist unter geltendem BÜPF ein Zugriff des NDB auf IP-Adressen nicht möglich. Im Fall des Inkrafttretens des totalrevidierten BÜPF gemäss aktueller Fassung werden auch sogenannte „Anbieterinnen abgeleiteter Kommunikationsdienste“ von der Überwachungsmöglichkeit erfasst, was einen Zugriff auf IP-Adressen auch für den NDB ermöglichen würde, allerdings ebenfalls mit den in der Botschaft zum BÜPF, S. 2707 erläuterten Erschwerungen bei der praktischen Umsetzung (Sitz der entsprechenden Unternehmen im Ausland, etc.).

3. Verfassungsmässige Zuständigkeiten in Bezug auf die Bekanngabe von Internetadressen ausserhalb eines Strafverfahrens

3.1 Ausgangslage

Nach Artikel 57 Absatz 1 BV sorgen der Bund und die Kantone im Rahmen ihrer Zuständigkeit für die Sicherheit des Landes und den Schutz der Bevölkerung. Die Verfassungsnorm bestimmt, dass beide Staatsebenen gewisse Aufgaben im Bereich der Sicherheit des Landes und des Bevölkerungsschutzes zu erfüllen haben. Welcher Art diese Aufgaben sind und welche staatliche Ebene

für welchen Teilbereich zuständig ist, besagt Artikel 57 Absatz 1 BV hingegen nicht. Dies bedeutet, dass eine andere explizite oder implizite Verfassungsbestimmung die Befugnisse des Bundes im Bereich der Sicherheit umschreiben muss, damit der Bund auf diesem Gebiet tätig werden kann. Wo die BV keine Kompetenzzuweisung an den Bund vornimmt, kommen primär die Kantone zum Zug.

Die BV enthält diverse Bestimmungen, die dem Bund ausdrücklich gewisse Gesetzgebungskompetenzen zuweisen, die für einzelne Teilbereiche oder Aspekte der inneren Sicherheit relevant sind.¹⁹ Auch gilt als anerkannt, dass der Bund gestützt auf implizite Verfassungsgrundlagen (sogenannte inhärente Kompetenzen) befugt ist, die notwendigen Massnahmen zum Schutz seiner Organe und Institutionen zu treffen, soweit es darum geht, Gefahren abzuwehren, die für den Staat existentiellen Charakter haben. Dazu kommen weitere Verfassungsbestimmungen, die dem Bund auf einem Gebiet umfassende Gesetzgebungskompetenzen einräumen und ihn damit auch ermächtigen, in solchen sektoriellen Gesetzgebungen Belange der inneren Sicherheit zu regeln.²⁰

Gemäss Artikel 57 Absatz 2 BV müssen der Bund und die Kantone ihre Anstrengungen im Bereich der inneren Sicherheit koordinieren. Sinn und Tragweite dieser Norm sind bislang nicht abschliessend geklärt worden. Dem Wortlaut nach enthält Artikel 57 Absatz 2 BV keine explizite Kompetenzzuweisung an den Bund. Nach konstanter Praxis des Bundesrates begründet diese Verfassungsbestimmung indessen nicht bloss eine Koordinationspflicht; die Verfassungsnorm hat nach Auffassung des Bundesrates zudem – wenn auch in einem eng begrenzten Sinn – kompetenzbegründenden Charakter. Eine Gesetzgebungszuständigkeit des Bundes in Zusammenhang mit der in Artikel 57 Absatz 2 BV statuierten Koordinationspflicht ist jedoch nur dann gegeben, wenn es sich um Sicherheitsbelange handelt, die mindestens teilweise in die Zuständigkeit des Bundes fallen und die aus dessen Sicht eine Koordination unter Einbezug des Bundes erfordern. Die Zuständigkeit des Bundes darf dabei nicht bloss marginale Bedeutung haben. Wenn diese Voraussetzungen gegeben sind, kann der Bund in Ausübung der auf Artikel 57 Absatz 2 BV abgestützten Gesetzgebungskompetenz auch Belange regeln, die an sich in den Zuständigkeitsbereich der Kantone fallen.

3.2 Verfassungsrechtliche Zuständigkeiten auf dem Gebiet der Polizei

Das Polizeirecht im engeren Sinn gehört zu den Kernkompetenzen der Kantone (originäre kantonale Polizeihohheit²¹): Die Kantone verfügen im Bereich der Sicherheits- und Kriminalpolizei innerhalb ihrer Territorien über eine umfassende Zuständigkeit. Soweit es demnach um die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung sowie die Beseitigung von Störungen geht,

¹⁹ Vgl. z.B. Art. 58 Abs. 2 und 3, Art. 61, Art. 123, Art. 173 Abs. 1 Bst. b und c und Art. 185 Abs. 3 BV.

²⁰ So z.B. Art. 87 BV (Eisenbahnen und weitere Verkehrsträger), der als Verfassungsgrundlage für die bundesrechtlich geregelte Bahnpolizei gilt.

²¹ Botschaft des Bundesrates über eine neue Bundesverfassung, BBl 1997 I 237.

sind grundsätzlich die Kantone zuständig.²² Zu den Aufgaben der polizeilichen Gefahrenabwehr zählt nach neuem Verständnis auch die Gefahrenvorsorge, die darauf ausgerichtet ist, künftige Gefährdungslagen und Bedrohungen durch vorausschauendes Handeln abzuwehren oder zu verhindern. Ebenfalls Kantonssache sind Polizeiaufgaben, die der Erkennung und Aufklärung begangener Straftaten dienen, soweit sich diese Tätigkeit im Bereich der Vorermittlungen bewegt. Erst wenn ein hinreichender Tatverdacht besteht, der die Eröffnung eines Strafverfahrens erlaubt, erwachsen der Polizei gerichtspolizeiliche Funktionen, die sie nach bundesrechtlichen Regeln - denjenigen der Schweizerischen Strafprozessordnung - ausüben haben.

Die vorliegende Standesinitiative verlangt, dass präventiv Internetadressen von Organisatoren bekannt gegeben werden dürfen, die zu gefahrenträchtigen Demonstrationen und Grossanlässen aufrufen. Die Preisgabe der Identität der Organisatoren soll somit im Vorfeld eines solchen Anlasses erfolgen, auch wenn der Aufruf der Organisatoren keine Aufforderung zu Gewalttaten enthalten hat (vgl. Art. 259 StGB) und zu diesem Zeitpunkt noch gar keine StGB-Straftat begangen worden ist. Erklärtes Ziel der ins Auge gefassten Regelung ist die Schaffung von Kontaktmöglichkeiten zu den anonymen Organisatoren, um verbindliche Abmachungen hinsichtlich des Ablaufs der angekündigten Anlässe zu treffen und allfällige Haftungsfragen vorgängig zu klären. Damit soll ein reibungsloser Ablauf und eine Minimierung der Gefahren anlässlich von Demonstrationen und anderen Manifestationen gewährleistet werden. Die zur Diskussion stehende Massnahme ist somit als Instrument der präventiven Gefahrenabwehr zum Schutz von klassischen Polizeigütern zu verstehen; eine entsprechende Regelung wäre dem materiellen Polizeirecht zuzuordnen.

3.3 Kompetenzaufteilung zwischen Bund und Kantonen bei der Bekanntgabe von Internetadressen ausserhalb eines Strafverfahrens

Nach dem Gesagten liegt die Befugnis zum Erlass von polizeirechtlichen Regelungen primär bei den Kantonen. Auf den ersten Blick scheint daher auch im vorliegenden Fall eine bundesrechtliche Regelung ausgeschlossen. Die postulierte präventivpolizeiliche Massnahme beschlägt indessen angesichts ihres technischen Charakters auch eine wichtige Bundeskompetenz: Die Identität der Organisatoren von Demonstrationen und anderen öffentlichen Anlässen lässt sich nur über die Aufhebung des Fernmeldegeheimnisses feststellen. Das Post- und Fernmeldewesen ist gemäss Artikel 92 Abs. 1 BV Sache des Bundes; es gilt als anerkannt, dass diese Verfassungsbestimmung auch die fernmeldetechnischen Aspekte der Internetkommunikation erfasst.²³ Nach herrschender Lehre handelt es sich bei Artikel 92 BV um eine umfassende, ausschliessliche Kompetenz des Bundes.²⁴

²² Vgl. auch Bericht des Bundesrates vom 2. März 2012 in Erfüllung des Postulats Malama 10.3045 (BBl 2012 4459 ff.).

²³ Hettich/Steiner, St. Galler Kommentar, 3. Aufl., Zürich/St. Gallen 2014, Art. 92 BV, Rz. 5.

²⁴ Hettich/Steiner, St. Galler Kommentar, a.a.O., Art. 92, Rz. 4; Tschannen, Staatsrecht der Schweizerischen Eidgenossenschaft, 3. Aufl., Bern 2011, § 20, Rz. 32; Auer/Malinverni/Hottelier, Droit constitutionnel suisse Vol. I, 3. Aufl., Berne 2013, Rz. 1052.

Bei vorliegender Konstellation kommen somit umfassende Kompetenzen beider Staatsebenen zum Tragen, die unangefochtene Polizeihochheit der Kantone einerseits und die Kompetenz des Bundes im Bereich des Fernmeldewesens andererseits. Soweit es um die eigentliche polizeiliche Tätigkeit geht, ist die Zuständigkeit der Kantone gegeben; wo die technische Umsetzung der Teilnehmeridentifikation Platz greift, kann Artikel 92 Absatz 1 BV – in Verbindung mit Artikel 57 Absatz 2 BV – herangezogen werden. Eine Abstützung auf Artikel 123 Absatz 1 BV erscheint demgegenüber nicht angezeigt: Zum Zeitpunkt, in dem die besagte präventivpolizeiliche Massnahme ergriffen werden soll, ist in aller Regel noch keine Straftat nach dem Strafgesetzbuch begangen worden – ein inhaltlicher Bezug zum Strafrecht fehlt somit. Ebenso wenig kann der Bund gestützt auf Art. 123 Absatz 1 BV legiferieren, indem er den Aufruf zu nicht bewilligten Kundgebungen unter Strafe stellt und den Straftatbestand in den Katalog von Artikel 273 StPO aufnimmt. Die zu schaffende Strafnorm wäre dem Verwaltungsstrafrecht zuzuordnen, zumal das tatbestandsmässige Handeln nicht an sich strafwürdig ist, sondern nur in Zusammenhang mit einem Verstoss gegen bestimmte Gebots- oder Verbotsnormen des Verwaltungsrechts; im vorliegenden Zusammenhang gegen Normen des kantonalen oder kommunalen Polizeirechts. Die Zuständigkeit für die Sanktionierung solcher Widerhandlungen stützt sich auf die jeweilige Sachkompetenz. In einem Sachgebiet wie dem Polizeirecht, wo der Bund nur über spezifische Rechtsetzungsbefugnis verfügt, verfügt er auch nicht über die generelle Kompetenz, Strafnormen als Mittel zur Durchsetzung des Verwaltungsrechts zu erlassen. Deshalb finden sich die (Übertretungs-) Straftatbestände des Versammlungsrechts denn auch auf den kommunalen und kantonalen Ebenen des föderalen Staates.

Aus kompetenzrechtlicher Sicht ist demnach der Bund befugt, zum Zweck der Erfüllung der genannten polizeilichen Aufgabe ein Fernmeldeüberwachungssystem zu betreiben. Die Statuierung der Bedingungen für die Nutzung des Instruments obliegt hingegen grundsätzlich den Kantonen. Diese müssen in ihren Polizeierlassen namentlich regeln, in welchen Fällen, unter welchen Voraussetzungen und in welchem Verfahren die Identifikation der Organisatoren von Demonstrationen durch die zuständige kantonale Behörde angeordnet werden kann. Angesichts der grundrechtlichen Tragweite dieser Massnahme erscheint eine Regelung auf formellgesetzlicher (kantonal) Ebene unerlässlich. Das skizzierte Vorgehen drängt sich nicht zuletzt auch aufgrund der Artikel 5a und 43a Absatz 1 BV auf: Die Ausübung von Bundeskompetenzen muss unter Beachtung des Subsidiaritätsprinzips erfolgen; nach diesem Grundsatz soll der Bund nur diejenigen Aufgaben übernehmen, welche die Möglichkeiten der Kantone übersteigen oder die einer einheitlichen, gesamtschweizerischen Lösung bedürfen. Demgegenüber können Aufgaben aus dem originären Wirkungsbereich der Kantone mittels interkantonaler Vereinbarungen (Art. 48 BV) geregelt werden, sofern das Bedürfnis nach einer gewissen Rechtsvereinheitlichung besteht. Ein solcher Lösungsansatz wäre auch im vorliegenden Fall angezeigt.

4. Regelung zur Aufhebung der Anonymität von aufrufenden Personen

4.1 Ausgangslage

Nach den Ausführungen in Ziffer 3 liegt die Befugnis zum Erlass von polizeirechtlichen Regelungen primär bei den Kantonen. Im vorliegenden Zusammenhang bedeutet dies, dass die Zuständigkeit der Kantone dort gegeben ist, wo es um die eigentliche polizeiliche Tätigkeit geht. Wo die technische Umsetzung der Teilnehmeridentifikation Platz greift, könnte Artikel 92 Absatz 1 BV – in Verbindung mit Art. 57 Absatz 2 BV – herangezogen und dem Bund qua Gesetz die Aufgabe zugewiesen werden, ein diesem Zweck dienendes Fernmeldeüberwachungssystem zu betreiben. Der Normierungsbedarf des Bundes hätte sich dabei im Wesentlichen auf die zum Betrieb des Systems sowie zu dessen Finanzierung notwendigen Regeln sowie auf die Definierung der Zugriffsmodalitäten zu beschränken. Demgegenüber wären alle weiteren Regelungsinhalte kantonsseitig und vorzugsweise auf Konkordatsstufe zu schaffen. Das Aufzeigen der gesetzgeberischen Massnahmen, die von Bund und Kantonen im Einzelnen getroffen werden müssten, würde den Rahmen des vorliegenden Berichts sprengen. Aus den nachfolgend dargelegten Gründen hegt der Bundesrat Zweifel an der Rechtmässigkeit eines solchen Vorhabens.

4.2 Grundrechtsrelevanz der Massnahme (insbes. der Bekanntgabe von Internetadressen)

Wird die Anonymität der Organisatoren von Kundgebungen aufgehoben, ist dies in verschiedener Hinsicht grundrechtsrelevant. Berührt ist zunächst das Recht auf Privatsphäre (Art. 13 BV), insbesondere das Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV). IP-Adressen sind aber auch Adressierungselemente im Sinne der Fernmeldegesetzgebung (BGE 136 II 508 E. 3.1). Dynamische IP-Adressen fallen unter das Fernmeldegeheimnis, denn dies sind Verbindungsdaten.²⁵

Betroffen ist auch die *Versammlungsfreiheit* (Art. 22 BV). Diese verbietet staatliche Massnahmen gegen die Teilnahme bzw. Nichtteilnahme an einer Versammlung sowie gegen die Einberufung, Organisation, Durchführung oder Gestaltung einer Versammlung.²⁶ Geschützt sind damit auch vorbereitende Handlungen wie z.B. das Versenden von Einladungen,²⁷ auch wenn dies über das Internet erfolgt.²⁸ Nicht durch Artikel 22 BV geschützt sind hingegen unfriedliche Versammlungen,²⁹ sofern der unfriedliche Verlauf zum Vornherein feststeht.³⁰ Eine Versammlung kann nicht schon deshalb als unfriedlich gelten, wenn es zu rechtswidrigen Handlungen oder zu einem unfriedlichen Verlauf

²⁵ Hansjakob, Kommentar BÜPF, Art. 14 BÜPF N 26 und Entscheid des BGER 1B_344/2014 vom 14. Januar 2015 (zur Publikation vorgesehen), E. 5.1.

²⁶ BGE 137 I 31 E. 6.1 S. 44.

²⁷ Christoph Errass, in: St. Galler Kommentar, 3. Aufl., Zürich/St. Gallen 2014, Art. 22, Rz. 25.

²⁸ Errass, in: St. Galler Kommentar, a.a.O., Art. 22, Rz. 17

²⁹ BGE 111 Ia 322 E. 6a) S. 322.

³⁰ Errass, in: St. Galler Kommentar, a.a.O., Art. 22, Rz. 22 und 62.

kommen *könnte*.³¹ Eine öffentliche Kundgebung darf insbesondere auch provozieren.³²

Bewilligungs- und Meldepflichten greifen in die Versammlungsfreiheit ein.³³ Entsprechendes muss für die zwangsweise Identifizierung der Organisatoren von Kundgebungen gelten. Die Versammlungsfreiheit kann zudem auch mittelbar beeinträchtigt werden. Dies ist der Fall, wenn von staatlichen Massnahmen Abschreckungswirkungen bzw. Einschüchterungseffekte ausgehen, welche die Grundrechtsträger von der Ausübung der Versammlungsfreiheit abhalten.³⁴ Es ist nicht ausgeschlossen, dass die Möglichkeit der zwangsweisen Identifizierung die Grundrechtsträger davon abhält, Veranstaltungen über das Internet zu organisieren, entsprechende Aufrufe mittels Social Media weiterzuverbreiten oder auf Social Media-Plattformen die Teilnahme an der Veranstaltung zu erklären.

Veranstaltungen mit Appellwirkung an die Öffentlichkeit stehen zudem unter dem Schutz der *Meinungsfreiheit* (Art. 16 BV).³⁵ Auch die Meinungsfreiheit kann durch Abschreckungswirkungen oder Einschüchterungseffekte mittelbar beeinträchtigt werden,³⁶ wie sie von einer zwangsweisen Identifizierung grundsätzlich ausgehen können. Je nach Art der Kundgebung können zudem spezielle Grundrechte tangiert sein, etwa die *Glaubens- und Gewissensfreiheit* (Art. 15 BV) sofern z.B. die Religionsausübung im öffentlichen Raum betroffen ist. Zu prüfen wäre ferner, inwiefern Grundrechte der zur Herausgabe von Personendaten verpflichteten Unternehmen betroffen sind. Ein Eingriff in die *Wirtschaftsfreiheit* (Art. 27 BV) kann nicht ausgeschlossen werden.³⁷

4.3 Öffentliches Interesse

Die Verhinderung von gewaltsamen Ausschreitungen und Straftaten im Rahmen von Kundgebungen liegt im öffentlichen Interesse.³⁸ Mit Blick auf die durch die Polizei zu treffenden Sicherheitsmassnahmen besteht auch ein Interesse daran, über die Durchführung von Kundgebungen sowie deren Art und Ablauf informiert zu werden.³⁹ Erfolgt die Aufhebung der Anonymität der Organisatoren von Kundgebungen mit dem Zweck, gewalttätige Ausschreitun-

³¹ BGE 111 Ia 322 E. 6a) S. 323; Biaggini, Giovanni (2007): BV Kommentar. Zürich: Orell Füssli, Art. 22 BV, Rz. 10.

³² Urteil des EGMR Nr. 29221/95 und 29225/95 i.S. Stankov et Organisation macédonienne unie Ilinden c. Bulgarien vom 2. Oktober 2001., § 86.

³³ Errass, in: St. Galler Kommentar, a.a.O., Art. 22, Rz. 53 und 62; Urteil des Bundesgerichts 1C_140/2008 vom 17. März 2009 E. 8.

³⁴ Errass, in: St. Galler Kommentar, a.a.O., Art. 22, Rz. 54.

³⁵ BGE 127 I 164 E. 3a S. 167.

³⁶ Urteil des Bundesgerichts 5A_888/2011 vom 20. Juni 2012 E. 5.3.

³⁷ Vgl. bezogen auf eine gesetzliche Auskunftspflicht gewerbmässiger Transporteure Biaggini, Giovanni (2009): Verfassungsrechtliche Abklärung betreffend die Teilrevision des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (Vorlage «BWIS»), Gutachten vom Juni 2009. In: VPB 4/2009 vom 2. Dezember 2009, S. 238 ff., Ziff. 3: „Das Erbringen von Transportdienstleistungen durch private Unternehmen ist durch die Wirtschaftsfreiheit (Art. 27 BV) geschützt. Die Auskunftspflicht gewerblicher Transporteure (Art. 13c E-BWIS) tangiert die freie Ausübung einer privatwirtschaftlichen Erwerbstätigkeit.“

³⁸ BGE 132 I 256, E. 3 und 4, S. 259 ff.; s.a. BGE 130 I 368 E. 7.4 S. 383 f.

³⁹ Urteil des Bundesgerichts 1C_140/2008 vom 17. März 2009 E. 8.2

gen zu verhindern und die notwendigen Sicherheitsvorkehrungen zu ergreifen, ist dies ebenfalls durch ein öffentliches Interesse gedeckt.

4.4 Verhältnismässigkeit

Die Verhältnismässigkeit eines Grundrechtseingriffs beurteilt sich nach deren Geeignetheit, Erforderlichkeit und Zumutbarkeit für die Betroffenen.⁴⁰ Im Polizeirecht kommt dem Verhältnismässigkeitsgrundsatz ein hoher Stellenwert zu.⁴¹ Die Interessenabwägung hat auch dem ideellen Gehalt der Versammlungs- und Meinungsfreiheit angemessen Rechnung zu tragen.⁴²

Eine Identifikation der Organisatoren von Kundgebungen ermöglicht den Behörden, mit ihnen in Kontakt zu treten und Absprachen über den Ablauf zu treffen. Allerdings dürfte sich das *Hauptproblem* der spontanen Gewaltexzesse gerade nicht verhindern lassen, sind doch die Einflussmöglichkeiten der Organisatoren auf (gewaltbereite) Teilnehmer regelmässig beschränkt oder es gehen die Gewalttätigkeiten von Dritten aus, welche der ursprünglichen Versammlung nicht zugerechnet werden können. Fraglich ist zudem, ob die Aufhebung der Anonymität auch dazu geeignet ist, *Haftungsfragen* vorgängig zu diskutieren. Die zivilrechtliche Haftung für Schäden trifft nicht den Organisator einer Demonstration als solchen. Es wäre unvereinbar mit der Meinungs- und Versammlungsfreiheit, dem Organisator einer Kundgebung eine Haftung ohne eigenes Verschulden für alle Schäden, die im Zusammenhang oder im Nachgang zur vorgesehenen Demonstration als Folgen von Ausschreitungen eintreten, zu überbürden.⁴³ Eine Haftung des Organisators kommt nur dann in Frage, wenn er selber zu Gewalt aufruft, dazu anstiftet und u.U. wenn er spezifische Mitwirkungspflichten missachtet.⁴⁴ Mit Blick auf die Geeignetheit bleibt ferner zu bedenken, dass wie in Ziffer 2.1.3 erwähnt, viele bedeutende Anbieterinnen abgeleiteter Kommunikationsdienste nicht (bzw. nur mittels Rechtshilfe) ins Schweizerische Recht gefasst werden können, da sie ihren Sitz und ihre Infrastruktur im Ausland haben.

Die Aufhebung der Anonymität könnte häufig gar nicht innert nützlicher Frist umgesetzt werden, um im Vorfeld sicherheitspolizeiliche Massnahmen zu veranlassen. Allerdings lässt die letztgenannte Problematik die Aufhebung der Anonymität für sich genommen nicht als geradezu untaugliches Mittel erscheinen.

Mit Bezug auf die *Erforderlichkeit* stellt sich die Frage nach *milderen* Mitteln. Nicht ausgeschlossen ist eine *Bestrafung* der Organisatoren wegen eines Verstosses gegen gesetzliche Bewilligungs- und Meldepflichten.⁴⁵ Der Grundsatz der Erforderlichkeit verlangt aber, dass sich eine polizeiliche Massnahme gegen diejenigen Personen richtet, welche den polizeiwidrigen Zustand unmit-

⁴⁰ BGE 136 I 17, E. 4.4 S. 26; BGE 140 I 2 E. 9.2.2 S. 24.

⁴¹ BGE 140 I 2, E. 9.2.2 S. 24.

⁴² BGE 138 I 274 E. 2.2.2 S. 283.

⁴³ Stellungnahme des Bundesrates vom 18.05.2005 auf die Motion 05.3043 Jasmin Hutter-Hutter.

⁴⁴ Gander, Christine (2008): Sicherheit und Demonstrationen – Grenzen eines Grundrechts. In: Sicherheit & Recht 2/2008, S. 67 ff., 75; Stellungnahme des Bundesrates vom 18.05.2005 auf die Motion 05.3043 Jasmin Hutter-Hutter.

⁴⁵ Urteil des Bundesgerichts 1C_225/2012 vom 10. Juli 2013, E. 5; Errass, in: St. Galler Kommentar, a.a.O., Art. 22 BV, Rz. 69; Gander, a.a.O., 75.

telbar zu verantworten haben (*Störerprinzip*),⁴⁶ was auch bezogen auf Versammlungen gilt.⁴⁷ Ausschreitungen durch Dritte sind dem Organisator jedoch nicht zuzurechnen, sofern er sich nicht selber an den Gewalttätigkeiten beteiligt oder dazu aufgerufen bzw. angestiftet hat. Eine polizeirechtliche Qualifikation als Störer scheint allerdings dann nicht ausgeschlossen, wenn die Organisatoren die Störung der öffentlichen Sicherheit *bewusst in Kauf nehmen* (sog. „Zweckveranlasser“).⁴⁸ Damit führen jedoch auch sehr weit entfernte Folgen zu einer polizeirechtlichen Zurechnung,⁴⁹ wofür es – auch angesichts der Bedeutung der Versammlungs- und Meinungsfreiheit im demokratischen Gemeinwesen – jedenfalls *konkreter* Anhaltspunkte bedürfte. Eine mangelnde Kooperation kann zwar den Schluss zulassen, dass auf die Mitwirkung der Organisatoren zwecks Aufrechterhaltung der öffentlichen Sicherheit nicht gezählt werden kann,⁵⁰ reicht aber für sich genommen nicht aus, dem Organisator ein *bewusstes* Inkaufnehmen von Gewalttätigen zu unterstellen.

Bezogen auf die *Zumutbarkeit* ist zu bedenken, dass den Organisator einer Versammlung im Rahmen seiner Möglichkeiten eine gewisse Verantwortung trifft, gewalttätige Ausschreitungen und Missbräuche zu verhindern.⁵¹ Auch bestehen Mitwirkungspflichten, etwa die Pflicht zur frühzeitigen Information der Behörden oder eine Pflicht zur Teilnahme an Besprechungen, um Sicherheitsfragen oder Fragen betreffend die Routenwahl klären zu können.⁵² Eine zwangsweise Identifizierung der Organisatoren bewirkt jedoch einen erheblichen Eingriff in die Persönlichkeitssphäre und die informationelle Selbstbestimmung (Art. 13 Abs. 2 BV). Gleichzeitig stellt das blosses Aufrufen zu einer Versammlung oder einer Kundgebung weder eine Straftat noch eine unmittelbare Gefahr für die öffentliche Sicherheit dar. Beschränkungen der Versammlungsfreiheit erscheinen nur zulässig, wenn solche Gefährdungen tatsächlich zu befürchten sind, wofür alleine der Umstand eines anonymen Aufrufs nicht ausreichen dürfte. Sodann spielt auch im Rahmen der *Zumutbarkeit* das Störerprinzip eine Rolle.⁵³ Derjenige der zu einer Kundgebung anonym aufruft, dürfte – wie gezeigt – nur ausnahmsweise als Störer im polizeirechtlichen Sinne in Frage kommen.

Es bestehen somit Zweifel, dass die Aufhebung der Anonymität ein verhältnismässiges Mittel darstellt, um Gewalttätigkeiten anlässlich von Kundgebungen präventiv zu verhindern oder Fragen der Haftung klären zu können. Die

⁴⁶ Tschannen, Pierre/Zimmerli Ulrich/Müller Markus (2014): Allgemeines Verwaltungsrecht, 4. Aufl., Bern: Stämpfli, § 56, Rz. 28 f.

⁴⁷ Rhinow, René/Schefer, Markus (2009): Schweizerisches Verfassungsrecht, 2., erweiterte Aufl. Basel: Helbing Lichtenhahn, Rz. 1701; Errass, in: St. Galler Kommentar, a.a.O., Art. 22 BV, Rz. 64.

⁴⁸ Tschannen/Zimmerli/Müller, a.a.O., § 56, Rz. 33.

⁴⁹ Mohler, Markus H.F. (2012): Grundzüge des Polizeirechts in der Schweiz. Basel: Helbing und Lichtenhahn, Rz. 713, Rz. 719.

⁵⁰ BGE 132 I 256 E. 4.4.3 S. 266.

⁵¹ Urteil des Bundesgerichts 1C_225/2012 vom 10. Juli 2013 E. 3.5; Errass, in: St. Galler Kommentar, a.a.O., Art. 22 BV, Rz. 39.

⁵² Vgl. zu den Mitwirkungspflichten Errass, in: St. Galler Kommentar, Art. 22, Rz. 39; Gander, a.a.O., 72:“; s.a. Wyss, Martin Philipp (2002): Appell und Abschreckung. Verfassungsrechtliche Beobachtungen zur Versammlungsfreiheit. In: ZBl 103/2002, 393 ff., 397; Urteil des Bundesgerichts 1P.53/2001 vom 20. September 2001, E. 2d/aa; Urteil des Bundesgerichts 1C_225/2012 vom 10. Juli 2013, E. 3.5; BGE 132 I 256, E. 3 S. 260 und 4.4.3 S. 265 f.

⁵³ Vgl. Mohler, a.a.O., Rz. 713.

zwangsweise Aufhebung der Anonymität setzt jedenfalls voraus, dass Gewalttätigkeiten und Ausschreitungen konkret und ernsthaft zu befürchten sind, der Organisator aufgrund konkreter Anhaltspunkte als Störer in Frage kommt und eine Kontaktaufnahme mit dem Organisator tatsächlich dazu beitragen kann, Gefährdungen für die öffentliche Sicherheit zu beugen. Zudem muss sicher gestellt sein, dass lediglich der Organisator bzw. der Initiator einer Versammlung identifiziert wird und nicht auch potentielle Veranstaltungsteilnehmer oder Personen, welche einen Aufruf bloss weiterleiten. Mit anderen Worten kann eine Identifizierung nur gegenüber solchen Personen in Frage kommen, welche am Ursprung des Aufrufs zu einer Versammlung stehen. Andere Personen können nicht als Störer gelten und auch mit Blick auf potentielle Einschüchterungseffekte hat ihnen gegenüber eine Identifizierung im Gefahrenvorfeld zu unterbleiben.⁵⁴ Schliesslich bedarf es konkreter Anhaltspunkte, dass der Organisator seine Mitwirkungspflichten, insbesondere seine gesetzlichen Informationspflichten nicht wahrnehmen wird.

5. Schlussfolgerungen

Aus diesen Erkenntnissen und aus den vorangehenden Erwägungen und Analysen zur Bekanntgabe von Internetadressen ausserhalb eines Strafverfahrens leiten sich folgende Schlussfolgerungen ab: Es kommen vorliegend sowohl umfassende Kompetenzen der Kantone als auch des Bundes zum Tragen, nämlich die Polizeihochheit der Kantone einerseits und die Kompetenz des Bundes im Bereich des Fernmeldewesens andererseits. Soweit es um die eigentliche polizeiliche Tätigkeit geht, ist die Zuständigkeit der Kantone gegeben; wo die technische Umsetzung der Teilnehmeridentifikation Platz greift, kann Artikel 92 Absatz 1 BV – in Verbindung mit Artikel 57 Absatz 2 BV – herangezogen werden. Die Statuierung der Bedingungen für die Nutzung des Instruments obliegt hingegen grundsätzlich den Kantonen. Diese müssen in ihren Polizeierlassen namentlich regeln, in welchen Fällen, unter welchen Voraussetzungen und in welchem Verfahren die Identifikation der Organisatoren von Demonstrationen durch die zuständige kantonale Behörde angeordnet werden kann. Angesichts der grundrechtlichen Tragweite dieser Massnahme erscheint eine Regelung auf formell gesetzlicher (kantonal) Ebene unerlässlich. Der Grundsatz der Verhältnismässigkeit verlangt, dass die Einschränkung von Grundrechten nicht über das hinausgeht, was erforderlich ist, um den angestrebten Zweck zu erfüllen; die Eingriffe müssen unter möglicher Schonung der grundrechtlich garantierten Positionen der Betroffenen vorgenommen werden und in einem vernünftigen Verhältnis zu den eingesetzten Mitteln stehen. Aus Sicht des Bundesrates bestehen jedoch erhebliche Zweifel an der Verhältnismässigkeit und damit an der Rechtmässigkeit eines solchen Vorhabens.

Die Ausübung von Bundeskompetenzen muss unter Beachtung des Subsidiaritätsprinzips erfolgen; nach diesem Grundsatz soll der Bund nur diejenigen Aufgaben übernehmen, welche die Möglichkeiten der Kantone übersteigen oder die einer einheitlichen, gesamtschweizerischen Lösung bedürfen. Demgegenüber können Aufgaben aus dem originären Wirkungsbereich der Kantone mittels interkantonalen Vereinbarungen (Art. 48 BV) geregelt werden, sofern das Bedürfnis nach einer gewissen Rechtsvereinheitlichung besteht. Nach

⁵⁴ Vgl. Errass, in: St. Galler Kommentar, Rz. 68 und 54.

Meinung des Bundesrates wäre ein solcher Lösungsansatz auch im vorliegenden Fall angezeigt.

Der Bund kann zwar im Rahmen seiner Fernmeldekompetenz organisatorische und administrative Fragen zum Verfahren der Datenerhebung auf Bundesebene regeln. Wie oben dargelegt, obliegt es jedoch in erster Linie den Kantonen, gesetzliche Regelungen zu schaffen, welche dem Verhältnismässigkeitsprinzip angemessen Rechnung tragen.