Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement
Bundesamt für Justiz

Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens

über den Bericht und den Vorentwurf

zur Änderung des Bundesgesetzes vom 6. Oktober 2000

betreffend

die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Bern, Mai 2011

Inhaltsverzeichnis

I. Einleitung 10
II. Übersicht der Ergebnisse 11
1. Generelle Einschätzung 11
2. Zustimmung ohne Vorbehalt 11
3. Die wichtigsten Vorbehalte 11
III. Stellungnahmen zu den einzelnen Bestimmungen des VE-BÜPF 14
1. Allgemeine Bestimmungen 14
1.1. Artikel 1 Sachlicher Geltungsbereich 14
1.2. Artikel 2 Persönlicher Geltungsbereich 14
1.3. Artikel 3 Überwachungsdienst 19
1.4. Artikel 4 Bearbeitung von Personendaten 20
1.5. Artikel 5 Post- und Fernmeldegeheimnis 20
2. Informatiksystem zur Verarbeitung der durch die Überwachung des Fernmeldeverkehrs gewonnenen Daten 21
2.1. Artikel 6 Grundsatz 21
2.2. Artikel 7 Zweck des Verarbeitungssystems 21
2.3. Artikel 8 Inhalt des Verarbeitungssystems 22
2.4. Artikel 9 Zugriff auf das Verarbeitungssystem 22
2.5. Artikel 10 Akteneinsichtsrecht und Auskunftsrecht über die Daten 24
2.6. Artikel 11 Aufbewahrungsfrist von Daten 24
2.7. Artikel 12 Sicherheit 26
2.8. Artikel 13 Verantwortung 26
3. Aufgaben des Dienstes 26
3.1. Artikel 14 Auskünfte über Fernmeldeanschlüsse 26
3.2. Artikel 15 Allgemeine Aufgaben der Überwachung 27
3.3. Artikel 16 Aufgaben bei der Überwachung des Fernmeldeverkehrs 28
3.4. Artikel 17 Qualitätskontrolle 30
3.5. Artikel 18 (i.V.m. Art. 24) Zertifizierung 31
4. Pflichten bei der Überwachung des Postverkehrs 32
4.1. Artikel 19 32
5. Pflichten bei der Überwachung des Fernmeldeverkehrs 34
5.1. Artikel 20 Auskünfte über Fernmeldeanschlüsse 34
5.2. Artikel 21 Pflichten bei der Durchführung von Überwachungen 38
5.3. Artikel 22 Identifizierung von Internet-Benutzern 41
5.4. Artikel 23 Datenaufbewahrung 42
5.5. Artikel 24 Zertifizierung 44
5.6. Artikel 25 Information über Technologien und Dienste 44
5.7. Artikel 26 Betreiberinnen von internen Fernmeldenetzen und Hauszentralen und Personen nach Artikel 2 Absatz 1, die ihre Tätigkeit im Bereich des Fernmeldeverkehrs nicht berufsmässig ausüben 45
6. Überwachung ausserhalb von Strafverfahren 45
6.1. Artikel 27 Notsuche 45
6.2. Artikel 28 Suche nach verurteilten Personen 46
6.3. Artikel 29 Verfahren 47
7. Kosten und Gebühren 47
7.1. Artikel 30 48
8. Strafbestimmungen 50
8.1. Artikel 31 Übertretungen 50
8.2. Artikel 32 Gerichtsbarkeit 51
9. Aufsicht und Rechtsschutz 52
9.1. Artikel 33 Aufsicht 52
9.2. Artikel 34 Rechtsschutz 53
10. Schlussbestimmungen 54
10.1. Artikel 35 Vollzug 54
10.2. Artikel 36 Aufhebung und Änderung bisherigen Rechts 54
10.3. Artikel 37 Übergangsbestimmung 54

10.4. Artikel 38 Referendum und Inkrafttreten 55
11. Aufhebung und Änderung bisherigen Rechts (Anhang; Art. 36 VE-BÜPF) 55
11.1. Strafprozessordnung vom 5. Oktober 2007 (StPO) 55
11.2. Militärstrafprozess vom 23. März 1979 (MStP) i 62
11.3. Fernmeldegesetz vom 30. April 1997 (FMG) 64

Liste der Teilnehmer am Vernehmlassungsverfahren mit Abkürzungen

KANTONE

Regierungsrat Kt. Zürich	ZH
Regierungsrat Kt. Bern	BE
Regierungsrat Kt. Luzern	LU
Regierungsrat Kt. Uri	UR
Regierungsrat Kt. Schwyz	SZ
Regierungsrat Kt. Obwalden	OW
Regierungsrat Kt. Nidwalden	NW
Regierungsrat Kt. Glarus	GL
Regierungsrat Kt. Zug	ZG
Conseil d'Etat du canton de Fribourg	FR
Regierungsrat Kt. Solothurn	SO
Regierungsrat Kt. Basel-Stadt	BS
Regierungsrat Kt. Basel-Landschaft	BL
Regierungsrat Kt. Schaffhausen	SH
Regierungsrat Kt. Appenzell Ausserrhoden	AR
Standeskommission Kt. Appenzell Innerrhoden	AI
Regierungsrat Kt. St. Gallen	SG
Regierungsrat Kt. Graubünden	GR
Regierungsrat Kt. Aargau	AG
Regierungsrat Kt. Thurgau	TG
Consiglio di Stato del Cantone del Ticino	TI
Conseil d'Etat du canton de Vaud	VD
Conseil d'Etat du canton de Valais	VS
Conseil d'Etat du canton de Neuchâtel	NE
Conseil d'Etat du canton de Genève	GE
Gouvernement du canton du Jura	JU

POLITISCHE PARTEIEN

CSP Christlich-soziale Partei CSP
PCS Parti chrétien-social
PCS Partito cristiano sociale
PCS Partida cristian-sociala

CVP Christlichdemokratische Volkspartei der Schweiz CVP
PDC Parti démocrate-chrétien suisse
PPD Partito popolare democratico svizzero
PCD Partida cristiandemocrata svizra

FDP. Die Liberalen FDP
PLR. Les Libéraux-Radicaux
PLR. I Liberali
PLD. Ils Liberals

Grüne Partei der Schweiz GPS
Les Verts Parti écologiste suisse
I Verdi Partito ecologista svizzero
La Verda Partida ecologica svizra

Piratenpartei Schweiz PPS
Parti Pirate Suisse

SP Schweiz Sozialdemokratische Partei der Schweiz SP
PS Parti socialiste suisse
PS Partito socialista svizzero
PS Partida socialdemocrata da la Svizra

SVP Schweizerische Volkspartei SVP
UDC Union Démocratique du Centre
UDC Unione Democratica di Centro
PPS Partida Populara Svizra

GESAMTSCHWEIZERISCHE DACHVERBÄNDE DER GEMEINDEN, STÄDTE UND BERGGEBIETE

Schweizerischer Städteverband SSV
Union des villes suisses
Unione delle città svizzere

GESAMTSCHWEIZERISCHE DACHVERBÄNDE DER WIRTSCHAFT

economiesuisse economiesuisse
Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss business federation

Schweiz. Gewerkschaftsbund Union syndicale suisse (USS) Unione sindacale svizzera (USS)	SGB
Schweizerischer Arbeitgeberverband Union patronale suisse Unione svizzera degli imprenditori	SAG
Schweizerischer Bauernverband Union suisse des paysans (USP) Unione svizzera dei contadini (USC)	SBV

ÜBRIGE ORGANISATIONEN, INSTITUTIONEN UND EINZELPERSONEN

Cablecom GmbH	Cablecom
Centre Patronal	CP
Chaos Computer Club Zürich	CCC
Cognizant Technology Solutions S.A	COG
Colt Telecom Services AG	Colt
Demokratische Juristinnen und Juristen der Schweiz Juristes Démocrates de Suisse (JDS) Giuristi e Giuriste Democratici Svizzeri (GDS)	DJS
Die Schweizerische Post	
Eidgenössische Spielbankenkommission Commission fédérale des maisons de jeu (CFMJ) Commissione federale delle case da gioco (CFCG)	ESBK
„ePower für die Schweiz“ Parlamentariergruppe	ePower
ETH Eidgenössische Technische Hochschule Zürich	ETH
Finecom Telecommunications AG	Finecom
grundrechte.ch droitsfondamentaux.ch dirittifondamentali.ch	gr.ch
Hauser Ralf	HR
Hewlett-Packard (Schweiz) GmbH	hp
ICTSwitzerland Information and Communication Technology	ICT

ifpi Schweiz (Dachverband der Ton- und Tonbildträgerhersteller)	ifpi
Information Security Society Switzerland	ISSS
INT Informatik AG	INT
Komitee für eine freie Gesellschaft	KFG
Konferenz der kantonalen Justiz- und Polizeidirektoren Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP)	KKJPD
Konferenz der kantonalen Polizeikommandanten der Schweiz Conférence des commandants des polices cantonales de suisse (CCPCS) Conferenza dei comandanti delle polizie cantonali della svizzera (CCPCS)	KKPKS
Konferenz der Strafverfolgungsbehörden der Schweiz Conférence des autorités de poursuite pénale de Suisse (CAPS) Conferenza della autorità inquirenti svizzere (CAIS)	KSBS
Konsumentenforum kf	kf
Métille Sylvain	MS
Orange Communications SA	Orange
privatim - Die schweizerischen Datenschutzbeauftragten privatim - Les commissaires suisses à la protection des données privatim - Gli incaricati svizzeri della protezione dei dati	privatim
Rosenthal David	RD
Schweizerische Informatikkonferenz Conférence suisse sur l'informatique Conferenza svizzera sull'informatica	SIK
Schweizerische Kriminalistische Gesellschaft Société Suisse de droit pénal (SSDP) Società svizzera di diritto penale (SSDP)	SKG
SAFE Schweizerische Vereinigung zur Bekämpfung der Piraterie	safe
Schweizerischer Anwaltsverband Fédération suisse des avocats (FSA) Federazione svizzera degli avvocati (FSA)	SAV
Schweizerischer Verband der Telekommunikation Association Suisse des Télécommunications (asut)	asut

Schweizerisches Polizei-Institut Institut suisse de police (ISP) Istituto svizzero di polizia (ISP)	SPI
Sitrox AG	Sitrox
Stiftung für Konsumentenschutz	SKS
Sunrise Communications AG	Sunrise
SWICO (Der Wirtschaftsverband für die Digitale Schweiz)	SWICO
SIMSA swiss internet industry association	SIMSA
Swiss Internet User Group	SIUG
SWISS POLICE ICT (Schweizer Polizei Informatik Kongress SPIK)	SPICT
Swisscable (Verband für Kommunikationsnetze)	Swisscable
Swisscom (Schweiz) AG	Swisscom
SWITCH Serving Swiss Universities	switch
Switchplus AG	switchplus
United Security Providers AG **Fargate AG** **Futurecom Interactive AG** **OneConsult GmbH** **Stories AG** **Neidhart + Schön Group AG** **Viollier Consulting AG** **midix.com ag** **Open systems ag** **Namics AG** **InVisible GmbH** **Köpfli & Partner AG** **Dinotronic AG** **terreActive** **von salis engineering GmbH** **Dr. Hartwig Thomas** **Icontel AG** **ISPIN AG** **WIRZ Grupppe**	IT(19)
Universität St. Gallen	UNISG
Universität Zürich	UNIZH

Verband Schweizerischer Polizei-Beamter Fédération suisse fonctionnaires de polices (FSFP) Federazione svizzera dei funzionari di polizia (FSFP)	VSPB
Verein Swiss Privacy Foundation	VSPF
Verizon Switzerland AG	Verizon
3D4X Internetagentur & Softwareentwicklung	3D4X

I. Einleitung

Mit Beschluss vom 19. Mai 2010[1] hat der Bundesrat das Eidgenössische Justiz- und Polizeidepartement (EJPD) beauftragt, über den Bericht[2] und den Vorentwurf[3] zur Änderung des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)[4] ein Vernehmlassungsverfahren durchzuführen. Es handelt sich dabei um eine Totalrevision des BÜPF mit dem vorrangigen Ziel, das Gesetz an die technische Entwicklung der letzten Jahre, insbesondere im Internetbereich, anzupassen.

Mit Rundschreiben vom 19. Mai 2010 hat das EJPD die Kantone, die in der Bundesversammlung vertretenen Parteien sowie die interessierten Verbände und Organisationen zur Stellungnahme bis am 18. August 2010 eingeladen.

Es sind 106 Stellungnahmen eingegangen, die zusammen ca. 700 Seiten umfassen. Von den 93 zur Stellungnahme eingeladenen Adressaten sind 55 Antworten eingegangen, worunter 4 ausdrückliche Verzichte auf eine inhaltliche Vernehmlassung. Somit haben 51 Vernehmlassungsteilnehmer von sich aus die Möglichkeit wahrgenommen, sich am Vernehmlassungsverfahren zu beteiligen.

Es haben Stellung genommen:

26 Kantone

6 politische Parteien

74 interessierte Kreise.

---

1 http://www.bj.admin.ch/content/bj/de/home/dokumentation/medieninformationen/2010/ref_2010-05-19.html

2 http://www.bj.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/vn-ber-d.pdf

3 http://www.bj.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/entw-d.pdf

4 SR 780.1

II. Übersicht der Ergebnisse

1. Generelle Einschätzung

Die Notwendigkeit das BÜPF an die technische Entwicklung der letzten Jahre, insbesondere im Internetbereich, anzupassen, wurde von den Vernehmlassungsteilnehmern durchwegs anerkannt bzw. nicht bestritten. Bezüglich der gesetzgeberischen Umsetzung wurden von verschiedenen Seiten jedoch zahlreiche, zum Teil strukturelle und umfassende Vorbehalte zu den einzelnen Bestimmungen des Vorentwurfs angebracht oder gar eine komplette Überarbeitung vorgeschlagen. Mehrere Teilnehmer[5] bemängeln zudem die umständliche Sprache des Vorentwurfs (VE-BÜPF). Nachfolgend werden zunächst diejenigen Teilnehmer aufgeführt, welche dem Vorentwurf vorbehaltlos zustimmten (Ziff. 2). Anschliessend werden die wichtigsten Vorbehalte angeführt (Ziff. 3), bevor unter III. die Stellungnahmen zu den einzelnen Bestimmungen zusammengefasst dargestellt werden.

2. Zustimmung ohne Vorbehalt

3 Kantone (UR, OW, GE) sowie die Schweizerische Post (soweit die Überwachung des Postverkehrs betreffend) stimmen dem Vorentwurf vorbehaltlos zu.

3. Die wichtigsten Vorbehalte

Persönlicher Geltungsbereich (Art. 2 VE-BÜPF)

Einige Teilnehmer[6] bemängeln generell, dass aus dem Wortlaut von Artikel 2 VE-BÜPF nicht klar erkennbar ist, wer konkret erfasst werden soll. Etliche Teilnehmer[7] lehnen die Ausdehnung des persönlichen Geltungsbereiches in Artikel 2 Absatz 1 Buchstabe b VE-BÜPF ab und fordern die Streichung, die Beschränkung oder zumindest eine Umformulierung. Manche Teilnehmer beantragen bezüglich Artikel 2 Absatz 2 VE-BÜPF eine Klarstellung, wer konkret betroffen ist[8], und in Verbindung mit Artikel 26 VE-BÜPF, welche Pflichten diese Personen treffen[9]. GPS, SGB und INT verweisen zudem darauf, dass die Ausweitung des Geltungsbereiches insbesondere für kleinere Betriebe existenzbedrohend sein kann. Gemäss RD ist es systemwidrig, das BÜPF über den Kreis der Fernmeldedienstanbieterinnen hinaus auf Personen auszudehnen, die nicht dem Fernmeldegeheimnis unterstehen.

Informatiksystem zur Verarbeitung der durch die Überwachung des Fernmeldeverkehrs gewonnenen Daten (Art. 6 – 13 VE-BÜPF)

Etliche Teilnehmer[10] lehnen die dauernde zentrale Aufbewahrung der Daten beim Überwachungsdienst (nachfolgend: Dienst) ab und beantragen die grundsätzliche Beibehaltung des alten Systems (Aufzeichnung der Daten, Überspielen auf Datenträger, Übermittlung an die

---

5 BE, SZ, NW, SH, LU, SH, CVP, KSBS, SKG.
6 FR, VD, CVP, ISSS, CP, RD.
7 FDP, PPS, SIUG, switch, switchplus, RD, SWICO, hp, COG, ISSS, DJS, gr.ch, SKS, GPS, SGB, KFG, INT, SIK, asut, Finecom, Orange, Swisscom, Colt, Verizon, VSPF.
8 LU, ETH, UNISG, asut, Swisscom, Finecom, Orange, Colt, Sunrise, Verizon, Swisscable, switch.
9 LU, BL, AR, SP, privatim.
10 SO, BE, NW, BL, LU, SZ, SO, SG, SH, SKG, KSBS.

ermittelnden Behörden, Löschung der Daten beim Dienst). Einige Teilnehmer[11] sprechen sich dafür aus gesetzlich festzuhalten, dass die Umstände des Einzelfalls (bspw. im Rahmen der internationalen Rechtshilfe) eine postalische Zustellung mittels Datenträgern oder Dokumenten (bisheriges System) nach wie vor erforderlich machen können. Andere[12] wiederum beantragen, die zentrale dauernde Speicherung der Daten verbunden mit einem externen Zugriff aufgrund der anfallenden, immensen Menge von Daten für den Bereich Internetüberwachung vorzusehen, Telefonüberwachungen aber, wie bisher, auf Datenträgern zu speichern und zu versenden. Mehrere Teilnehmer[13] sehen im neuen System eine Verletzung der Parteirechte, da die Parteien gemäss der Schweizerischen Strafprozessordnung vom 5. Oktober 2007 (StPO)[14] Zugriff auf die Originalakten haben müssen. Ein Zugriff der Parteien wird aus sicherheitstechnischen Gründen abgelehnt. Eine grössere Teilnehmerzahl[15] hält die Regelung des Akteneinsichts- und Auskunftsrechts in Artikel 10 VE-BÜPF für unnötig, da die StPO ausreichende Schutzbestimmungen für personenbezogene Daten enthält. Diverse Teilnehmer[16] halten schliesslich die Regelung der Aufbewahrungsfristen in Artikel 11 VE-BÜPF, welche an die Verjährungsfristen anknüpft, für zu kompliziert und aufwändig und sprechen sich auch vor diesem Hintergrund für die Beibehaltung des alten Systems aus. Die Aufbewahrungsfristen sollen sich ausschliesslich nach der StPO richten.

Fehlende Prüfungspflicht des Dienstes und Rechtsschutz

Zahlreiche Teilnehmer[17] fordern, dass der Dienst die Pflicht haben muss, die rechtliche Zulässigkeit angeordneter Überwachungen zu überprüfen (vgl. auch Bemerkungen in III. Ziff. 3.2.1 zu Art. 15 Bst. a und in III. Ziff. 3.3.1 zu Art. 16 Bst. a), und dementsprechend in Artikel 34 VE-BÜPF (Rechtsschutz) für die zur Überwachung Verpflichteten die Möglichkeit vorgesehen werden muss, die Rechtmässigkeit einer Überwachungsanordnung gerichtlich überprüfen zu lassen. In diesem Zusammenhang weisen einige Teilnehmer[18] auf den Widerspruch im Verhältnis zu Artikel 33 VE-BÜPF hin, wonach der Dienst über die Einhaltung der Gesetzgebung wacht.

Pflichten bei der Durchführung der Überwachung (Art. 21 VE-BÜPF)

Für eine Vielzahl von Teilnehmern[19] sind die konkreten Pflichten für Personen, welche eine Überwachung durchzuführen haben, zu wenig klar geregelt. Im Sinne der Rechtssicherheit fordern sie daher, teilweise mit konkreten Formulierungsvorschlägen, ein klares Pflichtenheft vorzusehen.

Identifizierung von Internet-Benutzern (Art. 22 VE-BÜPF)

Eine grosse Anzahl Teilnehmer[20] beantragt die Streichung bzw. Anpassung der Bestimmung.

---

11 ZH, LU, AG, GL, GR, TG, VS, JU, KKJPD, KKPKS, CCC.
12 LU, SZ, SO, SG, SH, KSBS.
13 BE, NW, BS, BL, SKG, SAV, MS.
14 AS 2010 1881; in Kraft per 1.1.2011.
15 LU, NW, BL, SG, GL, TG, VS, JU, KKJPD KSBS, SKG.
16 BE, SZ, NW, BL, SH, SG, AG, VD, KSBS.
17 ZG, BE, BL, AR, FDP, SP, Swisscable, SWICO, SSV, Cablecom, asut, Orange, Swisscom, Colt, Sunrise, Verizon, KSBS, privatim, economiesuisse, SIUG, hp, COG, ISSS, VSPF, GPS, SKS, IT(19).
18 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, SWICO, hp, COG.
19 CVP, FDP, SVP, GPS, SKS, economiesuisse, ICT, ePower, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, SIUG, SPICT.
20 VD, GPS, SVP, FDP, ISSS, SSV, privatim, DJS, gr.ch, RD, IT(19), Cablecom, switch und switchplus, CP, SAV, KFG, PPS, ETH, UNISG, UNIZH.

Eine flächendeckende Identifikationspflicht für Internet-Benutzer wird als unverhältnismässig und unpraktikabel empfunden. Schliesslich wird auch auf zahlreiche Umgehungsmöglichkeiten hingewiesen.

Verlängerung der Datenaufbewahrungsfrist auf zwölf Monate (Art. 23 VE-BÜPF)

Eine grosse Teilnehmerzahl[21] lehnt die Bestimmung – zum Teil mit Verweis auf die Kriterien, wie sie vom deutschen Bundesverfassungsgericht[22] im Zusammenhang mit der Vorratsdatenspeicherung entwickelt worden sind – ab bzw. verlangt eine revidierte Regelung. Einige Teilnehmer[23] betonen in diesem Zusammenhang, dass systematisch Daten unverdächtiger Personen auf Vorrat gespeichert werden.

Wegfall der Entschädigung für Personen, welche Überwachungen durchzuführen haben (Art. 30 Abs. 1 VE-BÜPF)

Etliche Teilnehmer[24] sprechen sich gegen die vorgesehene Streichung der Entschädigung für die Durchführung von Überwachungsmassnahmen aus. Die meisten dieser Teilnehmer[25] betonen, dass die Strafverfolgung eine staatliche Aufgabe und daher durch das Gemeinwesen zu tragen ist. Einige[26] weisen auf die Notwendigkeit der Beschaffung teurer Infrastruktur hin, um den neuen Anforderungen des Gesetzes Genüge zu tun. Manche Teilnehmer beantragen eine differenziertere Regelung[27].

Abfangen und Entschlüsselung von Daten (Art. 270bis StPO); Einführung von Informatikprogrammen in fremde Datenverarbeitungssysteme

Zehn Teilnehmer[28] lehnen die Einführung von Informatikprogrammen („Government Software“, oft auch „Bundestrojaner“ genannt) in ein fremdes Datensystem gänzlich ab; eine grössere Teilnehmergruppe[29] bringt erhebliche Vorbehalte an. Es wird dabei insbesondere auf den massiven Eingriff in die Privatsphäre der Betroffenen hingewiesen, bei welchem sämtliche Daten des betroffenen Datenverarbeitungssystems einsehbar sind. Überdies wird bemängelt, dass nirgends auf das Grundsatzurteil des deutschen Bundesverfassungsgerichts[30] zum Thema „Online-Durchsuchung“ eingegangen wird. Etliche Teilnehmer[31] führen zudem generell Sicherheitsbedenken an, welche sowohl das Informatikprogramm selber und dessen Missbrauch durch Kriminelle als auch das Datenverarbeitungssystem bzw. das Netzwerk betreffen, in welches eingedrungen werden soll. BS, FR, SP und privatim fordern zudem eine Einschränkung des Deliktkatalogs von Artikel 269 Absatz 2 Buchstabe a StPO für den Einsatz von „Bundestrojanern“.

---

21 BL, GPS, SP, SKS, SGB, DJS, gr.ch, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SIUG, ISSS, SWICO, hp, privatim, COG, 3D4X, PPS.

22 Siehe Fn. 120 sowie Ausführungen in III. Ziff. 5.4.

23 DJS, gr.ch, GPS, SKS.

24 SP, CVP, FDP, SVP, GPS, PPS, DJS, gr.ch, RD, ISSS, MS, SIUG, SIMSA, INT, asut, Finecom, Orange, Swisscom, Sunrise, Colt, Verizon, Cablecom, SAV, SKS, Swisscable, CP, CCC, Sitrox, economiesuisse, IT(19), SWICO, hp, COG.

25 CVP, FDP SVP, GPS, asut, Finecom, Orange, Swisscom, Sunrise, Verizon, Cablecom, SAV, SKS Swisscable, SIUG, CP, CCC, Sitrox, PPS.

26 SP, Colt, SIUG, SIMSA, INT, ISSS, PPS, GPS.

27 Die CVP will die Kosten für die Aufrüstung der Systeme entschädigen, wohingegen die SP eine Differenzierung nach Unternehmensgrösse bzw. wirtschaftlicher Tragbarkeit fordert.

28 GPS, DJS, gr.ch, Cablecom, CCC, SKS, SIUG, KFG, PPS, ISSS.

29 ZH, BL, AR, LU, SP, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SIUG, privatim, economiesuisse, Swisscable.

30 BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333); vgl. auch III. Ziff. 11.1.2.

31 GPS, DJS, gr.ch, SKS, KFG, PPS, SIUG.

III. Stellungnahmen zu den einzelnen Bestimmungen des VE-BÜPF

1. Allgemeine Bestimmungen

1.1. Artikel 1 Sachlicher Geltungsbereich

[1] Dieses Gesetz gilt für die Überwachung des Post- und Fernmeldeverkehrs, einschliesslich des Internetverkehrs, die angeordnet und durchgeführt wird:

- *a. im Rahmen eines Strafverfahrens;*
- *b. zum Vollzug eines Rechtshilfeersuchens;*
- *c. im Rahmen der Suche nach vermissten Personen;*
- *d. im Rahmen der Suche nach Personen, die zu einer Freiheitsstrafe verurteilt wurden oder gegenüber denen eine freiheitsentziehende Massnahme angeordnet wurde.*

[2] Für Auskünfte über den Zahlungsverkehr, der dem Postgesetz vom 30. April 1997 untersteht, gelten die Artikel 284 und 285 der Strafprozessordnung vom 5. Oktober 2007 (StPO).

1.1.1 Artikel 1 Absatz 1

Einige Teilnehmer[32] erachten die Begriffe „Post- und Fernmeldeverkehr" sowie „Internetverkehr" in Absatz 1 als zu unpräzis. Den Begriff „Internetverkehr" als Teil des Fernmeldeverkehrs zu bezeichnen, zeugt gemäss der PPS von Unverständnis für dieses Medium sui generis, da das Internet eben kein erweitertes Telefon und auch kein erweitertes Fax ist. Für UNISG, switch und switchplus ist insbesondere unklar, ob bspw. die Nutzung weiterer auf TCP[33]/IP[34] basierender Dienste wie HTTP[35], FTP[36] und Telnet[37] zum Internetverkehr im Sinne des Gesetzes zählen oder nicht. Dasselbe gilt gemäss UNIZH für Dienste wie Skype-Telefonie[38], PPTP[39] und Teredo[40]. asut vertritt die Meinung, dass eine Überwachungsmassnahme nur die Individualkommunikation umfassen darf, d.h. nur bestimmte Anschlüsse überwacht werden dürfen. Demgegenüber ist der VSPB der Ansicht, dass die oben genannten Begriffe im Hinblick auf einen zukünftigen technologischen Ausbau zu eingrenzend sind und daher eine leichtere und vollständigere, aber vor allem flexiblere Formulierung gefunden werden sollte.

Zur neu vorgesehenen Möglichkeit, nach verurteilten Personen zu fahnden (Art. 1 Abs. 1 Bst. d VE-BÜPF), siehe die Bemerkungen in III. Ziffer 6.2 zu Artikel 28 VE-BÜPF.

1.1.2 Artikel 1 Absatz 2

Keine Bemerkungen.

1.2. Artikel 2 Persönlicher Geltungsbereich

[1] Nach diesem Gesetz führen folgende Personen Überwachungen durch:

- *a. Anbieterinnen von Post- und Fernmeldediensten, einschliesslich Internet-Anbieterinnen, die ihre Tätigkeit berufsmässig ausüben;*

---

32 VD, UNIZH, PPS, UNISG, switch, switchplus, ETH.
33 Transmission Control Protocol.
34 Internet-Protokoll.
35 Hypertext Transfer Protocol.
36 File Transfer Protocol.
37 Telecommunication Network.
38 Kostenlose VoIP (Voice over IP) Software.
39 Point-to-Point Tunneling Protocol.
40 Teredo ist ein Kommunikationsprotokoll für den Datenverkehr mit dem Internet.

b. Personen, die berufsmässig für Personen nach Buchstabe a Kommunikationsdaten verwalten, an Dritte Kommunikationsdaten weiterleiten oder die dafür notwendige Infrastruktur zur Verfügung stellen.

[2] Betreiber von internen Fernmeldenetzen und Hauszentralen sowie die in Absatz 1 genannten Personen, die ihre Tätigkeit im Bereich des Fernmeldeverkehrs nicht berufsmässig ausüben, sind gehalten, Überwachungen nach diesem Gesetz zu dulden.

Mehrere Teilnehmer[41] fordern generell eine Präzisierung von Artikel 2, da unklar ist, wer konkret erfasst werden soll.

NE, ETH und UNISG beantragen, den Begriff „berufsmässig" durch „kommerziell" zu ersetzen bzw. gemäss anderen Teilnehmern[42] durch „kommerziell und mit Gewinnabsicht".

1.2.1 Artikel 2 Absatz 1 Buchstabe a

Einige Teilnehmer[43] bemängeln, dass der Begriff „Internet-Anbieterinnen" nicht im Gesetz definiert wird. switch schlägt vor, als „Internet-Anbieterinnen" diejenigen zu erfassen, welche E-Mail und Telefondienste über IP anbieten.

1.2.2 Artikel 2 Absatz 1 Buchstabe b

Eine grosse Anzahl Teilnehmer[44] erachtet die vorgeschlagene Ausweitung des Geltungsbereichs für dringend erforderlich. kf begrüsst, dass mit höherer Genauigkeit festgelegt wird, wer dem Gesetz untersteht.

Demgegenüber lehnen etliche Teilnehmer[45] die Ausdehnung des Geltungsbereichs ab und fordern die Streichung, die Beschränkung oder zumindest eine Umformulierung von Buchstabe b. Gemäss einigen Teilnehmern[46] werden mit der Ausdehnung des Geltungsbereichs neu sämtliche Anbieter von Diensten, Inhalten oder technischen Leistungen, die für die Nutzung oder den Betrieb von Inhalten und Diensten im Internet erforderlich sind, erfasst, bzw. gemäss RD und PPS jedes Unternehmen, das in irgendeiner Weise beruflich mit Kommunikationsdaten zu tun hat. Damit sind sämtliche Firmen und Personen in einem kompletten Wirtschaftszweig zur aktiven Überwachung, Anschaffung der entsprechenden Ausrüstung und Bereitstellung von Personalressourcen verpflichtet – und dies auf eigene Kosten. Eine solche Ausdehnung ist unverhältnismässig und nicht akzeptabel. Es wird gefordert, dass der Geltungsbereich weiterhin auf professionelle Internet-Zugangsanbieterinnen zu beschränken ist, und nicht auf Hosting-Provider und Inhaltsanbieterinnen ausgedehnt werde.

Mehrere Teilnehmer[47] wollen sodann den Geltungsbereich auf Unternehmen bzw. juristische Personen beschränken, welche Fernmeldedienste anbieten oder geschäftsmässig bzw. kommerziell und mit Gewinnabsicht[48] oder berufsmässig[49] Kommunikationsdaten für Fernmeldedienstanbieterinnen verwalten.

---

41 FR, VD, CVP, ISSS, CP, RD.
42 switch, asut, Finecom, Swisscom, Colt, Sunrise, Verizon.
43 SIUG, switch, switchplus, HR, ETH, UNISG.
44 ZH, ZG, LU, SZ, NW, AR, SO, SH, SG, GR, AG, TG, TI, VS, NE, GE, JU, FDP, ICT, ePower, SPICT, KKJPD, KKPKS, KSBS.
45 FDP, SIUG, VSPF, switch, switchplus, RD, PPS, SWICO, hp, COG, ISSS, DJS, gr.ch, SKS, GPS, SGB, KFG, INT, SIK, asut, Finecom, Orange, Swisscom, Colt, Verizon, VSPF.
46 SIUG, VSPF, switch, switchplus, RD, PPS.
47 asut, Finecom, Orange, Swisscom, Colt, Verizon, SWICO, hp, COG, ISSS.
48 asut, Finecom, Orange, Swisscom, Colt, Verizon.
49 Orange, Cablecom.

Gemäss SIMSA muss das massgebliche Kriterium bei der Festlegung der überwachungspflichtigen Personen das Angebot der Individualkommunikation sein. Das Bestreben, möglichst alle Formen von Kommunikation unter den Vorbehalt der Überwachung zu stellen, kommt gemäss DJS und gr.ch deutlich im erweiterten Geltungsbereich zum Ausdruck.

SKS, GPS, SGB und KFG empfinden es als unerhört, dass die Auswirkungen auf die neu Unterstellten nicht dargestellt werden. Gemäss GPS und SGB sind für die kleinen lokalen Provider schon die für die Überwachung erforderlichen Investitionskosten ein Dilemma und unter Umständen existenzbedrohend. Als kleiner, von dieser Ausweitung direkt betroffener Hosting-Anbieter ist INT zudem der Ansicht, dass die Revision mit Blick auf die Kosten äusserst wirtschaftsfeindlich ist, da dadurch vor allem kleinen Unternehmen praktisch die Möglichkeit genommen wird, eine Kommunikations-Infrastruktur gesetzeskonform zu betreiben. Zudem ist die Realität im Zeitalter des Internets so, dass jedem Nutzer kostenlose, sichere Verschlüsselung und Anonymisierung (z.B. Tor oder Freenet) zur Verfügung steht und darum jede Überwachung des Internets eine Farce ist. Die Revision ist daher nutzlos und zudem KMU-feindlich.

RD weist zudem darauf hin, dass das Ziel, bestimmte Anbieter, wie etwa Betreiber reiner E-Mail-Plattformen wie GMX, Hotmail oder Gmail, neu zu erfassen, schon aus praktischen Gründen nicht erreicht werden kann, da sie sich erfahrungsgemäss alle im Ausland befinden und dort das BÜPF keine Anwendung findet. Die geplante Erweiterung des Geltungsbereichs löst zudem das Problem nicht, dass der Endbenutzer seine Kommunikation bzw. seine Daten verschlüsselt (Skype-Problematik) und seinem Internet-Anbieter (ob Fernmeldedienstanbieter im Sinne des Gesetzes oder nicht) seinen Schlüssel nicht anvertraut. Es darf zudem nicht vergessen werden, warum es das BÜPF überhaupt gibt. Der Grund hierfür ist u.a., dass Fernmeldedienstanbieter unter dem Fernmeldegeheimnis stehen und deshalb gesetzlich geregelt sein muss, wann und wie sie Informationen, die eben diesem Berufsgeheimnis unterstehen, herausgeben müssen. Das bedeutet aber auch, dass es systemwidrig ist, das BÜPF nun über den Kreis eben jener Fernmeldedienstanbieter hinaus auch auf andere Personen auszudehnen, die nicht dem Fernmeldegeheimnis unterstehen. Die anderen Anbieter, die erfasst werden sollen, unterliegen dem Fernmeldegeheimnis höchstens ausnahmsweise. Ihre Unterlagen sind somit auch unter Verwendung der herkömmlichen strafprozessualen Mittel zugänglich. Es gibt schon deshalb keinen Grund, solche Anbieter ebenfalls dem BÜPF zu unterstellen. Tut man es doch, wird die Aufgabe der Strafverfolgungsbehörden möglicherweise sogar erschwert, da diesfalls ohne Weiteres vertreten werden kann, dass durch die Regelung in einem Spezialgesetz alle anderen allgemeinen Regelungen betreffend Herausgabe von Unterlagen, Erteilung von Auskünften oder Beschlagnahmungen mitunter nicht mehr gelten. Die geplante Erweiterung des Anwendungsbereichs ist schon deshalb problematisch, weil die Pflichten auf Fernmeldedienstanbieter zugeschnitten sind und deshalb überhaupt nicht klar ist, wie die neu Verpflichteten diese erfüllen können. Letztere können bspw. Betreiber einer Website sein, die über irgendeine Funktion verfügt, mit der Personen einander Mitteilungen zukommen lassen können. Einerseits betreiben diese entweder Mailserver für Dritte bzw. haben ihn an einen Server einer Fernmeldedienstanbieterin angebunden, andererseits übertragen sie bei jedem Übermittlungsvorgang E-Mails von Dritten an den Mailserver des Empfängers. Es kann ohne Weiteres vertreten werden, dass dies somit Unternehmen sind, die berufsmässig an Dritte Kommunikationsdaten weiterleiten bzw. die dafür nötige Infrastruktur zur Verfügung stellen. Weiter würden auch unzählige Hosting-Provider in den Geltungsbereich fallen, so z.B. auch solche, die E-Commerce-Plattformen anbieten, wie etwa eBay oder Ricardo und jede Firma, die es auf ihrer Website Dritten erlaubt, irgendwelche Kommentare kund zu tun (z.B. in einem Gästebuch oder einem Blog). Denn auch diese leiten letztlich Kommunikationsdaten (z.B. den Inhalt einer Verkaufsanzeige) an Dritte (die Besucher) weiter bzw. stellen die dafür nötige Infrastruktur zur Verfügung. Der erläuternde Bericht spricht denn in diesem Zusammenhang auf Seite 17 offen davon, dass reine

„Hosting-Provider“ erfasst werden sollen. Auch alle elektronischen Medien, die Leserbriefe oder Anzeigen im Internet veröffentlichen, sind nach heutigem Verständnis Hosting-Provider und sollen offenbar erfasst werden. All diese Unternehmen müssten somit enorme Infrastrukturen auf eigene Kosten aufbauen, um die vorgesehenen Pflichten erfüllen zu können. Zweifellos ist es für eine Strafverfolgungsbehörde verlockend, in alle und jegliche Vorgänge im Internet jederzeit Einblick erhalten zu können. Dies kann und sollte jedoch nicht Zweck des BÜPF sein, das lediglich der Überwachung der Telekommunikation, und nicht aller Teile der „digitalen“ Welt dienen soll.
RD sei kein westliches Land bekannt, welches das Internet derart weitgehend überwacht, wie dies der Vorentwurf im Ergebnis vorsieht. Selbst Betreiber von internen Fernmeldenetzen und Hauszentralen, die zwar in Absatz 2 separat aufgeführt werden, könnten aufgrund der Formulierung in Artikel 2 Absatz 1 Buchstabe b VE-BÜPF nunmehr erfasst sein, denn sie würden die zur Weiterleitung von Kommunikationsdaten an Dritte erforderliche Infrastruktur bereitstellen. Selbst wenn dem entgegengehalten wird, dass damit der Verkehr der Unternehmen selbst nicht gemeint ist, könnten trotzdem zahlreiche Unternehmen erfasst sein, nämlich solche, die ihren Mitarbeitern erlauben, private Telefongespräche zu führen oder E-Mails zu versenden oder Unternehmen, die innerhalb von Firmengruppen als IT- und Telecom-Service-Center auftreten und in dieser Funktion für andere Gruppengesellschaften Fernmeldedienstleistungen erbringen. Auch hier sind die Konsequenzen der Erweiterung des persönlichen Anwendungsbereichs im VE-BÜPF völlig unverhältnismässig. Auch Firmen, die Dienstleistungen im Netzwerksicherheitsbereich anbieten (z.B. Managed Security Services), in dem sie z.B. Netzwerke von Firmen überwachen und verwalten (z.B. durch den Betrieb von Firewalls), können in den Geltungsbereich fallen. Denn es könnte vertreten werden, dass sie z.B. mit der Bereitstellung einer Firewall beruflich die notwendige Infrastruktur zur Verfügung stellen, damit Kommunikationsdaten an Dritte weitergeleitet werden können. Auch Firmen, die Netzwerk-Hard- oder Software in der Schweiz verkaufen, fallen unter den Geltungsbereich, da sie Fernmeldedienstanbietern bzw. auch anderen Unternehmen zweifellos notwendige Infrastruktur zur Verfügung stellen, indem sie solche verkaufen oder vermieten. Gemäss RD zeigen diese Beispiele auf, dass die Erweiterung des Anwendungsbereichs des BÜPF und die Folgen nicht wirklich durchdacht worden sind. Er plädiert daher für den Verzicht auf die Erweiterung bzw. sie zumindest grundlegend umzugestalten, so dass selbst bei weiter Auslegung tatsächlich nur jene erfasst werden, die es treffen soll.

SIK betont, dass sämtliche ihrer Mitglieder, also die öffentlichen Verwaltungen aller Staatsebenen, durch die fragliche Bestimmung dem BÜPF unterstellt werden könnten, betreiben sie doch in der Regel Computer- und Telefonnetze, an die zum Zweck der Erfüllung von Verwaltungsaufgaben auch Dritte (z.B. Kantone, Gemeinden, andere Behörden) angeschlossen sind. Daher hält SIK die Bestimmung im Allgemeinen und ihre Anwendung auf die Netze öffentlicher Verwaltungen im Besonderen für problematisch und beantragt Streichung von Buchstabe b.

VD weist in seiner Stellungnahme darauf hin, dass der Begriff „Kommunikationsdaten“ in Artikel 2 Absatz 1 Buchstabe b für die Frage, wer nun in den Geltungsbereich fällt, nicht weiterhilft. Gemäss heutiger Praxis sind die meisten Fernmeldeanbieter bereit, den Polizeibehörden Daten direkt oder auf Ersuchen eines Magistraten herauszugeben, weil sie davon ausgehen, dass sie nicht dem Fernmeldegeheimnis unterstehen. Es stellt sich deshalb die Frage, ob die vorgeschlagene Totalrevision zur Folge hat, dass diese inskünftig nur noch im Rahmen des BÜPF tätig werden dürfen.

ETH und UNISG machen auf folgenden Widerspruch aufmerksam: Gemäss erläuterndem Bericht sind „Schulen“ von der Überwachungspflicht ausgenommen, werden aber im erläuternden Bericht zu Artikel 22 („Identifizierung von Internet-Benutzern“) trotzdem als Verpflichtete erwähnt. Buchstabe b ist deshalb dahingehend zu präzisieren, dass nur diejenigen An-

bieter unter das BÜPF fallen, die Leistungen für Personen nach Buchstabe a erbringen. ETH verlangt zudem, dass sie als öffentlichrechtliche Anstalt, welche Dienste nur für Studierende und nahestehende Organisationen anbietet, nicht dem BÜPF im Sinne von Absatz 1 unterstellt wird. Gemäss UNIZH lässt der Begriff „Personen" offen, ob das Gesetz auf Anstalten anwendbar ist. Aufgrund der aktuellen Formulierung gehe sie jedoch davon aus, dass das Gesetz für sie als Anstalt des Kantons nicht anwendbar ist. Sie geht überdies davon aus, dass das konturlose Merkmal der „Berufsmässigkeit" nicht auf sie zutrifft, da sie im Dienst der Pflege und Entwicklung der Wissenschaft steht. SWITCH fordert in diesem Zusammenhang eine Präzisierung von Buchstabe b, wonach Schulen und Hochschulen und die mit der Erbringung deren (Netz-) Infrastruktur beauftragten Institutionen wie SWITCH nicht dem BÜPF unterstehen.

1.2.3 Artikel 2 Absatz 2 in Verbindung mit Artikel 26

Art. 2 Abs. 2

[2] Betreiber von internen Fernmeldenetzen und Hauszentralen sowie die in Absatz 1 genannten Personen, die ihre Tätigkeit im Bereich des Fernmeldeverkehrs nicht berufsmässig ausüben, sind gehalten, Überwachungen nach diesem Gesetz zu dulden.

Art. 26 Betreiberinnen von internen Fernmeldenetzen und Hauszentralen und Personen nach Artikel 2 Absatz 1, die ihre Tätigkeit im Bereich des Fernmeldeverkehrs nicht berufsmässig ausüben

Die Betreiberinnen von internen Fernmeldenetzen und Hauszentralen müssen den vom Dienst beauftragten Personen Zutritt gewähren. Die in Artikel 2 Absatz 1 genannten Personen, die ihre Tätigkeit im Bereich des Fernmeldeverkehrs nicht berufsmässig ausüben, sind gehalten, den vom Dienst beauftragten Personen Zutritt zu den von ihnen verwendeten Einrichtungen zu gewähren. Die oben erwähnten Betreiberinnen und Personen müssen den vom Dienst beauftragten Personen die notwendigen Auskünfte erteilen.

Einige Teilnehmer[50] fordern mit konkreten Formulierungsvorschlägen eine Präzisierung von Absatz 2 und Artikel 26, um klarzustellen, dass u.a. alle Arten von Schulen sowie Spitäler und Hotels nicht unter Artikel 2 Absatz 1 fallen. ETH hält fest, dass sie als Betreiberin von internen Fernmeldenetzen und einer Hauszentrale gemäss Absatz 2 zu gelten hat. Sie erbringt keinen Fernmeldedienst gemäss Artikel 2 Buchstabe c der Verordnung vom 9. März 2007 über Fernmeldedienste (FDV)[51] und ist nicht Internet-Anbieterin im Sinne von Artikel 2 Buchstabe a der Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)[52]. Die Teilnehmer schlagen vor, den Begriff „nicht berufsmässig" durch „nicht kommerziell und ohne Gewinnabsicht" zu ersetzen.

Angesichts der drohenden strafrechtlichen Folgen und im Interesse der Rechtssicherheit fordert LU eine Klarstellung der Frage, wer die „nicht berufsmässigen" Anbietenden von Post- und Fernmeldediensten sind, und zusammen mit BL, AR, SP und privatim, welche konkreten Pflichten Personen nach Absatz 2 treffen. Gemäss SIUG werden alle Privatpersonen, Organisationen und Unternehmen, welche Internetdienstleistungen nebenbei anbieten, zur passiven Mithilfe und zur Bereitstellung ihrer Räumlichkeiten und Computereinrichtungen gezwungen. Dies kann bedeuten, dass Passwörter und Verschlüsselungscodes bekanntgegeben werden müssen und unter Zuhilfenahme privater Gerätschaften Abhörmassnahmen durchgeführt werden. Für nicht berufsmässige Akteure dürfen daher weiterhin keine Mithilfe- und Auskunftspflichten bestehen.

Nach Ansicht des CCC wird mit Artikel 26 VE-BÜPF ein Instrument geschaffen, um in private Räume einzudringen. Artikel 26 VE-BÜPF steht somit in Konflikt mit Artikel 13 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV)[53].

---

[50] ETH, UNISG, asut, Swisscom, Finecom, Orange, Colt, Sunrise, Verizon, Swisscable, switch.
[51] SR 784.101.1
[52] SR 780.11
[53] SR 101

Für die PPS gibt es keinen Nutzer und keine Nutzerin des Internets, welche die Voraussetzungen von Artikel 2 Absatz 2 nicht erfüllen. Jeder Betreiber eines LAN (inklusive Privatpersonen) muss daher eine Überwachung seitens des Internet Service Providers (ISP) dulden.

Cablecom bemängelt, dass der Verweis in Artikel 26 VE-BÜPF auf Artikel 2 Absatz 1 VE-BÜPF nicht korrekt ist, da in Absatz 1 der Kreis eindeutig auf die berufsmässige Ausübung beschränkt ist. Richtigerweise muss sich der Verweis auf Artikel 2 Absatz 2 VE-BÜPF beziehen.

1.3. Artikel 3 Überwachungsdienst

[1] Der Bund betreibt einen Dienst für die Überwachung des Post- und Fernmeldeverkehrs (Dienst).

[2] Der Dienst erfüllt seine Aufgaben selbstständig. Er ist weisungsungebunden und dem EJPD nur administrativ zugeordnet.

[3] Er arbeitet im Rahmen seiner Aufgaben mit den im Post- und Fernmeldewesen zuständigen Konzessions- und Aufsichtsbehörden zusammen.

1.3.1 Artikel 3 Absatz 1

Keine Bemerkungen.

1.3.2 Artikel 3 Absatz 2

Die CVP beantragt, die Vermischung der normsetzenden und ausführenden Tätigkeiten des Dienstes zu beheben. ICT, ePower und SPICT empfinden es geradezu als befremdlich, dass ein und derselbe Dienst als Empfänger von Anordnungen der Strafverfolgungsbehörden agiert und gleichzeitig Vollzugsnormen setzt und zertifizieren kann. Sie beantragen deshalb eine Zweiteilung des Dienstes. Andere Teilnehmer[54] weisen darauf hin, dass aufgrund der Tatsache, dass der Dienst weisungsungebunden ist, dieser durchaus auch Funktionen in der Rechtsanwendung übernehmen kann.

1.3.3 Artikel 3 Absatz 3

ZH, LU, AG, KKPKS und CVP betonen die Bedeutung einer engen Zusammenarbeit zwischen dem Dienst und den Strafverfolgungsbehörden. Diese ist zwingend und daher als gesetzlicher Auftrag zu verankern. Rechtsetzung und Entwicklung der Technologien müssen kongruent verlaufen. Daher ist Absatz 3 mit „sowie den Strafverfolgungsbehörden“ zu ergänzen. In diesem Zusammenhang empfinden es auch ICT, ePower und SPICT für bemerkenswert, dass die Zusammenarbeit mit den Strafverfolgungsbehörden nicht in Absatz 3 erwähnt ist. Für Cablecom ist überdies nicht klar, weshalb der Dienst ausschließlich das Recht, nicht aber die Pflicht haben soll, bei eventuell auftauchenden technischen Fragen Auskunft zu geben. Als Kompetenzzentrum für Überwachungen muss er sein Wissen auch den Providern zugänglich machen. Ansonsten besteht die Gefahr, dass aufgrund einer Wissensdiskrepanz Missverständnisse entstünden. Cablecom schlägt deshalb folgenden neuen Absatz 4 vor: „Er ist der Ansprechpartner für Behörden und Verpflichtete in Bezug auf die Überwachungsmassnahmen und unterstützt bei Fragestellungen“.

[54] asut, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

1.4. Artikel 4 Bearbeitung von Personendaten

Die Behörden, die Überwachungen anordnen oder genehmigen, sowie die Personen, die Überwachungen nach diesem Gesetz durchführen, dürfen diejenigen Personendaten bearbeiten, die sie benötigen, um die Ausführung der Überwachungsanordnungen gewährleisten zu können.

Neun Teilnehmer[55] halten die Bestimmung über die Bearbeitung von Personendaten für unnötig. Dass die Strafverfolgungsbehörden sowie der Dienst und die Dienstleistungserbringer zum Zweck der Strafverfolgung Personendaten bearbeiten können, versteht sich von selbst.

Für ZG, BL, SP und privatim stellt Artikel 4 VE-BÜPF eine unzulässige Generalklausel dar, welche die Zweckbindung aufweicht. Im Rahmen der Überwachungen gemäss BÜPF werden potentiell auch besonders schützenswerte Personendaten bearbeitet. Gemäss Artikel 17 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG)[56] ist eine Unterscheidung in der Qualifikation der Daten in Bezug auf deren gesetzliche Grundlage notwendig. Diese Unterscheidung wird in Artikel 4 VE-BÜPF nicht berücksichtigt. Demgemäss müssen Datenbearbeitungen, welche besondere Personendaten oder Persönlichkeitsprofile betreffen, ausdrücklich im Gesetz geregelt sein. Eine Regelung muss umso bestimmter sein, desto heikler die Personendaten sind. Die Generalklausel entbindet folglich nicht davor, die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen auf eine separate ausdrückliche Gesetzesgrundlage abzustützen, die dem Gebot der Bestimmtheit genügt. Auch BS und VD fordern generell eine Präzisierung der Norm. NE beantragt überdies, den Erlass von Bestimmungen über die Vernichtung nutzloser bzw. irrtümlich erlangter Daten oder zumindest einen Hinweis auf das Datenschutzgesetz.

Neun Teilnehmer[57] weisen darauf hin, dass die Grundsätze von Artikel 4 DSG wie Verhältnismässigkeit, Treu und Glauben und Zweckbindung der Daten zu beachten sind. Ein Grossteil der erwähnten Teilnehmer[58] schlagen folgende Formulierung vor: „Die Behörden, die Überwachungen anordnen oder genehmigen, sowie die Personen, die Überwachungen nach diesem Gesetz durchführen, dürfen diejenigen Personendaten bearbeiten, die sie benötigen, um die Ausführung der *gerichtlich angeordneten und rechtmässigen* Überwachungsanordnungen gewährleisten zu können. *Die Grundsätze des Bundesgesetzes über den Datenschutz müssen dabei eingehalten werden.“*

kf sieht die Gefahr, dass unbescholtene Personen überwacht und deren Daten über Jahre aufbewahrt werden.

1.5. Artikel 5 Post- und Fernmeldegeheimnis

Die Überwachung und alle die Überwachung betreffenden Informationen unterliegen dem Post- und Fernmeldegeheimnis nach Artikel 321ter StGB.

Einige Teilnehmer[59] weisen darauf hin, dass das Fernmeldegeheimnis bereits in Artikel 43 des Fernmeldegesetzes vom 30. April 1997 (FMG)[60] verankert ist. Die Erwähnung im BÜPF ist deshalb verwirrend, da man annehmen könnte, dass auch Daten, welche unter dem Titel „Auskunft über Anschlüsse“ erteilt werden, unter das Fernmeldegeheimnis fallen. Zudem un-

---

55 LU, NW, GL, GR, TG, VS, JU, KKJPD, KSBS.
56 SR 235.1
57 SGB, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
58 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
59 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
60 SR 784.10

terliegt nicht in erster Linie die „Überwachung“ dem Fernmeldegeheimnis, wie es der Wortlaut der Bestimmung suggeriert, sondern generell jegliche Kommunikation über öffentliche Fernmeldenetze. Die Überwachung begründet somit nicht das Fernmeldegeheimnis, sie ist vielmehr ein Eingriff in dasselbe. Gemäss RD hat die Bestimmung generell zur Konsequenz, dass Informationen, die sonst nicht dem Fernmeldegeheimnis unterliegen, dies aufgrund der Bestimmung trotzdem tun.

2. Informatiksystem zur Verarbeitung der durch die Überwachung des Fernmeldeverkehrs gewonnenen Daten

2.1. Artikel 6 Grundsatz

Der Dienst betreibt ein Informatiksystem zur Verarbeitung der durch die Überwachung des Fernmeldeverkehrs gewonnenen Daten im Sinne von Artikel 1 Absatz 1 (Verarbeitungssystem).

SH lehnt die dauernde zentrale Aufbewahrung der Daten beim Dienst ab. Demgegenüber begrüssen ICT und ePower die zentrale Lagerung der Daten als eindeutigen Fortschritt, der mithelfen wird, die Kosten im Überwachungsprozess zu senken.

IT(19) beantragen eine Ergänzung der Bestimmung mit klaren Vorschriften über die nötigen Kontrollen aller Überwachungsdaten sowie mit klar strukturierten Definitionen der Aufgaben des zentralen Dienstes. Sofern die Einschleusung von Informatikprogrammen Teil des Informatiksystems ist, beantragt PPS die Bestimmung mit der Bearbeitung von überwachten Datensystemen zu erweitern. Falls dies nicht zutreffen sollte, braucht es dafür eine entsprechende eigene Definition und eine gesetzliche Grundlage.

DJS und gr.ch verlangen, dass das Verarbeitungssystem so eingerichtet wird, dass die Ausübung des Einsichts- und Auskunftsrechts gewährleistet ist. Die Ausführungen im erläuternden Bericht wecken diesbezüglich gewisse Bedenken.

CP ist der Ansicht, dass das Verarbeitungssystem wegen der grossen Gefahr von elektronischen Angriffen mit den höchsten Sicherheitsstandards ausgerüstet werden muss.

2.2. Artikel 7 Zweck des Verarbeitungssystems

[1] Das Verarbeitungssystem dient dazu:

a. die durch die Überwachung des Fernmeldeverkehrs gewonnenen Daten zentral aufzubewahren;

b. den Onlinezugriff auf diese Daten nach Artikel 9 zu ermöglichen.

Sechs Teilnehmer[61] unterstützen ein System der zentralen Bereitstellung der Daten. Die neue gesetzliche Regelung sollte allerdings nicht ausschliessen, dass Daten im Bedarfsfall auf zusätzliche Datenträger überspielt und den anordnenden Behörden zur Verfügung gestellt werden. Wie dies heutiger Praxis entspricht, wird diese Möglichkeit insbesondere für die Leistung internationaler Rechtshilfe weiterhin erforderlich sein, denn nur so wird die Weitergabe an die Gerichte möglich bleiben.

KSBS ist der Auffassung, dass auch künftig nicht der Dienst die Daten von normalen Telefonüberwachungen aufbewahren soll, sondern dass die Daten weiterhin auf Datenträgern bei den Strafakten liegen und deshalb der Zweck des Verarbeitungssystems angepasst werden

[61] ZH, GL, VS, JU, KKJPD, KKPKS.

muss.

ZG, BL und privatim sind der Ansicht, dass aus verfassungs- und datenschutzrechtlicher Sicht die zentrale Aufbewahrung ein Mittel und kein Zweck ist. ZG beantragt deshalb, Buchstabe a von Artikel 7 entsprechend zu korrigieren. Der Kanton BL beantragt, zu prüfen, ob die zentrale Aufbewahrung nicht durch einen weiteren Zweck gerechtfertigt werden muss und privatim schlägt folgende Formulierung vor: „Im Verarbeitungssystem werden die durch die Überwachung des Fernmeldeverkehrs gewonnenen Daten zentral aufbewahrt, um den Onlinezugriff auf diese Daten nach Artikel 9 VE-BÜPF zu ermöglichen.“.

Einige Teilnehmer[62] bemängeln, dass die vorgeschlagene Bestimmung nicht festhält, dass der Zweck des Verarbeitungssystems zunächst die Entgegennahme der Daten umfasst und unterbreiten einen entsprechenden Formulierungsantrag.

ISSS ist der Ansicht, dass ein zentrales System mit Bezug auf den Schutz der Grundrechte und der Privatsphäre, aber auch aufgrund der Missbrauchsgefahr, zwingend eine Kontrolle durch eine unabhängige Instanz erfordert, wie bspw. durch den Eidg. Datenschutzbeauftragten.

2.3. Artikel 8 Inhalt des Verarbeitungssystems

Das Verarbeitungssystem enthält:

a. den Fernmeldeverkehr der überwachten Person, einschliesslich des empfangenen Fernmeldeverkehrs;

b. die Daten, welche darüber Auskunft geben, wann und mit welchen Anschlüssen die überwachte Person über den Fernmeldeverkehr Verbindung hat oder gehabt hat, sowie die Verkehrs- und Rechnungsdaten.

Mehrere Teilnehmer[63] beantragen, dass Artikel 8 Buchstabe b ausdrücklich auch die geografische Informationen aufführt. KKPKS ist der Ansicht, dass auch der Versuch eines Verbindungsaufbaus entscheidend sein kann, und beantragt deshalb, dies gesetzlich festzuhalten. LU, SG, BL, NW und KSBS verlangen eine klarere Formulierung des Buchstabens b, namentlich eine gesetzliche Klarstellung des Unterschieds zwischen den so genannten Verbindungsdaten und den Verkehrs- und Rechnungsdaten. NW, SG und KSBS verlangen zudem eine entsprechende klarere Formulierung von Artikel 273 StPO sowie gemäss Ansicht von BL zusätzlich von Artikel 16 Buchstabe e VE-BÜPF.

Manche Teilnehmer[64] vertreten die Auffassung, dass Artikel 7 VE-BÜPF als Prinzip genügt und deshalb Artikel 8 VE-BÜPF als überflüssig gestrichen werden kann. Cablecom kritisiert, dass Buchstabe a unnötig bzw. missverständlich formuliert ist. So ist es unklar, weshalb der empfangene Fernmeldeverkehr ausdrücklich erwähnt wird, nicht aber der gesendete Verkehr. Die Aussage in Buchstabe b muss bezüglich des Internetverkehrs als unrealistisch betrachtet werden.

2.4. Artikel 9 Zugriff auf das Verarbeitungssystem

[1] Der Dienst gewährt den anordnenden Behörden und den von ihnen bezeichneten Personen im Rahmen der ihnen gewährten Bewilligung den Onlinezugriff auf die durch die entsprechende Überwachung gewonnenen Daten, die im Verarbeitungssystem enthalten sind.

---

62 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, Cablecom.
63 ZH, AG, TI, GL, TG, VS, JU, KKJPD, KKPKS.
64 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

[2] Die anordnende Behörde und die von ihr bezeichneten Personen nach Absatz 1 haben einen Onlinezugriff auf die durch die entsprechende Überwachung gewonnenen Daten, solange die anordnende Behörde mit dem Verfahren befasst ist, aber nicht länger als ein Jahr nach Beendigung der Überwachung. Die anordnende Behörde benachrichtigt den Dienst über die Abtretung des Verfahrens und das Ende der Überwachung; die Artikel 274 Absatz 5 und 275 StPO bleiben vorbehalten. Die anordnende Behörde kann, solange sie mit dem Verfahren befasst ist, den Dienst um Verlängerung des Zugriffs auf die Daten um jeweils höchstens ein Jahr ersuchen. Der Dienst benachrichtigt diese Behörde über den bevorstehenden Ablauf des Onlinezugriffs auf die Daten.

[3] Die anordnende Behörde, welche das Dossier abgetreten hat, teilt dem Dienst die gegebenenfalls neu mit dem Verfahren befasste Behörde mit.

[4] Der Dienst gewährt auf Ersuchen der neu mit dem Verfahren befassten Behörde sowie den von ihr bezeichneten Personen im Rahmen der ihnen gewährten Bewilligung den Onlinezugriff auf die durch die entsprechende Überwachung gewonnenen Daten, die im Verarbeitungssystem enthalten sind. Die neue Behörde und die von ihr bezeichneten Personen haben Zugriff auf diese Daten, solange die neue Behörde mit dem Verfahren befasst ist, aber nicht mehr als ein Jahr seit dem Ersuchen um Zugriff auf die Daten. Im Übrigen gelten die Absätze 2 und 3 sinngemäss.

[5] Falls infolge technischer Schwierigkeiten der Onlinezugriff auf die durch die entsprechende Überwachung gewonnenen Daten nicht möglich ist, können diese mittels Datenträgern und Dokumenten postalisch zugestellt werden.

Neun Teilnehmer[65] beantragen, in Absatz 5 ausdrücklich festzuhalten, dass die Umstände des Einzelfalls oder technische Schwierigkeiten eine postalische Zustellung mittels Datenträgern oder Dokumenten erfordern können. Um Missbrauch oder Erpressung vorzubeugen, sollen ferner die am Verfahren Beteiligten, insbesondere die Verteidigung, ausschliesslich über den Anschluss der zuständigen Staatsanwaltschaft oder Untersuchungsrichters Zugriff auf die Daten erhalten. Die Daten sollen vor dem Zugriff von Unberechtigten, bspw. mittels Datenverschlüsselung, geschützt werden. VD kann dem „Online-Zugriff" nur unter der Voraussetzung zustimmen, dass die Parteien und Gerichte den gleichen Zugriff erhalten wie nach dem heutigem System.

BE, NW, BL und SKG beantragen die Beibehaltung des alten Systems. Die vorgeschlagene Zugriffsregelung ist kompliziert, pannenanfällig und unnötig. Verfahren werden zuweilen abgetreten, vereinigt oder getrennt. Das neue System trägt diesen Verfahrensmöglichkeiten keine Rechnung. Die vorgeschlagene Zugriffsregelung steht teilweise auch in Widerspruch zu den Bestimmungen der StPO. So müssen die Parteien gemäss StPO Zugriff auf die Originalakten haben. Bei einem Zugriff der Parteien direkt auf das System des Dienstes bestehen zudem sicherheitstechnische Bedenken. Das neue System hat grosse Nachteile ohne nennenswerte Vorteile. LU, SZ, SO, SG, SH und KSBS beantragen ebenfalls, das alte System beizubehalten und allenfalls zu prüfen, ob es nicht Sinn machen würde, die zentrale Speicherung wegen der anfallenden, immensen Menge von Daten auf das Internet zu beschränken, Telefonüberwachungen aber, wie bisher, auf Datenträgern zu speichern und zu versenden. LU wirft die Frage auf, ob die Daten noch vorhanden sein werden, falls später im Rahmen einer Revision des Strafurteils auf diese Daten zurückgegriffen werden müsste. Dies wird gemäss erläuterndem Bericht nicht sichergestellt. ZG beantragt die Prüfung einer einfacheren Regelung. Für BS, SAV und MS verletzt das vorgeschlagene System die Parteirechte und es braucht einen Überwachungsmechanismus, damit sichergestellt wird, dass sich alle sachdienlichen Daten auch im Dossier befinden.

Die CVP macht im Bereich des Internets auf die Missbrauchsgefahr aufmerksam und fordert eine Sicherstellung, dass nur auf Daten zugegriffen werden kann, die bei der Überwachung gewonnen wurden.

Für manche Teilnehmer[66] erfolgt die erstmalige Erwähnung des Datenschutzgesetzes in Absatz 2 viel zu spät. Der Datenschutz muss im Zeitpunkt beginnen, an dem die Daten ge-

---

65 ZH, AG, GL, TG, VS, JU, KKJPD, KKPKS, CCC.

66 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

sammelt werden. In Absatz 1 wird überdies nicht gesagt wer die Bewilligung erteilt. Im ganzen Artikel fehlen Prozesse zur Sicherstellung des Datenschutzes.

2.5. Artikel 10 Akteneinsichtsrecht und Auskunftsrecht über die Daten

[1] Das Akteneinsichtsrecht und das Auskunftsrecht über die Daten der betroffenen Person, die im Rahmen eines Strafverfahrens (Art. 1 Abs. 1 Bst. a) gewonnen wurden, richten sich nach den Artikeln 95, 97, 98, 99 Absatz 1, 101 Absatz 1, 102 und 279 StPO.

[2] Das Akteneinsichtsrecht und das Auskunftsrecht über die Daten der betroffenen Person, welche im Rahmen des Vollzugs eines Rechtshilfeersuchens (Art. 1 Abs. 1 Bst. b) gewonnen wurden, richten sich nach der Spezialgesetzgebung in diesem Bereich sowie nach dem Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), wenn die für das Rechtshilfeersuchen zuständige Behörde eine Bundesbehörde ist, oder nach kantonalem Recht, wenn diese Behörde eine kantonale Staatsanwaltschaft ist.

[3] Das Akteneinsichtsrecht und das Auskunftsrecht über die Daten der betroffenen Person, welche im Rahmen der Suche nach vermissten Personen (Art. 1 Abs. 1 Bst. c) oder nach verurteilten Personen (Art. 1 Abs. 1 Bst. d) gewonnen wurden, richten sich nach kantonalem Recht. Artikel 29 bleibt vorbehalten.

[4] Die betroffene Person, über die durch eine entsprechende Überwachung Daten gewonnen wurden, kann ihre Rechte gegenüber der mit dem Verfahren befassten Behörde geltend machen. Falls keine Behörde mehr mit dem Verfahren befasst ist, kann sie diese gegenüber der letzten damit befassten Behörde oder der ihr nachfolgenden Behörde geltend machen. Die betroffene Person kann ihr Auskunftsrecht nicht gegenüber dem Dienst geltend machen.

Eine grössere Teilnehmerzahl[67] lehnt den Artikel 10 ab, da die StPO ausreichende Schutzbestimmungen für personenbezogene Daten enthält. Der Grundsatz in Absatz 1, wonach für das Akteneinsichts- und Auskunftsrecht die StPO gilt, ist eine Selbstverständlichkeit. Die in Absatz 1 aufgeführten Artikel der StPO sind aber für geheime Überwachungen gerade nicht einschlägig. BL stimmt dem zu und beantragt deshalb eine entsprechende Anpassung der Gesetzesbestimmung. Die Einführung einer eigenen schweizerischen Zuständigkeit für Ersuchen aus dem Ausland in Absatz 2 macht keinen Sinn. Für die Notsuche gemäss Absatz 3 könnte ohne weiteres Artikel 279 StPO als sinngemäss anwendbar erklärt werden. Der Verweis in Absatz 3 auf kantonales Recht macht keinen Sinn. Demgegenüber befürwortet SZ diesen Verweis. Absatz 4 ist unnötig.

FR ist der Meinung, dass die im Strafverfahren nicht beteiligten Dritte ebenfalls ein Einsichtsrecht zu Daten haben müssen, die sie betreffen.

PPS bemängelt, dass Absatz 4 zu einem Recht ohne Adressaten wird, wenn die Überwachung verdeckt durchgeführt und eine Mitteilung entsprechend Artikel 279 Absatz 2 StPO unterlassen wird.

2.6. Artikel 11 Aufbewahrungsfrist von Daten

[1] Die im Rahmen eines Strafverfahrens (Art. 1 Abs. 1 Bst. a) gewonnenen Daten sind im Verarbeitungssystem bis zum Ablauf der Strafverfolgungsverjährung aufzubewahren. Die mit dem Verfahren befasste Behörde teilt dem Dienst diese Frist mit.

[2] Die im Rahmen des Vollzugs eines Rechtshilfeersuchens (Art. 1 Abs. 1 Bst. b) gewonnenen Daten sind im Verarbeitungssystem solange aufzubewahren, wie es für das verfolgte Ziel erforderlich ist, aber nicht mehr als 30 Jahre.

[3] Die im Rahmen der Suche nach vermissten Personen (Art. 1 Abs. 1 Bst. c) gewonnenen Daten sind im Verarbeitungssystem solange aufzubewahren, wie es für das verfolgte Ziel erforderlich ist, aber nicht mehr als 30 Jahre.

[4] Die im Rahmen der Suche nach Personen, die zu einer Freiheitsstrafe verurteilt worden sind (Art. 1 Abs. 1 Bst. d), gewonnenen Daten sind im Verarbeitungssystem solange aufzubewahren, wie es für das verfolgte Ziel erforderlich ist, aber nicht länger als bis zum Ablauf der Strafvollstreckungsverjährung. Die mit dem Verfahren befasste Behörde teilt dem Dienst diese Frist mit. Die im Rahmen der Suche nach Personen, gegenüber denen eine

[67] LU, NW, BL, SG, GL, TG, VS, JU, KKJPD, KSBS, SKG.

freiheitsentziehende Massnahme angeordnet worden ist (Art. 1 Abs. 1 Bst. d), gewonnenen Daten sind im Verarbeitungssystem solange aufzubewahren, wie es für das verfolgte Ziel erforderlich ist, aber nicht mehr als 30 Jahre.

[5] Der Bund und jeder Kanton bezeichnen eine Behörde, welcher der Dienst den bevorstehenden Ablauf der Aufbewahrungsfrist der betroffenen Daten mitteilt. Diese Behörde leitet die Mitteilung an die mit dem Verfahren befasste Behörde weiter oder, falls keine Behörde mehr mit dem Verfahren befasst ist, an die letzte damit befasste Behörde oder der ihr nachfolgenden Behörde. Bei Ablauf der Aufbewahrungsfrist der betroffenen Daten im Verarbeitungssystem kann die Behörde, welche diese Mitteilung erhalten hat, den Dienst ersuchen, ihr die Daten zu übertragen. Nach erfolgter Übertragung oder wenn kein solches Ersuchen gestellt wurde, vernichtet der Dienst die betroffenen Daten im Verarbeitungssystem.

Verschiedene Teilnehmer[68] lehnen den Artikel 11 VE-BÜPF ab und verweisen darauf, dass mit der geforderten Beibehaltung des bisherigen Systems die umständliche Regelung der Verjährungs- und Aufbewahrungsfristen obsolet wäre. Das heutige System, bei dem das Schicksal der Daten das gleiche ist wie für alle anderen Akten im betreffenden Dossier, wird einer Sonderregelung vorgezogen. Die Bestimmung ist nur nötig, weil die Daten beim Dienst und nicht bei den Strafakten aufbewahrt werden, was aber nicht sinnvoll ist. Das Anknüpfen der Aufbewahrungsfristen der Daten an die Strafverfolgungsverjährung ist unklar und verursacht einen unnötigen Administrativaufwand. Die vorgeschlagene Meldeorganisation ist zu kompliziert, das ganze Verfahren zu komplex und aufwändig. Die Aufbewahrungsfristen sollten sich nach der StPO richten, da unterschiedliche Regelungen nicht sinnvoll sind. Will man das vorgeschlagene System beibehalten, vertritt KSBS die Auffassung, dass eine Bestimmung genügt, wonach die Behörde, welche über die Akten verfügt, nach Ablauf der Aufbewahrungsfrist sicherstellt, dass die beim Dienst gespeicherten Daten gelöscht werden. AG beantragt die Festsetzung einer einheitlichen Aufbewahrungsfrist (bspw. 10 oder 15 Jahre).

ZG beantragt, Absatz 1 so zu präzisieren, dass klar wird, welche Behörde dem Dienst die Frist der Strafverfolgungsverjährung mitteilt.

CVP, GPS, DJS und gr.ch kritisieren die in Artikel 11 vorgesehenen überlangen Aufbewahrungsfristen. Die CVP beantragt deshalb eine Reduzierung der Aufbewahrungsfrist. GPS, DJS und gr.ch fordern, die Daten spätestens nach Abschluss des Strafverfahrens auszugliedern und sie nur noch für die Einsicht der Betroffenen aufzubewahren. Da das Verfahren abgeschlossen ist, steht auch der vollständigen Einsicht der Betroffenen nichts im Wege. Den Betroffenen sollten deshalb automatisch sämtliche Aufzeichnungen in einem handelsüblichen Format ausgehändigt werden.

PPS beantragt, dass mit dem Auslaufen der in Absatz 1 vorgesehenen Aufbewahrungsfrist die Daten gelöscht werden. Für die Fristen sollen ferner nicht, wie vorgeschlagen, die verfolgten Ziele entscheidend sein, sondern die Verjährung.

IT(19), ISSS, SWICO, hp und COG beantragen, den Artikel 11 mit Regeln zu ergänzen, die bestimmen, welche Instanz über die tatsächliche Dauer der Aufbewahrung der Daten im Einzelfall entscheidet. Ferner sind die Voraussetzungen und Pflichten sowie das Vorgehen für die unverzügliche Vernichtung der für die Zwecke der Überwachung nicht mehr benötigten Daten zu regeln, sowie eine Kontrolle der tatsächlichen Löschung vorzusehen.

Acht Teilnehmer[69] beantragen, Absatz 5 wie folgt zu ergänzen: "...im Verarbeitungssystem und aus sämtlichen Sicherungsmedien...".

---

[68] BE, SZ, NW, BL, SH, SG, AG, VD, KSBS.

[69] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

2.7. Artikel 12 Sicherheit

Der Dienst ist für die Sicherheit des Verarbeitungssystems verantwortlich. Der Bundesrat erlässt Vorschriften über technische und organisatorische Schutzmassnahmen, insbesondere gegen den Zugang, die Änderung, die unbefugte Verbreitung und die ungewollte oder unbefugte Vernichtung der Daten. Personen, die Überwachungen nach diesem Gesetz durchführen, müssen bei der Übertragung der Daten aus der Überwachung den entsprechenden Anweisungen des Dienstes für die Datensicherheit folgen.

IT(19) beantragen eine Ergänzung von Artikel 12 mit klaren Vorschriften über die nötigen Kontrollen aller Überwachungsdaten sowie mit klar strukturierten Definitionen der Aufgaben des Dienstes.

SWICO, hp und COG stellen die Frage, welche Pflichten und Auflagen sowie damit verbundenen Kosten die vom Bundesrat zu erlassene Verordnung über die technischen und organisatorischen Schutzmassnahmen für die in Artikel 12 ebenfalls erwähnten Fernmeldedienstanbieterinnen und ISP nach sich ziehen wird und stellen den Antrag, dass diese Pflichten kostenneutral bleiben müssen.

PPS beantragt, dass nicht nur der Dienst und die die Überwachung durchführenden Personen den Vorschriften über die technischen und organisatorischen Schutzmassnahmen unterstellt werden, sondern auch die das Verarbeitungssystem nutzenden Behörden und die von ihnen bestimmten Dienststellen.

2.8. Artikel 13 Verantwortung

Die Behörden, welche Zugriff zum Verarbeitungssystem haben (Art. 9), sind die Inhaber der Datensammlung bezüglich derjenigen Daten, die im Rahmen von Überwachungen, die in ihre Kompetenz fallen, gewonnen wurden.

Einige Teilnehmer[70] unterbreiten folgenden Abänderungsantrag: "Die *anordnenden* Behörden, welche Zugriff zum Verarbeitungssystem haben (Art. 9), sind *verantwortlich für die gesetzmässige Verwendung* der Datensammlung bezüglich derjenigen Daten, die im Rahmen von Überwachungen, die in ihre Kompetenz fallen, gewonnen wurden". Cablecom beantragt seinerseits folgende Präzisierung: "*Die anordnenden Behörden* sind die Inhaber der Datensammlung bezüglich derjenigen Daten, die im Rahmen von Überwachungen, die in ihre Kompetenz fallen, gewonnen wurden".

3. Aufgaben des Dienstes

3.1. Artikel 14 Auskünfte über Fernmeldeanschlüsse

Der Dienst erteilt auf Gesuch hin ausschliesslich den folgenden Behörden zu den folgenden Zwecken Auskünfte über die Daten nach Artikel 20 Absätze 1-3:

a. den eidgenössischen und kantonalen Behörden, welche eine Überwachung des Fernmeldeverkehrs anordnen oder genehmigen dürfen: zur Bestimmung der zu überwachenden Anschlüsse und Personen;

b. dem Bundesamt für Polizei und den Polizeikommandos der Kantone und Gemeinden: für die Erfüllung von Polizeiaufgaben;

c. den zuständigen Behörden des Bundes und der Kantone: zur Erledigung von Verwaltungsstrafsachen.

safe weist darauf hin, dass nach Artikel 14 Absatz 2 in Verbindung mit Absatz 4 geltendes BÜPF das vereinfachte Verfahren zur Offenlegung der Identität eines Anschlussinhabers anwendbar ist. Diese Bestimmung soll laut dem erläuternden Bericht im Wesentlichen in Ar-

[70] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

tikel 14 i.V.m. Artikel 20 Absatz 3 VE-BÜPF übernommen werden. Das vereinfachte Verfahren steht nach Artikel 14 Absatz 2 Buchstabe b und c geltendes BÜPF den zuständigen Polizei-/Verwaltungsbehörden für Polizeiaufgaben und Verwaltungsstrafverfahren offen – im Übrigen nach Buchstabe a aber nur den „*eidgenössischen und kantonalen Behörden, welche eine Überwachung des Fernmeldeverkehrs anordnen oder genehmigen dürfen*“ (Art. 6 geltendes BÜPF; Strafverfolgungsbehörden), und nur „*zur Bestimmung der zu überwachenden Anschlüssen und Personen*“. Damit ist gemäss safe der Verwendungszweck dieser Angaben auf Überwachungsfälle bezüglich der Straftaten von Artikel 269 Absatz 2 Buchstabe a StPO beschränkt. Das kann aber nicht die Absicht des Gesetzgebers gewesen sein. Vielmehr muss dieses Verfahren allen Strafverfolgungsbehörden für die Verfolgung, vor allem für die Beweissicherung, im Internet begangener Straftaten generell zur Verfügung stehen. Ausserdem ist die Offenlegung vielfach auch eine Voraussetzung für eine wirksame Kriminalprävention. safe beantragt deshalb, Artikel 14 Buchstabe a VE-BÜPF wie folgt abzuändern: „a. den eidgenössischen und kantonalen *Strafverfolgungsbehörden: zu Zwecken der Strafverfolgung und Kriminalprävention*“.

3.2. Artikel 15 Allgemeine Aufgaben der Überwachung

Bei einer Überwachung des Post- und Fernmeldeverkehrs hat der Dienst folgende Aufgaben:

a. *Er prüft, ob die Überwachung eine gemäss dem anwendbaren Recht überwachungsfähige Straftat betrifft und von der zuständigen Behörde angeordnet wurde. Bei klar unrichtigen oder unbegründeten Anordnungen nimmt er mit der Genehmigungsbehörde Kontakt auf, bevor Sendungen oder Informationen an die anordnende Behörde weitergeleitet werden.*

b. *Er weist die Personen, die Überwachungen nach diesem Gesetz durchführen, an, wie diese durchzuführen sind, fordert sie auf, die für die Überwachung notwendigen Massnahmen zu treffen, und kontrolliert die Ausführung.*

c. *Er setzt die von den Genehmigungsbehörden angeordneten Vorkehren zum Schutz von Berufsgeheimnissen um.*

d. *Er führt eine Kontrolle über die bewilligte Dauer der Überwachung und stellt diese bei Ablauf ein, wenn kein Verlängerungsgesuch gestellt ist.*

e. *Er teilt der Genehmigungsbehörde unverzüglich die Einstellung der Überwachung mit.*

Einige Teilnehmer[71] beantragen, Artikel 15 VE-BÜPF mit folgendem Buchstabe f zu ergänzen: „Er berät Behörden und Anbieterinnen von Fernmeldediensten in technischen Fragen im Zusammenhang mit Überwachungen des Fernmeldeverkehrs.“.

PPS bemängelt, dass die allgemeine Aufgabe des Dienstes hinsichtlich Erstellung und Wartung eines Infiltrationssystems fehle (vgl. hinten III. Ziff. 11.1.2 zu Art. 270bis StPO).

3.2.1 Buchstabe a

Die FDP beantragt, die Rolle des Dienstes generell klarer zu regeln, insbesondere was dessen Kompetenzen gegenüber den Strafverfolgungsbehörden betrifft.

Etliche Teilnehmer[72] stellen fest, dass die Kompetenz des Dienstes, die Zulässigkeit angeordneter Überwachungen zu überprüfen, fehlt. In der Praxis leitet der Dienst lediglich die Anordnungen weiter, selbst wenn die Anordnungen klar unrichtig sind. Es kommt hinzu, dass die überwachungspflichtigen Personen keine Rechtsmittel haben, um das Fehlen einer gesetzlichen Grundlage für die entsprechende Überwachungsmassnahme zu rügen (vgl. entsprechende Anträge in III. Ziff. 9.2 zu Art. 34 VE-BÜPF: Rechtsschutz). Das Bundesverwal-

---

71 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.

72 Swisscable, SWICO, SKS, Cablecom, asut, Orange, Swisscom, Colt, Sunrise, Verizon, KSBS, economiesuisse, GPS, SKS, IT(19).

tungsgericht als Beschwerdeinstanz kann zudem nur Sachverhalte prüfen, welche der Dienst bereits als Vorinstanz geprüft hat und diese Voraussetzung fehlt. Es wird daher folgender Formulierungsantrag gestellt: „a. Er prüft, ob die Überwachung von einer zuständigen Behörde angeordnet wurde, ob die Art der angeordneten Überwachungsmassnahme gesetzlich vorgesehen ist und ob die Art der angeordneten Überwachungsmassnahme in technischer und organisatorischer Hinsicht durchgeführt werden kann. Er prüft nicht, ob die Anordnung einer Überwachung im konkreten Einzelfall die Voraussetzungen gemäss Artikel 269 lit. b. und c. der Strafprozessordnung erfüllt und ob die Anordnung angemessen ist.“. BL weist darauf hin, dass wenn die technische und organisatorische Machbarkeit gemäss Artikel 34 Absatz 2 VE-BÜPF ein Beschwerdegrund darstellt, sie folgerichtig vorher geprüft werden muss. Artikel 15 Buchstabe a VE-BÜPF ist entsprechend zu ergänzen (vgl. die Ausführungen in III. Ziff. 9.2.2 zu Art. 34 Abs. 2 VE-BÜPF).

Einige Teilnehmer[73] beantragen zudem, den Buchstaben a um folgenden Satz zu erweitern: „Bei Unklarheiten über das Bestehen einer Pflicht zur Durchführung einer Überwachung entscheidet er mittels Verfügung unter Anwendung der massgebenden gesetzlichen Bestimmungen“. Generell werfen sie die Frage auf, ob der Dienst gegenüber den Fernmeldedienstanbieterinnen überhaupt verfügen kann, denn der Begriff der Verfügung setzt voraus, dass derjenige, welcher verfügt, auch rechtlich prüft und begründet, was er verfügt. Cablecom weist zudem auf den Widerspruch zu Artikel 33 VE-BÜPF hin, welcher festhält, dass der Dienst über die Einhaltung der Gesetzgebung wacht.

3.2.2 Buchstabe b

Mehrere Fernmeldedienstanbieterinnen[74] schlagen folgende Ergänzung des Buchstabens b vor: „Er weist die Personen, die Überwachungen nach diesem Gesetz durchführen, *im Rahmen der massgebenden gesetzlichen Grundlagen* an, wie diese durchzuführen sind, fordert sie auf, die für die Überwachung notwendigen Massnahmen zu treffen, und kontrolliert die Ausführung“.

3.2.3 Buchstaben c – e

Keine Bemerkungen.

3.3. Artikel 16 Aufgaben bei der Überwachung des Fernmeldeverkehrs

Bei einer Überwachung des Fernmeldeverkehrs hat der Dienst zusätzlich folgende Aufgaben:

a. *Wenn der Dienst der Meinung ist, dass die angeordnete Überwachung technisch nicht ausgeführt werden kann oder dass deren Ausführung mit erheblichen Schwierigkeiten verbunden ist, so nimmt er unverzüglich mit der anordnenden Behörde und mit der Genehmigungsbehörde Kontakt auf.*

b. *Sind an der zu überwachenden Fernmeldedienstleistung mehrere Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, beteiligt, so erteilt der Dienst derjenigen Person den Überwachungsauftrag, die für die Verwaltung der Nummer zuständig ist oder die Überwachung mit dem geringsten technischen Aufwand vollziehen kann.*

c. *Er nimmt von den Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, den umgeleiteten Fernmeldeverkehr der überwachten Person entgegen, zeichnet diesen auf und ermöglicht der anordnenden Behörde seine Kenntnisnahme.*

d. *Er weist die Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, an, den Fernmeldeverkehr der überwachten Person direkt der von der anordnenden Behörde bezeichneten Polizeistelle zuzuleiten, wenn er aus technischen Gründen nicht in der Lage ist, den Fernmeldeverkehr entgegenzunehmen, aufzuzeichnen oder der anordnenden Behörde auszuliefern.*

---

[73] asut, Orange, Swisscom, Colt, Sunrise, Verizon.

[74] asut, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

e. Er nimmt von den Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, die Daten entgegen, welche darüber Auskunft geben, wann und mit welchen Anschlüssen die überwachte Person über den Fernmeldeverkehr Verbindung hat oder gehabt hat, sowie die Verkehrs- und Rechnungsdaten, zeichnet diese auf und ermöglicht der anordnenden Behörde die Kenntnisnahme.

f. Auf Ersuchen der anordnenden Behörde weist er die Personen, welche die Überwachung des Fernmeldeverkehrs nach diesem Gesetz durchführen, an, nur bestimmte Daten aus dem Datenstrom zu liefern.

3.3.1 Buchstabe a

KSBS begrüsst explizit den pragmatischen Mechanismus. Für ZH und KKPKS stellt die Formulierung in Buchstabe a nicht sicher, dass der Dienst die Machbarkeit der Überwachung eingehend prüft. Daher schlagen sie folgende Formulierung vor: „Wenn der Dienst nach eingehender Prüfung zum Schluss kommt...".

Mehrere Teilnehmer[75] sind der Meinung, dass mit der richtigen Formulierung von Artikel 15 Buchstabe a (vgl. oben III. Ziff. 3.2.1 zu Art. 15 Bst. a VE-BÜPF) der Buchstabe a von Artikel 16 VE-BÜPF obsolet wird.

Cablecom stellt sich die Frage, woher der Dienst das vertiefte Wissen aller möglichen Technologien herholen soll, um fachlich korrekt zu beurteilen, dass eine Überwachung mit erheblichen Schwierigkeiten verbunden ist. Sie schlägt deshalb vor, in speziellen Fällen sämtliche Beteiligten an einen Tisch zu holen, um die Möglichkeiten und Auswirkungen zu diskutieren.

3.3.2 Buchstabe b

Gemäss privatim lässt sich die Formulierung „Verwaltung der Nummer" nicht auf den Internetverkehr übertragen und schlägt stattdessen die Formulierung „Verwaltung des Anschlusses" vor.

Sechs Teilnehmer[76] beantragen mit einem konkreten Formulierungsvorschlag, den Überwachungsauftrag jeweils der Anbieterin des zu überwachenden Teilnehmers zu erteilen.

Cablecom weist darauf hin, dass gemäss dieser Bestimmung ein Provider dazu verpflichtet werden kann, die Aufgaben eines anderen Verpflichteten zu übernehmen, wenn der Dienst der Meinung ist, der Erstgenannte könne diese Pflichten besser übernehmen. Unklar ist dabei, aufgrund welcher Kriterien der Dienst dies entscheidet. Angesichts der Tatsache, dass die Überwachungen nicht vergütet werden sollen, wird ein wirtschaftliches Ungleichgewicht geschaffen, indem die grossen Provider mit grosser Wahrscheinlichkeit Aufträge für die kleinen Provider ausführen müssen, da sie technisch eher in der Lage sein werden, Überwachungen durchzuführen. Cablecom schlägt deshalb vor, den Überwachungsauftrag derjenigen Person zu erteilen, welche gegenüber dem zu überwachenden Fernmeldedienstteilnehmer die Leistungserbringerin ist.

3.3.3 Buchstabe c

Keine Bemerkungen.

---

75 asut, Orange, Swisscom, Colt, Sunrise, Finecom.

76 asut, Finecom, Orange, Swisscom, Colt, Sunrise.

3.3.4 Buchstabe d

Die Bestimmung wird von einigen Teilnehmern[77] explizit begrüsst. Demgegenüber sprechen sich Teilnehmer aus der Fernmeldedienstbranche[78] für eine Streichung von Buchstabe d aus, weil der Überwachungsdienst jederzeit in der Lage sein muss, den Fernmeldeverkehr entgegenzunehmen, da ja im Gegenzug auch für Fernmeldedienstanbieterinnen eine verbindliche Pflicht zur Erfüllung ihrer Aufgaben besteht. Gemäss SAV muss die Direktschaltung die absolute Ausnahme bleiben.

3.3.5 Buchstabe e

Mehrere Teilnehmer[79] sind der Meinung, dass Verbindungsdaten auch künftig nicht über das Überwachungssystem ISS[80] laufen sollen. Die bisherige Lösung der direkten Zustellung von Fernmeldedienstanbieterinnen an die auswertende Behörde stellt lediglich insofern eine Schwierigkeit dar, als je nach Fernmeldedienstanbieterin nicht ein einheitliches Format geliefert wird. Das Problem lässt sich jedoch problemlos durch technische Richtlinien lösen. Auch BL spricht sich für die Vorgabe eines einheitlichen Formates für die Datenlieferung aus und verlangt überdies eine gesetzliche Klarstellung, worin der Unterschied – falls ein solcher überhaupt existiert – zwischen den so genannten „Verbindungsdaten" einerseits, und den „Verkehrs- und Rechnungsdaten" andererseits besteht.

3.3.6 Buchstabe f

Mehrere Teilnehmer aus der Fernmeldedienstbranche[81] sind der Meinung, dass das Ausscheiden bestimmter Daten aus einem Datenstrom ausschliesslich Sache der anordnenden Behörde oder des Dienstes sein muss und beantragen daher die Streichung der Bestimmung (vgl. auch III. Ziff. 5.2.3 zu Art. 21 Abs. 3 VE-BÜPF). Cablecom beantragt ebenfalls die Streichung der Bestimmung und weist zudem darauf hin, dass bei einer Filterung seitens der Fernmeldedienstanbieterinnen die Gefahr einer Überwachungslücke entsteht. Dabei können wichtige Daten unwiderruflich verloren gehen. Die Filterung soll von den Untersuchungsbehörden, die den Fall kennen, vorgenommen werden.

3.4. Artikel 17 Qualitätskontrolle

[1] Der Dienst ergreift präventive oder nachträgliche Massnahmen zur Qualitätskontrolle der Daten, welche von den Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, geliefert werden.

[2] Sofern der Dienst zu diesem Zweck vom Inhalt der Daten Kenntnis nehmen muss, darf die Qualitätskontrolle nur mit vorgängigem Einverständnis der anordnenden Behörde durchgeführt werden.

VSPB hält die Bestimmung für sehr wichtig. Die Qualitätskontrolle muss gesichert werden und hat regelmässig zu erfolgen. Er beantragt deshalb, dass bei Nichterfüllung der verlangten Standards klare Konsequenzen, wie bspw. Konzessionsentzug, gezogen werden. KFG vermag demgegenüber den Zweck der Bestimmung nicht zu erkennen. Eine Qualitätskontrolle macht nur im Zusammenhang mit der Prüfung der Vollständigkeit Sinn. Daher soll die Bestimmung präzisiert oder gestrichen werden.

---

77 AG, GL, GR, TG, JU, KSBS, KKJPD.
78 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Cablecom.
79 NW, AG, GL, GR, TG, JU, KKJPD.
80 Interception System Schweiz.
81 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.

3.5. Artikel 18 (i.V.m. Art. 24) Zertifizierung

Art. 18:

Der Dienst bescheinigt den Anbieterinnen von Fernmeldediensten auf deren Kosten, dass sie Überwachungen wirksam durchzuführen imstande sind. Er regelt die Modalitäten der Zertifizierung.

Art. 24:

Anbieterinnen von Fernmeldediensten ohne Zertifikat müssen die Kosten tragen, die entstehen, wenn der Dienst oder Dritte zur Ausführung einer angeordneten Überwachung beigezogen werden müssen. Tritt dieser Fall ein, müssen sie sich anschliessend so schnell wie möglich gemäss Artikel 18 zertifizieren lassen.

Etliche Teilnehmer[82] halten eine Zertifizierung grundsätzlich für sinnvoll. Sie beantragen jedoch eine Zertifizierungspflicht vorzusehen, wonach neue Dienstleistungen nur dann angeboten werden dürfen, wenn deren Überwachung sichergestellt ist.

VD ist der Meinung, dass das Ziel der Zertifizierung unklar ist und sich die Frage stellt, ob es nicht sinnvoll wäre, zu präzisieren, dass der Wert eines Beweismittels nicht mit der Zertifizierung zusammenhängt.

ZH und KKPKS schlagen mit Verweis auf die Bundesrepublik Deutschland eine Zertifizierung der Hersteller von Telekommunikationsgeräten vor. Einerseits ist die Zertifizierung der Fernmeldedienstanbieterinnen sehr aufwändig, andererseits ist es im Rahmen der europäischen Zusammenarbeit einfacher, ein bereits bestehendes Zertifikat zu übernehmen. Die Zertifizierung der Hersteller bedeutet gemäss KKPKS für die Anbieter mehr Rechtssicherheit sowie Innovationsschutz.

Mehrere Teilnehmer aus der Fernmeldedienstbranche[83] betonen, dass eine Zertifizierung solange keinen Sinn macht, als die Pflichten der Fernmeldedienstanbieterinnen nur ungenügend umschrieben sind und diese aufgrund des Fehlens eines wirksamen Rechtsmittels gegen neuartige Überwachungsmethoden ins Uferlose gehen. Der Erhalt eines Zertifikats ist unter diesen Voraussetzungen nichts weiter als eine Momentaufnahme und für die Zukunft völlig wertlos. Sie schlagen deshalb folgende Neuformulierung von Artikel 18 VE-BÜPF vor: „Der Dienst bescheinigt den Anbieterinnen von Fernmeldediensten, dass sie *die im Rahmen dieses Gesetzes vorgesehenen* Überwachungen *grundsätzlich* durchzuführen imstande sind. *Insbesondere bescheinigt er den verpflichteten Anbieterinnen von Fernmeldediensten, dass sie über die nötigen Schnittstellen verfügen, welche mit dem Verarbeitungssystem des Bundes kompatibel sind.* Er regelt die Modalitäten der Zertifizierung.“ Mit Blick auf die Verhältnismässigkeit schlägt Verizon überdies vor, dass Fernmeldedienstanbieterinnen die Möglichkeit haben, im Einzelfall Dritte herbeizuziehen, ohne dass dies eine unmittelbare Zertifizierungspflicht nach sich zieht. Eine Kostenübernahme durch die Verpflichteten wird von den genannten Teilnehmern abgelehnt. HR beantragt ebenfalls die Streichung der Kostenübernahme einer Zertifizierung durch die Verpflichteten und verweist zudem auf die industriepolitische Bedeutung der Regelungen: Der Internet-Bereich war in der Schweiz in den letzten Jahren die Quelle für eine lebhafte Start-Up Szene, die viele zukunftsfähige Arbeitsplätze geschaffen hat. Auch hat die Schweiz diverse namhafte Ansiedelungen erlebt, wie z.B. Google in Zürich. Insbesondere schwierig kalkulierbare Kosten und aufwändige Zertifizierungen sind erhebliche Markteintrittsbarrieren, die insbesondere die Erfolgschancen für Start-Up Unternehmen senken und internationale Ansiedelungen unattraktiv machen. Auch CCC, INT und PPS erachten die Kostenübernahme für eine Zertifizierung als unverhältnismässige Belastung für die Internetdienstleister. Cablecom verweist schliesslich darauf, dass bei jeder anderen Geschäftsbeziehung, die Kosten für die Integrationstests von technischen Schnitt-

---

82 LU, NW, BL, SG, AG, GL, GR, TG, JU, KKJPD, KSBS, VSPB, CP.

83 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.

stellen durch den Auftraggeber getragen werden, bzw. jeder die Kosten trägt, die auf seiner Seite entstehen. Es ist deshalb nicht nachvollziehbar, dass der Dienst Hilfspersonen für Zertifizierungen beschäftigt und sich diese auch noch von den Fernmeldedienstanbieterinnen bezahlen lässt. Aus diesen Gründen lehnt Cablecom die volle Kostenübernahme der Zertifizierung durch die Fernmeldedienstanbieterinnen ab und beantragt Streichung der Artikel 18 und 24 VE-BÜPF. Gemäss SIUG wird ein gesamter Wirtschaftszweig zusätzlich gezwungen, sich für die Strafuntersuchung fit zu machen und diese selbstständig für den Staat auszuführen. Wer sich nicht zertifzieren lässt, wird im Falle einer angeordneten Überwachung für unvorhergesehene Kosten aufkommen müssen. Dies kann für viele Betriebe zu einem finanziell schwer zu verkraftenden Schaden führen. Die Anbieterinnen, welche die Zertifizierung durchlaufen, müssen möglicherweise gar nie eine angeordnete Überwachung ausführen. In diesem Fall werden die Kosten und der Aufwand einem fehlenden Nutzen für die Strafverfolgung gegenüberstehen. SIUG beantragt deshalb ebenfalls die Streichung der Artikel 18 und 24 VE-BÜPF.

IT(19), SWICO, hp und COG beantragen, den Gegenstand und das Verfahren der Zertifizierung zu präzisieren und genauer zu umschreiben. Ferner soll Artikel 18 VE-BÜPF mittels einer Aufzählung klarstellen, wer sich zertifizieren lassen muss. Gemäss SWICO, hp und COG sind die Kosten einer Zertifizierung zudem vom Dienst zu übernehmen.

DJS und gr.ch sprechen sich für eine Streichung der Artikel 18 und 24 VE-BÜPF aus, da sonst im Ergebnis die Freiheit, moderne Formen der Kommunikation anbieten zu können, einem staatlichen Bewilligungs- und Kontrollsystem weicht.

Auch switch und switchplus sprechen sich gegen einen faktischen Zertifizierungszwang aus. Es soll klar festgehalten werden, dass die dem BÜPF unterstellten Personen einen „Compliance-Test“ zu bestehen haben und damit von der Zertifizierung befreit sind. Andernfalls sind die Anforderungen an die Zertifizierung mit denjenigen in den Richtlinien betreffend das „Acceptance Testing“ in Einklang zu bringen, damit der Aufwand nicht doppelt betrieben werden muss.

ISSS verweist darauf, dass der Gegenstand und die Verfahren der Zertifizierung sehr unbestimmt formuliert sind und sich die grundsätzliche Frage stellt, ob sich die Eignung einer Dienstanbieterin zur gesetzeskonformen Durchführung der Überwachung überhaupt in einem Zertifizierungsverfahren feststellen lässt. Zudem ist es unklar, ob sich ISP und die in Artikel 2 Absatz 1 Buchstabe b VE-BÜPF genannten Personen zertifizieren lassen müssen.

4. Pflichten bei der Überwachung des Postverkehrs

4.1. Artikel 19

[1] Personen, die Überwachungen des Postverkehrs nach diesem Gesetz durchführen, müssen der anordnenden Behörde Postsendungen und die Angaben, wann und mit welchen Personen die überwachte Person über den Postverkehr Verbindungen hat oder gehabt hat, sowie die Rechnungsdaten, soweit herausgeben, wie es in der Überwachungsanordnung festgelegt ist. Sie erteilen der anordnenden Behörde auf Verlangen weitere Auskunft über den Postverkehr einer Person.

[2] Sie müssen Daten nach Absatz 1 während zwölf Monaten aufbewahren.

4.1.1 Absatz 1

Gemäss mehreren Teilnehmern[84] stellt die Bestimmung nicht klar, dass bei der Überwachung des Postverkehrs nicht nur sichergestellt werden muss, dass die Anbieter die Postsendungen herausgeben, sondern auch, dass sie diese nach der Kontrolle durch die Polizei auch wieder ohne Verzug entgegennehmen und zustellen. Sie verlangen eine diesbezügliche Klarstellung im Gesetz.

Die Schweizerische Post betont, dass der Sendungsverkehr nicht lückenlos erfasst wird, weshalb auch nicht zu sämtlichen Einzelsendungen nachträgliche Auskünfte über den Inhalt oder die Randdaten der Sendungen erteilt werden können. Insbesondere die über einen Briefeinwurf am Strassenrand oder an einer Poststelle aufgegebenen sowie alle übrigen uneingeschriebenen (Brief-) Sendungen werden von keinem der Verarbeitungs- und Transportsysteme der Schweizerischen Post registriert, weshalb auch keinerlei Randdaten verfügbar sind, die nachträglich angefragt und mitgeteilt werden könnten. Gegenteiliges gilt für alle eingeschriebenen Briefe und Pakete und weitere Sendungen, die über das „Track & Trace System“ der Schweizerischen Post abrufbar sind. Zu ihnen können nachträgliche Auskünfte im bisher praktizierten Umfang erteilt werden. Sie hält fest, dass die Revision des BÜPF weder neue Möglichkeiten noch Verpflichtungen für die Schweizerische Post mit sich bringt.

Für GPS, DJS und gr.ch erscheint die Übertragung der Definition von Randdaten auf die Postüberwachung geradezu absurd. Sie weisen darauf hin, dass die Zahl der Postüberwachungen ohnehin in dem Masse abgenommen hat, als die elektronischen Formen der Kommunikation zugenommen haben und beantragen statt der Verdoppelung der Aufbewahrungsdauer die Streichung der Bestimmung und Aufhebung der darauf aufgebauten Praxis. Die GPS verweist dabei auf den immensen Datenbestand, der angehäuft wird und für die Verfolgung von Straftaten nur eine minimale Bedeutung hat. Gemäss DJS und gr.ch gibt es für die Richtigkeit von Absenderangaben – falls überhaupt erwähnt – keine Gewähr, ausser man verlangt bei jeder Postaufgabe einen persönlichen Identitätsnachweis. Mit Blick auf die Folgen einer wörtlichen Umsetzung halten auch SIUG und VSPF die Bestimmung für ungenügend.

4.1.2 Absatz 2

Eine grössere Anzahl Teilnehmer[85] begrüsst explizit die Ausdehnung der Aufbewahrungsfrist für Verkehrsdaten von sechs auf zwölf Monate. Davon fordern elf Teilnehmer[86] zu prüfen, ob die Aufbewahrungsfrist nicht noch wesentlich weiter ausgedehnt werden kann, nachdem die Daten von den Anbietenden in der Regel ohnehin während zehn Jahren aufbewahrt werden. SZ kann sich jedoch mit einer Verlängerung der Aufbewahrungsfrist nur dann einverstanden erklären, wenn gleichzeitig auch gesetzliche Massnahmen vorgesehen werden, welche die Datensicherheit, den Schutz vor missbräuchlicher Verwendung sowie die Transparenz der Datenübermittlung gewährleisten.

Für die Schweizerische Post stellt die geplante Erstreckung der Aufbewahrungsdauer der Randdaten aus dem Postverkehr auf zwölf Monate kein Problem dar.

Cablecom und SKS lehnen die Verlängerung der Aufbewahrungsfrist ab. SKS verweist darauf, dass die Postkommunikation zulasten der elektronischen Kommunikation stetig abge-

---

84 ZH, LU, NW, GL, GR, TG, VS, JU, KKJPD, KSBS.
85 ZH, LU, NW, GL, GR, TG, VS, JU, SZ, UR, OW, FR, SO, AG, GE, KKJPD, KSBS.
86 ZH, LU, NW, GL, GR, TG, VS, JU, SZ, KKJPD, KSBS.

nommen hat und die gesammelten Daten für die Strafverfolgung kaum praktischen Nutzen haben.

5. Pflichten bei der Überwachung des Fernmeldeverkehrs

Mehrere Teilnehmer aus der Fernmeldedienstbranche[87] beantragen folgende Neubenennung des Titels des 5. Abschnittes: „Pflichten der Anbieterinnen von Fernmeldediensten". Dies wird damit begründet, dass es bei den Auskünften über Fernmeldeanschlüsse (Art. 20 VE-BÜPF) nicht um eine Überwachung und auch nicht um einen Eingriff ins Fernmeldegeheimnis geht.

Swisscom beantragt, im 5. Abschnitt folgende drei Kategorien von Leistungen vorzusehen und innerhalb dieser Kategorien jeweils einen klareren Rahmen zu setzen: Auskünfte über Anschlüsse, Echtzeitüberwachungen sowie Aufbewahrung von Verbindungsdaten. Weiter sollen die Bestimmungen mit der StPO koordiniert werden. Aus dieser geht klar hervor, dass nur die Überwachung bestimmter Anschlüsse, welche von verdächtigen Personen benutzt werden, zulässig sein sollte. Eine generelle Suche nach Verdachtsmomenten ist demgemäss unzulässig. Es gilt gemäss Swisscom somit zu vermeiden, dass – wie dies bisher der Fall war – eine Anordnung erfolgt, welche gemäss der neuen StPO gar nicht möglich sein dürfte.

5.1. Artikel 20 Auskünfte über Fernmeldeanschlüsse

[1] Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, müssen dem Dienst folgende Daten über bestimmte Fernmeldeanschlüsse liefern:

- *a. Name, Vorname, Geburtsdatum, Adresse und, sofern vorhanden, Beruf der Teilnehmerin oder des Teilnehmers;*
- *b. die Adressierungselemente gemäss Artikel 3 Buchstabe f des Fernmeldegesetzes vom 30. April 1997;*
- *c. Arten der Anschlüsse.*

[2] Die Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, müssen während mindestens zwei Jahren nach Aufnahme der Kundenbeziehung die Auskünfte nach Absatz 1 auch über Personen erteilen können, welche die Kundenbeziehung für Mobiltelefone und Internet nicht über ein Abonnementsverhältnis aufgenommen haben.

[3] Wird eine Straftat über das Internet begangen, so müssen Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, dem Dienst alle Angaben machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen.

[4] Der Bundesrat regelt die Form der Gesuche und deren Aufbewahrung. Er kann den Behörden nach Artikel 14 den Zugriff auf bestehende nicht öffentliche Verzeichnisse gestatten. Er kann auch diese Daten dem Dienst durch ein Abrufverfahren zugänglich machen. Er kann vorsehen, dass die Mitteilung kostenlos und rund um die Uhr zu erfolgen hat.

IT(19), SWICO, hp und COG beantragen, eine externe Kontrollinstanz vorzusehen, welche den zentralen Dienst zu jedem Zeitpunkt überwacht und kontrolliert. SWICO, hp und COG verweisen zur Begründung darauf, dass der vorgeschriebene Zugriff auf sämtliche Kommunikationsdaten und die somit sichergestellte Identifikation der Teilnehmer den Bundesbehörden umfassende Überwachungsmöglichkeiten zusichert.

5.1.1 Absatz 1

UNISG und UNIZH möchten eine gesetzliche Klarstellung dahingehend, dass „Internetanschlüsse", welche gemäss dem erläuternden Bericht ebenfalls unter „Fernmeldeanschlüsse" zu subsumieren sind, explizit genannt werden. switch und switchplus halten fest, dass der

[87] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

Begriff „Fernmeldeanschluss“ weder im VÜPF noch im FMG definiert ist. Einzig in der Verordnung vom 9. Dezember 1997 des Bundesamtes für Kommunikation über Fernmeldedienste und Adressierungselemente (TAV)[88] ist davon die Rede. Gemeint ist dort die Telefonie über GSM[89]/UMTS[90], PSTN[91]/ISDN[92] und IP (VoIP). Wer VoIP-Dienste für die Öffentlichkeit erbringt, ist verpflichtet diese Daten bekannt zu geben. Nicht öffentliche VoIP-Dienste sind nicht erfasst.

Buchstabe a

Zehn Teilnehmer[93] begrüssen ausdrücklich, dass neu zusätzlich das Geburtsdatum zu erheben ist. ZH, LU, KKPKS und BL beantragen überdies, dass um die Identifikationen der Kundinnen und Kunden sicherzustellen, insbesondere im Bereich der Prepaid-Registrierungen im Mobile-Bereich, auch Ausweisart und -nummer erfasst werden. BL verweist in diesem Zusammenhang auf Missbräuche in der Praxis, wonach viele Kundenbeziehungen auf Grund von Personalien eröffnet werden, die von Anfang an nicht existiert haben oder dass nach einer korrekt verlaufenen Registrierung einer Prepaid-SIM-Karte von einem Angestellten der Verkaufsstelle noch weitere SIM-Karten auf sie eingetragen werden.

Andere Teilnehmer[94] beantragen, die Erhebung des Geburtsdatums wieder zu streichen.

UNISG und UNIZH weisen darauf hin, dass im Internetbereich, bspw. bei der Benutzung eines öffentlichen Terminals, Teilnehmer gar nicht ermittelt werden können.

Gemäss HR hat Buchstabe a zur Folge, dass E-Mail Adressen nicht mehr anonym vergeben werden können. Er fragt sich, ob auch Mehrwertdienstanbieter, die keine eigenen Adressen vergeben, Verknüpfung von E-Mail Adresse und natürlicher Person sicherstellen müssen oder ob sie dann auf die Domainbesitzer gemäss „Whois“ Protokoll verweisen dürfen. Weiter stellt er sich die Frage, ob es somit strafbar ist, ohne Abfrage des Geburtsdatums einen Forum- bzw. Blog-Eintrag zuzulassen.

Buchstabe b

Neun Teilnehmer[95] beantragen folgende Neuformulierung von Buchstabe b: „Die Adressierungselemente gemäss Artikel 3 Buchstabe f *und g* des Fernmeldegesetzes vom 30. April 1997“. Zur Begründung verweisen sie darauf, dass in Artikel 270ter und Artikel 274 Absatz 4 Buchstabe d StPO nur Mobiltelefongeräte aufgeführt sind. Laptops und Notebooks mit SIM-Karten für Übertragung über das Mobilfunknetz sind damit ausgeschlossen.

VD möchte eine gesetzliche Klarstellung bezüglich der Identifikation von IP-Adressen. Heute wird ein solches Gesuch als einfache Massnahme gemäss geltendem Artikel 14 BÜPF angesehen, was den Polizeibehörden erlaubt, ohne Bewilligung durch einen Magistraten die Daten zu erhalten. Diese Praxis kann gemäss VD aufgrund des VE-BÜPF nicht ohne weiteres beibehalten werden. Er beantragt daher Klarstellung, dass der Zugang zu IP-Adressen wie der Zugang zu einer Telefonnummer, nicht über ein Bewilligungsverfahren erfolgt, sondern wie heute, in einem einfachen Verfahren.

---

88 SR 784.101.113
89 Global System for Mobile Communications.
90 Universal Mobile Telecommunications System.
91 Public Switched Telephone Network.
92 Integrated Services Digital Network.
93 ZH, LU, SO, GL, GR, TG, VS, JU, KKJPD, KKPKS.
94 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
95 ZH, LU, GL, GR, TG, VS, JU, KKJPD, KKPKS.

Buchstabe c

Keine Bemerkungen.

5.1.2 Absatz 2

BL empfindet die vorgesehene Regelung über die Dauer der Auskunftspflicht als unklar. So ist insbesondere nicht erkennbar, weshalb die Frist losgelöst von einer aktiven Kundenbeziehung auf zwei Jahre festgelegt wird. Eine Fernmeldedienstanbieterin muss die Informationen gemäss Absatz 1 zu sämtlichen aktiven Kundenbeziehungen abgeben können. Er schlägt deshalb folgende Formulierung vor: *„(…) bis zwei Jahre nach Auflösung der Kundenbeziehung oder Deaktivierung des Anschlusses (…)“*. Zudem soll der Wortlaut von Artikel 20 Absatz 2 VE-BÜPF dahingehend ergänzt werden, dass die Fernmeldedienstanbieterinnen während der vorgesehenen Frist verpflichtet sind, immer auch die Ausweiskopien ihrer Kunden herausgeben zu können. VD beantragt zudem eine explizite Erwähnung von Prepaid-Wireless-Karten.

Acht Teilnehmer[96] beantragen folgende Neuformulierung: „Die Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, müssen während mindestens zwei Jahren nach Aufnahme der Kundenbeziehung die Auskünfte nach Absatz 1 auch über die *erstregistrierten* Personen erteilen können, welche die Kundenbeziehung für Mobiltelefone nicht über ein Abonnementsverhältnis aufgenommen haben“. Die Formulierung „und Internet“ ist zu streichen, da eine Registrierungspflicht, bspw. für „WLAN-Prepaidkarten“, nicht praktikabel ist.

UNIZH schlägt vor, die vorgeschlagene zweijährige Frist der allgemeinen Aufbewahrungsfrist von zwölf Monaten (vgl. Art. 19 Abs. 2 VE-BÜPF bzw. Art. 23 VE-BÜPF) anzugleichen, da ansonsten ein aufwändiges Trennungsverfahren nötig ist, um Daten mit verschiedenen Fristen auseinanderzuhalten.

5.1.3 Absatz 3

Für SO stellt die ausgeweitete Pflicht zur Identifikation von Urhebern eine wesentliche Erleichterung der Polizeiarbeit dar.

SSV möchte eine Präzisierung bezüglich Auskünfte über Fernmeldeanschlüsse, da nicht klar ist, welche Daten von den Anbietern von öffentlichen „Wi-Fi-Anschlüssen“ erhoben und aufbewahrt werden müssen.

Acht Teilnehmer[97] schlagen folgende Neuformulierung vor: „Wird eine Straftat über das Internet begangen, so müssen Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, dem Dienst alle *verfügbaren* Angaben *zu den Fernmeldeanschlüssen machen, die zur Identifikation des Urhebers oder der Urheberin beitragen können*“. Sie begründen die vorgeschlagenen Änderungen damit, dass es nur um Auskünfte über Anschlüsse, und nicht um Kommunikationsdaten gehen darf. Weiter dürfen Angaben, welche über Absatz 1 hinausgehen, nur soweit verfügbar verlangt werden. Die Identifikation des Urhebers kann das Ziel, aber keine verbindliche Bringschuld sein. Cablecom verweist schliesslich darauf, dass eine Identifikation des Gerätes, über welches die Tat begangen wurde, in den meisten Fällen zwar möglich ist, jedoch nicht, wenn sich das Zielgerät über einen privaten „Router“ verbindet. In diesem Fall ist nur die Identifizierung des „Routers“ mög-

---

96 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
97 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

lich, nicht aber die des verwendeten Endgerätes. In diesem Zusammenhang bemerkt UNIZH, dass zwischen der abonnierten Person und der zu überwachenden Person zu unterscheiden ist. Es sind nur Angaben über das Abonnement eines Kabelanschlusses oder über die Person möglich, für die ein Adressierungselement reserviert ist. Festzustellen, wer effektiv den Computer bzw. das Smartphone etc. gebraucht hat, ist eine kaum zu bewältigende Aufgabe. Deshalb schlägt sie folgende Formulierung vor: „…eine Identifikation des Urhebers oder der Urheberin ermöglichen, *sofern sie einen Fernmeldeanschluss betreffen*".

Gemäss switch und switchplus scheint Absatz 3 nicht mehr nur Fernmeldeanschlüsse zu betreffen. Sie möchten daher eine dahingehende Klarstellung, dass dies nur für Fernmeldeanschlüsse gelten kann, und nicht auch für „Domain-Namen".

ISSS beantragt, Gegenstand und Umfang der Teilnehmeridentifikation nach den heutigen und voraussehbaren künftigen Formen der Nutzung der digitalen Kommunikation und des Internets anzupassen und zu konkretisieren. Die Einführung einer Pflicht der Fernmeldedienstanbieter zur persönlichen Identifikation jedes einzelnen Teilnehmers am digitalen Kommunikationsverkehr und bei der Nutzung des Internets stellt die Verpflichteten vor praktisch unlösbare Aufgaben.

Für KFG stellt die Bestimmung einen Schritt in die totale Überwachung des Internets dar. Jeder User muss sich identifizieren. Es beantragt, die Bestimmung so anzupassen, dass nur jeweils registrierte Internetbenutzer eines Anschlusses ermittelt werden müssen, oder aber die Bestimmung ersatzlos zu streichen.

ifpi und safe weisen darauf hin, dass im Urheberstrafrecht private Rechte das geschützte Rechtsgut darstellen. Dabei wird die Rechtsordnung im gesamten Internet unterlaufen, wenn den Rechtsinhabern die Möglichkeit, sich direkt an den Rechtsverletzer zu wenden, aus der Hand genommen wird. Die Folge ist eine Strafverfolgung, welche den Zugriff auf den Rechtsverletzer erlaubt. Diese unerwünschte Kriminalisierung privater Rechtsverletzer ist entbehrlich, wenn die Rechtsinhaber diese kennen und sich mit zivilrechtlichen Mitteln direkt an diese wenden können. Sie beantragen deshalb, den VE-BÜPF dahingehend anzupassen, dass bei Glaubhaftmachung einer Rechtsverletzung unter Verwendung einer bestimmten IP-Adresse die Auskünfte gemäss Absatz 3 auf Anfrage auch dem Geschädigten zu erteilen sind oder der Geschädigte die Auskünfte direkt von den ISP erhalten kann.

5.1.4 Absatz 4

Einige Teilnehmer[98] kritisieren mit Verweis auf die Ratifizierung der Convention on Cybercrime[99] die Ausgestaltung als Kann-Vorschrift. Sie beantragen, eine kostenlose und jederzeitige Mitteilungspflicht auf Gesetzesstufe vorzusehen.

SZ, NW, SG und KSBS beantragen einen „Online-Zugriff" für Strafverfolgungsbehörden. Heute muss je nach Anbieterin auf die Beantwortung der Frage, wem eine bestimmte Telefonnummer gehört, unter Umständen mehrere Stunden gewartet werden, was in Fällen der Notsuche, aber auch nach schweren Straftaten unhaltbar ist. Die Anbieterinnen weigern sich, diese Daten elektronisch zur Verfügung zu stellen, weil sie befürchten, dass ihre Konkurrenten dann auf die Daten greifen könnten. Dieses Problem kann jedoch technisch ohne weiteres gelöst werden.

---

98 ZH, LU, GL, GR, TG, VS, JU, KKPKS, KKJPD.
99 BBl **2010** 4697

Teilnehmer aus der Fernmeldedienstbranche[100] betonen hingegen, dass von den Fernmeldedienstanbieterinnen nicht immer noch mehr Leistung verlangt werden kann. Sie beantragen die Streichung des letzten Satzes von Absatz 4.

Für Cablecom ist unklar, was mit dem in Absatz 4 beschriebenen Abrufverfahren gemeint ist.

UNISG und UNIZH empfinden eine behördliche Zugriffsmöglichkeit auf bestehende nicht öffentliche Verzeichnisse als problematisch.

switch und switchplus möchten die in der Bestimmung erwähnten nicht öffentlichen Verzeichnisse explizit auf Verzeichnisse beschränken, welche Fernmeldeanschlüsse betreffen.

5.2. Artikel 21 Pflichten bei der Durchführung von Überwachungen

[1] Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, müssen dem Dienst auf Verlangen den Fernmeldeverkehr der überwachten Person sowie die Daten, welche darüber Auskunft geben, wann und mit welchen Anschlüssen die überwachte Person über den Fernmeldeverkehr Verbindung hat oder gehabt hat, sowie die Verkehrs- und Rechnungsdaten zuleiten. Artikel 16 Buchstabe d bleibt vorbehalten. Ebenso haben sie die zur Vornahme der Überwachung notwendigen Informationen zu erteilen.

[2] Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, liefern die Daten, welche darüber Auskunft geben, wann und mit welchen Anschlüssen die überwachte Person über den Fernmeldeverkehr Verbindung hat oder gehabt hat, sowie Verkehrs- und Rechnungsdaten so rasch als möglich und den Fernmeldeverkehr der überwachten Person soweit möglich in Echtzeit. Von ihnen angebrachte Verschlüsselungen müssen sie entfernen.

[3] Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, leiten dem Dienst den gesamten Datenfluss der überwachten Person weiter. Auf Verlangen des Dienstes sind sie verpflichtet, dem Dienst nur den bezeichneten Typ oder die bezeichneten Typen von Daten aus dem Datenstrom zu liefern.

[4] Die Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, leisten dem Dienst die nötige Unterstützung, um eine Überwachung umzusetzen, für welche Informatik-Programme erforderlich sind, um die Daten abfangen und lesen zu können (Art. 270bis StPO und Art. 70a^{bis} des Militärstrafprozesses).

[5] Alle Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz ausführen und die an der zu überwachenden Fernmeldedienstleistung beteiligt sind, sind verpflichtet, ihre Daten der vom Dienst mit der Überwachung beauftragten Person zu liefern.

Für eine Vielzahl von Teilnehmern[101] sind die konkreten Pflichten zu wenig klar geregelt. Im Sinne der Rechtssicherheit fordern sie daher, teilweise mit konkreten Formulierungsvorschlägen, ein klares Pflichtenheft vorzusehen. Swisscom verlangt zudem, dass für alle von Dritten angebotenen Dienste die Fernmeldedienstanbieterinnen nicht verpflichtet werden dürfen, Koordinationsaufgaben zu übernehmen. Die Drittanbieter müssten direkt vom Dienst in die Pflicht genommen werden.

5.2.1 Absatz 1

KKPKS beantragt, die Auskunftspflicht auf Fälle auszudehnen, bei welchen die überwachte Person lediglich versuchte, eine Verbindung aufzubauen.

Mehrere Teilnehmer aus der Fernmeldedienstbranche[102] fordern mit konkreten Formulierungsvorschlägen eine einschränkende Präzisierung dahingehend, dass sich die Überwachungspflicht auf den Fernmeldeverkehr eines bestimmten Anschlusses bezieht, welcher von einer Fernmeldedienstanbieterin zur Verfügung gestellt wurde. Überdies schlagen sie die Schaffung eines separaten Artikels bezüglich der Erhebung von Verbindungsdaten vor.

---

[100] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.
[101] CVP, FDP, SVP, GPS, SKS, economiesuisse, ICT, ePower, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, SIUG, SPICT.
[102] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

Für Cablecom ist unklar, was mit „notwendige Informationen“ genau gemeint ist.

5.2.2 Absatz 2

Dieselben Teilnehmer[103] fordern entsprechend auch in Absatz 2 eine Beschränkung der Überwachungspflicht auf einen bestimmten Anschluss, welcher von einer bestimmten Fernmeldedienstanbieterin zur Verfügung gestellt wurde. Schliesslich beantragen sie eine Klarstellung dahingehend, dass die Lesbarkeit der gelieferten Daten nicht garantiert werden kann.

Eine grössere Anzahl Teilnehmer[104] fordert die Streichung der Begriffe „so rasch als möglich“ und „soweit möglich in Echtzeit“, da sie unpräzise und hinsichtlich der zu erwartenden Kosten für die Infrastruktur inakzeptabel sind. Auch KKPKS erachtet die Formulierung „so rasch als möglich…“ als unpräzis, fordert hingegen einen Verweis im Gesetz auf die technischen Richtlinien, wo der Zeitrahmen für die Datenlieferung zu definieren ist.

UNISG und UNIZH bezweifeln die technische Realisierbarkeit der vorgesehenen Entfernung von Verschlüsselungen. IT(19), SWICO, hp und COG fordern eine gesetzliche Regelung, wonach die Fernmeldedienstanbieterinnen ihre „überwachten“ Kunden noch vor der Einleitung einer Überwachungsmassnahme darüber zu unterrichten haben, dass die verwendete Verschlüsselung im Rahmen einer Überwachungsmassnahme nach BÜPF aufgehoben werden und der Kunde in der Folge Gegenstand einer Überwachung wird. Auch ISSS geht davon aus, dass Fernmeldedienstanbieterinnen aufgrund ihrer gesetzlichen Treue- und Sorgfaltspflicht ihre Kunden darüber aufklären müssen, dass die verwendete Verschlüsselung aufgehoben werden kann. Sie fordert, dass die Offenlegung der von Fernmeldedienstanbieterinnen angebrachten Verschlüsselung auf im Gesetz klar umschriebene Fälle beschränkt und ein Verfahren vorgesehen wird, in welchem die Fernmeldedienstanbieterinnen die Interessen ihrer Kunden an geschützter Kommunikation geltend machen und einer richterlichen Entscheidung zuführen können.

HR verweist auf den unklaren Wortlaut und fordert eine Klarstellung, wonach Verschlüsselungen nicht generell verboten sind. Eine Kryptographie „end-2-end“ ist insbesondere eine wichtige Arbeitsvoraussetzung für NGO’s[105] wie das IKRK oder Amnesty International.

5.2.3 Absatz 3

Elf Teilnehmer[106] sind der Meinung, dass die Aussonderung von bestimmten Daten aus dem zu liefernden Datenstrom technisch nicht gelöst werden kann und daher zu streichen ist (vgl. auch III. Ziff. 3.3.6 zu Art. 16 Bst. f VE-BÜPF). UNIZH stellt die technische Machbarkeit zumindest in Frage. Einige Teilnehmer[107] fordern, dass die Filterung des Datenstroms Sache des Dienstes sein muss.

privatim erachtet die Bestimmung als zu offen formuliert und schlägt folgende einschränkende Formulierung vor: „… den gesamten Datenfluss *im Rahmen der Anordnung*…“. Andernfalls wird nicht nur das Bestimmtheitsgebot, sondern es werden auch der Zweckbindungsgrundsatz und das Verhältnismässigkeitsprinzip missachtet.

---

[103] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
[104] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom, IT(19), ISSS, PPS.
[105] Non-Governmental Organization.
[106] SVP, GPS, SKS, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
[107] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

CP weist darauf hin, dass das Ausscheiden von Daten auch Einsicht in heikle persönliche Daten bedeutet und zudem die Gefahr eines Datenverlustes droht. Die Bestimmung muss entsprechend überarbeitet werden. Gemäss SIMSA eignet sich der Begriff „Datenfluss“ nicht, den Überwachungsumfang zu begrenzen und verletzt daher den Grundsatz des vertraulichen Umgangs mit Personendaten. Überwachungsrelevant können nur Daten aus der Individualkommunikation der überwachten Person sein. IT(19), SWICO, hp und COG vergleichen die Überwachung des gesamten Datenflusses mit einer Hausdurchsuchung. Eine solche Überwachungsmassnahme kann nur mit richterlicher Genehmigung erfolgen, welche den Fernmeldedienstanbieterinnen und ISP vorgängig vorzulegen ist. Zudem fordern sie, den Aufwand einer Datentriage zu entschädigen.

ISSS weist warnend darauf hin, dass die Entwicklung solcher Filtrierungs- und Triage-Systeme leider auch die Wirkung haben kann, die Ausforschung von Datenbeständen und Datenflüssen durch Unberechtigte zu erleichtern und daher das Niveau der Informationssicherheit in unserem Lande zu beeinträchtigen. ISSS beantragt daher, Analyse- und Filtrierungs-Programme nur in qualifizierten Einzelfällen aufgrund richterlicher Anordnung anzuordnen.

5.2.4 Absatz 4

Generelle Bemerkungen zum neu vorgesehenen Einsatz von Informatik-Programmen finden sich in III. Ziffer 11.1.2 zu Artikel 270bis StPO. Nachfolgend werden diejenigen Bemerkungen angeführt, welche in einem weiteren Sinne die in Absatz 4 erwähnte Unterstützungspflicht der verpflichteten Personen betreffen:

Mehreren Teilnehmern[108] erscheint es unklar, wer konkret für die Entwicklung, Beschaffung und den Einsatz solcher Programme zuständig ist. Daher fordern privatim, SIMSA und ISSS den Begriff „die nötige Unterstützung“ zu konkretisieren.

Gemäss anderen Teilnehmern[109] darf der Einsatz solcher Programme nicht an private Firmen delegiert werden, sondern ist von der zuständigen Behörde vorzunehmen. Eine zwangsweise Involvierung von Privaten in Polizeiaktionen ist im schweizerischen Rechtssystem nicht wünschenswert. Gemäss PPS muss das zwingend auch für die Herstellung und Wartung des Infiltrationssystems gelten.

Weitere Teilnehmer[110] finden es generell unzumutbar, nach Anweisungen des Dienstes „Government Software“ (oft auch „Bundestrojaner“ genannt) bei Kunden zu setzen. Eine solche zwangsweise Involvierung von Privaten in polizeiliche Aktionen ist einzigartig und beeinträchtigt das Vertrauensverhältnis zwischen Betreiber und Kundschaft massiv, da der Einsatz derartiger Programme im krassen Widerspruch zu den Interessen der Kunden steht. Sie lehnen entsprechende Ausführungs- und Mitwirkungspflichten strikt ab und fordern zusammen mit IT(19) und Cablecom die Streichung der Bestimmung.

RD weist darauf hin, dass diese Programme an sich schon problematisch und sehr umstritten sind. Die Anbieter nun noch zwingen zu wollen, die Behörden beim "Hacken" in die Systeme von Kunden und Dritter in jeder erdenklichen Form zu unterstützen, ohne dass das Gesetz klare Leitlinien aufstellt, geht aus seiner Sicht zu weit und ist auch nicht erforderlich. Es untergräbt das Vertrauen einer ganzen Industrie und schafft Sicherheitsrisiken, die letztlich der ganzen Wirtschaft schaden.

---

[108] ZH, BL, ZG LU, SP, privatim, ISSS.
[109] SVP, CVP, FDP, PPS, economiesuisse, Swisscable.
[110] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SWICO, hp, COG.

switch betont, dass sie als Netzwerkbetreiberin weitgehende Massnahmen gegen Schadens- und Spionageprogramme durchführt und im Falle einer Überwachung nicht zwischen ungewollter Schadenssoftware und Spionageprogramme unterscheiden kann. Eine Zusammenarbeit mit dem Dienst ist daher zwingend. Zudem hat eine solche Überwachungsmassnahme zur Folge, dass sämtliche Massnahmen gegen Schadsoftware einzustellen sind. Vor diesem Hintergrund verlangt switch eine dezidiertere Formulierung um den genannten Zielkonflikt zu vermeiden.

5.2.5 Absatz 5

VD fordert eine Klarstellung der Bestimmung. Andere Teilnehmer[111] beantragen die ersatzlose Streichung.

5.3. Artikel 22 Identifizierung von Internet-Benutzern

Die Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, müssen die nötigen technischen Vorkehren treffen, um die Personen identifizieren zu können, die über ihre Vermittlung Zugang zum Internet erhalten.

Eine grössere Anzahl Teilnehmer[112] begrüsst die Bestimmung ausdrücklich. Gemäss ZH vermag eine Identifizierung von Internet-Benutzern wichtige bzw. die entscheidenden Hinweise für die Strafverfolgung zu liefern. Umgekehrt kann die Identifizierungsmöglichkeit auch eine präventive Wirkung entfalten. SZ sowie KSBS verweisen auf die umliegenden Länder, wo es nicht mehr möglich ist, anonym und ohne Identifizierung Zugang zum Internet zu erhalten. Der damit verbundene administrative Aufwand für die Anbieterinnen bei temporärem Zugang zum Internet (Hotels, Internet-Cafés usw.) wird als vertretbar angesehen.

Eine Vielzahl von Teilnehmern[113] beantragt hingegen die Streichung bzw. Anpassung der Bestimmung. Für VD, ISSS und GPS ist eine derartige Verpflichtung, insbesondere hinsichtlich kabelloser Zugänge mittels „Wi-Fi“ (Bahnhöfe, Schulen, Hotels etc.), unverhältnismässig und führt dazu, dass viele der heute der Öffentlichkeit zur Verfügung gestellten Verbindungen aufgehoben würden. Sie beantragen, diese in Europa einzigartige Verpflichtung zu streichen bzw. erheblich anzupassen. Die SVP verweist auf den unverhältnismässigen Aufwand und spricht sich ebenfalls für die Streichung aus. Auch SSV und privatim lehnen die Bestimmung, u.a. mit Verweis auf die einfachen Umgehungsmöglichkeiten („Proxies“; Verbergen der IP-Adresse, Anmeldung mit SIM-Karte aus zweiter Hand) und dem unverhältnismässigen Eingriff in die persönliche Freiheit sämtlicher Internet-Benutzer ab. Für DJS und gr.ch ist die Bestimmung absurd und zeigt den totalitären Ansatz der Gesamtvorlage. So setzt das Telefonieren in einer öffentlichen Telefonzelle auch nicht voraus, dass die betreffende Person zunächst einen Identitätsnachweis erbringen muss. Als Konsequenz der Bestimmung muss bspw., wer einen Bekannten an seinen Computer oder an sein Smartphone lässt, damit dieser surfen kann, seinem Provider vorgängig die Identifizierung ermöglichen. Weiter bedeutet die Vorschrift, dass Provider ihren Nutzern verbieten müssten, nicht passwortgeschützte Netzwerke zu betreiben. Die vorgeschlagene Registrierung mittels Mobiletelefonnummer schliesst zudem Personen aus und ist leicht zu umgehen. Auch RD hält die Bestimmung für unsinnig und führt ebenfalls den Vergleich mit der fehlenden Identifikationspflicht bei der Telefonie an. Gemäss einer grösseren Teilnehmerzahl[114] kann eine Fernmeldedienstanbieterin

---

111 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.
112 ZH, LU, SZ, NW, SO, GL, GR, TG, VS, JU, KKJPD, KKPKS, KSBS.
113 VD, GPS, SVP, FDP, ISSS, SSV, privatim, DJS, gr.ch, RD, IT(19), Cablecom, switch und switchplus, CP, SAV, KFG, PPS, ETH, UNISG, UNIZH.
114 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SWICO, hp, COG, IT(19).

zwar ihre Abonnementskunden, also ihre Vertragspartner, identifizieren, nicht jedoch jeden einzelnen User, welcher über einen entsprechenden Anschluss ins Internet gelangt. Die Bestimmung ist zu streichen bzw. gemäss IT(19) ist klar zu definieren und abzugrenzen, wie hoch der Aufwand für eine Identifizierung sein darf. Zudem muss der Aufwand entschädigt werden. Auch Cablecom, switch und switchplus sprechen sich für eine Streichung bzw. für eine Umformulierung aus und halten fest, dass maximal eine Identifikation des verwendeten Gerätes realisiert werden kann. Auch diese Identifikation ist jedoch nur möglich, wenn sich alle dazwischen geschalteten Geräte („Router", „Wireless AP's", usw.) im Verantwortungsbereich und der technischen Kontrolle des Verpflichteten befinden. Die Identifikation mittels Mobiltelefonnummer ist nicht praktikabel: Wenn der Benutzer ein ausländisches Mobiltelefon verwendet, müssen die Benutzerdaten bei der ausländischen Anbieterin bestellt werden, die in diesem Fall gar nicht dem schweizerischen Recht untersteht. FDP, CP und SAV bezweifeln, dass man die Umsetzbarkeit bzw. die Folgen der Regelung genügend durchdacht hat. KFG und PPS beantragen, entweder die Identifizierungspflicht einzuschränken oder die Bestimmung zu streichen. Gemäss ETH, UNISG und UNIZH scheint der Gesetzgeber davon auszugehen, dass Schulen, Hotels etc. ihren Internetzugang über einen traditionellen Acces-Provider beziehen. Universitäten vergeben ihre eigene IP Adressen, bieten ihre Dienste aber nicht der Öffentlichkeit an. Somit sind sie zwar Access-Provider, aber keine Internet-Anbieterinnen im Sinne von Artikel 2 Buchstabe a VÜPF, womit Artikel 22 VE-BÜPF für sie nicht gilt. Gemäss den erwähnten Hochschulen hat Artikel 22 das Potential zur umfassenden Überwachung und ist daher unter dem Gesichtspunkt der Verhältnismässigkeit nochmals eingehend zu prüfen und zu präzisieren.

5.4. Artikel 23 Datenaufbewahrung

Die Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, sind verpflichtet, die Daten, welche darüber Auskunft geben, wann und mit welchen Anschlüssen die überwachte Person über den Fernmeldeverkehr Verbindung hat oder gehabt hat, sowie die Verkehrs- und Rechnungsdaten während zwölf Monaten aufzubewahren.

Eine Vielzahl von Teilnehmern[115] begrüsst grundsätzlich die Verlängerung der Aufbewahrungsfrist. FR findet es jedoch notwendig, die zusätzlichen Aufgaben, welche damit auf die Kantone zukommen, vorgängig abzuschätzen. SO verweist auf die Notwendigkeit einer verlängerten Frist insbesondere bei langwierigen Rechtshilfeverfahren. BS möchte zudem die Behandlung von Zufallsfunden geregelt haben. AR, SZ und VD beantragen die Bestimmung mit Vorschriften zur Datensicherheit, Schutz vor missbräuchlicher Verwendung und Transparenz der Datenübermittlung zu ergänzen.

Eine grössere Gruppe von Teilnehmern[116] beantragt, die Aufbewahrungsfrist über die vorgesehene Regelung hinaus auf zehn Jahre anzuheben, damit erfolgreiche Ermittlungsansätze auch nach Jahren noch verfügbar sind. Es wird darauf hingewiesen, dass die Fernmeldedienstsanbieterinnen die Daten von sich aus bereits zehn Jahre aufbewahren. Neun Teilnehmer[117] schlagen dabei vor, die Frist für das *Abrufen* der Daten unabhängig von einer zehnjährigen Aufbewahrungsfrist auf sechs bzw. zwölf Monate zu beschränken. Auch BE möchte die Aufbewahrungsfrist für Randdaten auf mehr als zwölf Monate ausdehnen.

---

[115] OW, ZH, LU, SZ, NW, BL, GL, GR, TG, VS, JU, FR, SO, BS, AR, AG, TI, VD, GE, CVP, FDP KKJPD KKPKS, VSPB, KSBS, SPICT.

[116] ZH, LU, SZ, NW, BL, GL, GR, TG, VS, JU, FDP, KKJPD, KSBS.

[117] NW, GL, GR, TG, VS, JU, FDP, KSBS, KKJPD.

Eine grosse Teilnehmerzahl[118] lehnt die Bestimmung hingegen ab. DJS, gr.ch, GPS und SKS betonen, dass systematisch Daten unverdächtiger Personen auf Vorrat gespeichert werden sollen. GPS und SKS empfinden dies als umso unverständlicher, als die Geschäftsprüfungsdelegation Ende Juni 2010 Zweifel an der Richtigkeit und Relevanz der Daten der ISIS-Datenbank äusserte. Mehrere Teilnehmer[119] verweisen zudem auf die mit der Verlängerung der Aufbewahrungsfrist einhergehenden höheren Kosten und die vorgesehene Streichung jeglicher Entschädigungen.

Gemäss SIUG erwähnt die Bestimmung die Erfassung des Antennenstandorts bei Mobilfunkverbindungen, welche heute im VÜPF vorgeschrieben ist, überhaupt nicht. Sie beantragt, falls eine solche Standorterfassung auch in Zukunft vorgesehen ist, sie auf Gesetzesstufe zu regeln. Die rückwirkende, flächendeckende und verdachtsunabhängige Überwachung betrifft alle Einwohnerinnen und Einwohner der Schweiz und ist daher nicht verhältnismässig. Die Speicherung der Randdaten für zwölf Monate ermöglicht es, ein detailliertes Kommunikations- und Bewegungsprofil sämtlicher Einwohnerinnen und Einwohner der Schweiz zu erstellen. Die Notwendigkeit der Verdoppelung der Speicherungsdauer ist zudem nicht nachgewiesen. Die Überwachungsarten, die zu speichernden Daten und die verwendeten Begriffe sind im Vorentwurf nicht genügend definiert. ISSS lehnt die Bestimmung ebenfalls ab, schlägt aber eventualiter vor, das Gesetz so anzupassen, dass der Dienst im Einzelfall eine Anbieterin auffordern kann, die Verbindungsdaten länger, bis maximal zwölf Monate, aufzubewahren.

BL, SP, 3D4X und privatim verlangen eine revidierte Regelung, die den Kriterien entspricht, wie sie vom deutschen Bundesverfassungsgericht im Zusammenhang mit seinem Entscheid zur Vorratsdatenspeicherung[120] entwickelt worden sind. 3D4X fragt sich, wie eine kleine IT-Firma Überwachungsinstrumente bezahlen soll, wenn es keine Entschädigung dafür gibt. Auch IT(19) verweisen auf die mit der Verlängerung der Aufbewahrungsfrist verbundenen höheren Kosten für die Verpflichteten.

Cablecom wirft die Frage auf, wie Internet-Provider die Datenaufbewahrung sicherstellen wollen, wenn sie gar keine Daten haben, da die Geräte nicht in ihrem Einflussbereich liegen.

Für SSV ist es unklar, welche Daten von den Anbietern von öffentlichen „Wi-Fi Anschlüssen“

---

[118] BL, GPS, SP, SKS, SGB, DJS, gr.ch, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SIUG, ISSS, SWICO, hp, privatim, COG, 3D4X, PPS.

[119] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SWICO, hp, COG, PPS.

[120] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. (1 - 345); Aus den Leitsätzen: "Eine sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter, wie sie die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 (ABl L 105 vom 13. April 2006, S. 54; im Folgenden: Richtlinie 2006/24/EG) vorsieht, ist mit Art. 10 GG nicht schlechthin unvereinbar; Der Grundsatz der Verhältnismäßigkeit verlangt, dass die gesetzliche Ausgestaltung einer solchen Datenspeicherung dem besonderen Gewicht des mit der Speicherung verbundenen Grundrechtseingriffs angemessen Rechnung trägt. Gemäss den Leitsätzen des Urteils sind hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes erforderlich (…) Der Abruf und die unmittelbare Nutzung der Daten sind nur verhältnismäßig, wenn sie überragend wichtigen Aufgaben des Rechtsgüterschutzes dienen. Im Bereich der Strafverfolgung setzt dies einen durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraus. (…) Eine nur mittelbare Nutzung der Daten zur Erteilung von Auskünften durch die Telekommunikationsdiensteanbieter über die Inhaber von Internetprotokolladressen ist auch unabhängig von begrenzenden Straftaten- oder Rechtsgüterkatalogen für die Strafverfolgung, Gefahrenabwehr und die Wahrnehmung nachrichtendienstlicher Aufgaben zulässig. Für die Verfolgung von Ordnungswidrigkeiten können solche Auskünfte nur in gesetzlich ausdrücklich benannten Fällen von besonderem Gewicht erlaubt werden (…)".

erhoben und aufbewahrt werden müssen.

ETH, UNISG und UNIZH halten mit Verweis auf den Wortlaut fest, dass für Betreiber von internen Fernmeldenetzen und Hauszentralen keine Aufbewahrungspflicht besteht.

SAV vermisst eine Begründung für die Verlängerung der Aufbewahrungsfrist.

switch und switchplus möchten eine Präzisierung des Wortlauts von Artikel 23 VE-BÜPF, damit klar wird, dass auch Personen nach Artikel 2 Absatz 2 VE-BÜPF Verkehrsdaten aufzubewahren haben.

safe beantragt, dass auch die Suche nach einer *unbekannten* Person, von welcher ein bestimmter Datenverkehrsvorgang im Internet ausging, in die Bestimmung aufgenommen wird. Gemäss safe ist der Wortlaut zu eng. Er erfasst den wesentlichen Fall nicht, wo nicht nach den Verbindungen einer bekannten bzw. überwachten Person gesucht wird, sondern gerade nach einer unbekannten Person, von welcher ein bestimmter Datenverkehrsvorgang im Internet ausging.

5.5. Artikel 24 Zertifizierung

Bemerkungen zur Zertifizierung finden sich in III. Ziffer 3.5 zu Artikel 18 VE-BÜPF.

5.6. Artikel 25 Information über Technologien und Dienste

Auf Anfrage des Dienstes informieren die Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, den Dienst jederzeit ausführlich über die Art und Merkmale von Technologien oder Diensten, welche sie der Öffentlichkeit zur Verfügung gestellt haben oder stellen werden.

Für neun Teilnehmer[121] fällt die Bekanntgabe von künftigen Dienstleistungen bzw. Technologien unter das Geschäftsgeheimnis. Eine diesbezügliche Regelung im Gesetz wird abgelehnt. In jedem Fall müssen aber derartige Expertenauskünfte entsprechend entschädigt werden. ISSS weist darauf hin, dass nebst der Gefahr für Geschäfts- und Betriebsgeheimnisse, die hier angesprochenen Technologien sich in einem Grossteil der Fälle im Besitz ausländischer Unternehmen befinden. Diese Bestimmung kann somit für den Wirtschaftsstandort Schweiz erhebliche Probleme hervorrufen und Retorsionsmassnahmen auslösen bzw. dazu führen, dass die Inhaber der Technologie ihrer aktuellen Systeme und Verfahren aufgrund der möglichen Preisgabegefahr in der Schweiz nicht mehr einsetzen. Damit wird der Informationsgesellschaft Schweiz ein Bärendienst erwiesen. ISSS verlangt daher, ein internationales Abkommen anzustreben.

SIMSA macht überdies auf die Gefahr für den Innovationsschutz aufmerksam. IT(19), SWICO, hp und COG verlangen eine Ergänzung der Bestimmung, wonach die Anbieterinnen davor bewahrt werden, Geschäfts- und Berufsgeheimnisse preisgeben zu müssen.

switch und switchplus beantragen Klarstellung, ob die Informationspflicht auch Personen nach Artikel 2 Absatz 2 VE-BÜPF trifft. Überdies betrachten sie eine derartige Pflicht als Schulungsaufwand für Bundesangestellte, welcher entsprechend zu entschädigen ist.

---

[121] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, ISSS, Cablecom.

5.7. Artikel 26 Betreiberinnen von internen Fernmeldenetzen und Hauszentralen und Personen nach Artikel 2 Absatz 1, die ihre Tätigkeit im Bereich des Fernmeldeverkehrs nicht berufsmässig ausüben

Bemerkungen zur Überwachungspflicht der titelvermerkten Personen finden sich in III. Ziffer 1.2.3 zu Artikel 2 Absatz 2 VE-BÜPF.

6. Überwachung ausserhalb von Strafverfahren

6.1. Artikel 27 Notsuche

[1] Ausserhalb von Strafverfahren kann eine auf Teilnehmeridentifikation, Verkehrsdaten und Standortidentifikation beschränkte Überwachung des Fernmeldeverkehrs angeordnet werden, um eine vermisste Person zu finden. Dabei dürfen, wenn erforderlich, auch Daten unbeteiligter Dritter eingesehen werden.

[2] Als vermisst gilt eine Person:

a. deren Aufenthalt die Polizei als unbekannt festgestellt hat; und

b. bei der dringende Anhaltspunkte für eine schwere Gefährdung ihrer Gesundheit oder ihres Lebens bestehen.

6.1.1 Absatz 1

Eine grössere Gruppe von Teilnehmern[122] beantragt, die Bestimmung dahingehend zu ergänzen, dass in bestimmten Fällen nicht nur die Verbindungsdaten, sondern auch die Gesprächsinhalte erhoben werden dürfen, damit verifiziert werden kann, ob wirklich die vermisste Person den überwachten Apparat benutzt hat. Da ohnehin ein Bewilligungsverfahren vorgesehen ist, wird dem Schutzbedürfnis der Betroffenen angemessen Rechnung getragen. VD erachtet ein einfacheres Verfahren für notwendig, damit die Überwachung noch vor der richterlichen Bewilligung vorgenommen werden kann.

Mehrere Teilnehmer aus der Fernmeldedienstbranche[123] verlangen, die Überwachung auf die Standortidentifikation zu beschränken und sprechen sich dagegen aus, Daten unbeteiligter Dritter einsehen zu können. Cablecom geht überdies davon aus, dass sich die Bestimmung ausschliesslich auf die Mobiltelefonie bezieht, da eine Standortermittlung bei internetbasierten Diensten aus heutiger Sicht nicht machbar ist.

SAV kann nicht verstehen, weshalb man den Artikel 8 Absatz 5 geltendes BÜPF gestrichen hat und beantragt daher eine diesbezügliche Ergänzung.

Gemäss SIMSA können die Anbieterinnen die Folgen dieser Norm, insbesondere bezüglich „Daten unbeteiligter Dritter", kaum abschätzen. Auch SZ möchte eine Präzisierung, welche Daten von unbeteiligten Dritten eingesehen werden dürfen. KFG befürchtet diesbezüglich, dass vermehrt Unbeteiligte überwacht werden, lediglich weil sie sich im Umfeld der überwachten Person aufhalten, und beantragt deshalb die Streichung der Bestimmung.

6.1.2 Absatz 2

Keine Bemerkungen.

---

[122] ZH, LU, SZ, SH, SG, AG, GL, GR, TG, VS, JU, KKJPD, KKPKS, KSBS, SKG.

[123] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

6.2. Artikel 28 Suche nach verurteilten Personen

Ausserhalb von Strafverfahren kann eine Überwachung des Post- und Fernmeldeverkehrs angeordnet werden, um eine Person zu finden, die rechtskräftig und vollstreckbar zu einer Freiheitsstrafe verurteilt wurde oder gegenüber der rechtskräftig und vollstreckbar eine freiheitsentziehende Massnahme angeordnet worden ist, sofern die bisherigen Untersuchungshandlungen erfolglos geblieben sind oder die Suche sonst aussichtslos wäre oder unverhältnismässig erschwert würde.

Etliche Teilnehmer[124] begrüssen die neu vorgesehene Möglichkeit für die Fahndung nach verurteilten Personen. OW und SO begrüssen zudem, dass sich die diesbezügliche Überwachung nicht nur auf die Randdaten beschränkt, sondern dass auch Gespräche aufgezeichnet werden können, die Hinweise zum Aufenthaltsort des Gesuchten liefern.

Aus Gründen der öffentlichen Sicherheit (Selbst- und Fremdgefährdung) verlangt ZG zu prüfen, ob nicht auch die fürsorgerische Freiheitsentziehung (Art. 397a ff. ZGB) aufzuführen sei.

privatim erachtet die Bestimmung aus datenschutzrechtlicher Sicht als zu generalklauselhaft. Es ist nicht klar wer, wie, wo und wann überwacht werden kann, obwohl es um potentiell schwere Grundrechtseingriffe geht, insbesondere für Personen aus dem Umfeld des Verurteilten. Es wird daher beantragt, Details dieser Überwachungsmöglichkeiten entweder in der StPO oder in der VÜPF zu regeln. SGB empfindet es als unverhältnismässigen Eingriff in die Privatsphäre, dass es neu auch möglich sein soll, alle Personen die vermeintlich Kontakt mit der verurteilten Person gehabt haben, überwachen zu können.

Acht Teilnehmer[125] wollen eine Präzisierung der Bestimmung dahingehend, dass es sich um eine *flüchtige* Person handeln muss. Cablecom fordert zudem eine Konkretisierung der Begriffe „aussichtslos“ und „unverhältnismässig erschwert“.

SAV weist darauf hin, dass, wer sich der Vollstreckung einer Freiheitsstrafe oder einer Massnahme entzieht, noch keine Straftat begeht. Es ist deshalb wichtig, dass das Verhältnismässigkeitsprinzip bei derartigen Grundrechtseingriffen beachtet wird, indem man auf die Schwere der Tat oder die verhängte Strafe abstellt. Stellt man auf die Schwere der Tat ab, so kann man sich auf den Straftatenkatalog in Artikel 269 Absatz 2 StPO beziehen. Wird die Strafe als massgebend erachtet, muss eine Grenze festgesetzt werden, ab der eine Überwachung zulässig ist, bspw. ein Jahr. VD und CP verlangen eine Beschränkung auf Freiheitsstrafen von mindestens sechs Monaten.

SIMSA betont, dass es vor einer derartigen Überwachungsmassnahme für niemanden ersichtlich ist, welche Gespräche Hinweise enthalten und welche nicht. Das hat zur Konsequenz, dass man entweder nicht überwacht oder dass die Norm zu einer generellen Überwachung der Gespräche führt. Sie weist zudem darauf hin, dass mit der neu vorgesehenen Möglichkeit der Fahndung nach Verurteilten ein erheblicher Mehraufwand auf die Verpflichteten zukommen wird.

AG beantragt, den Begriff „Untersuchungshandlungen“ durch „Fahndungsmassnahmen“ zu ersetzen, da nach einer rechtskräftigen Verurteilung keine Untersuchungshandlungen mehr vorgenommen werden.

---

[124] ZH, LU, SZ, VD, GE, UR, OW, NW, FR, SO, AR, TI, KKJPD, KKPKS, KSBS, VSPB, SKG.
[125] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

6.3. Artikel 29 Verfahren

[1] Für das Verfahren gelten die Artikel 271 bis 279 der Strafprozessordnung vom 5. Oktober 2007 sinngemäss. Die Anordnung bedarf der Genehmigung durch eine richterliche Behörde.

[2] Die Kantone bezeichnen die anordnende Behörde, die Genehmigungsbehörde und die Beschwerdeinstanz.

6.3.1 Absatz 1

SZ erachtet den Verweis auf die sinngemässe Anwendbarkeit der Vorschriften von Artikel 271 bis 279 StPO, anstatt wie bisher auf die Artikel 274 bis 279 StPO, für unbegründet und nicht nachvollziehbar. Es gilt gesetzlich klarzustellen, dass das Verfahren der Notsuche bzw. zur Auffindung Verurteilter durch die sinngemässe Anwendung der StPO nicht zu einem Strafverfahren wird, sondern ein verwaltungs- bzw. polizeirechtliches Verfahren bleibt. Eine gerichtliche Aussonderung von spezifischen Daten zum Schutze eines Berufsgeheimnisses kommt im Zusammenhang mit einer Notsuche gar nicht in Betracht. Die bei einer Notsuche erlangten Erkenntnisse aus einer auf Teilnehmeridentifikation und Verkehrsdaten beschränkten Überwachung dürfen nur zur Rettung der vermissten Person verwendet werden und sind zu vernichten, sobald der Grund der Überwachung weggefallen ist. Die Genehmigungspflicht wird zudem durch Artikel 29 Absatz 1 Satz 2 VE-BÜPF geregelt. Ein sinngemässer Verweis auf die Genehmigungspflicht nach Artikel 272 StPO ist überflüssig und eher verwirrend. In Artikel 273 StPO geht es ebenfalls um Anordnungen im Rahmen eines eröffneten Strafverfahrens. Auch der Verweis auf die sinngemässe Anwendbarkeit der Mitteilungspflicht von Artikel 279 StPO im Zusammenhang mit dem Abschluss einer Notsuche hat immer wieder zu Diskussionen Anlass gegeben und ist nicht weiterführend. Die Mitteilungspflicht ergibt sich aus dem kantonalen Datenschutz- bzw. Polizeirecht und nicht aus der StPO. Für einen zustimmungsbedürftigen Aufschub der Mitteilung durch das Zwangsmassnahmengericht besteht kein Regelungsbedarf; vielmehr werden dadurch das strafprozessuale und das verwaltungsrechtliche Verfahren vermischt. Bei der polizeilichen Mitteilung über die erfolgte Notsuche an die wieder aufgefundene Person bzw. deren Angehörige, verbunden mit einer allfälligen Kostenauflage, handelt es sich weiterhin um eine verwaltungsrechtliche Verfügung, die der Verwaltungsgerichtsbarkeit untersteht und nicht der Beschwerde nach den Artikeln 393 bis 397 StPO.

SSV hält den pauschalen Verweis auf die StPO für systemwidrig, da es sich bei der Notsuche nicht um ein strafprozessuales, sondern um ein sicherheitspolitisches Instrument handelt. Zudem erachtet SSV die richterliche Genehmigungspflicht generell für problematisch, da regelmässig „Gefahr in Verzug“ ist. Die Polizei sollte die Notsuche in eigener Kompetenz anordnen können, da möglichst rasches Handeln erforderlich ist. Der Verzicht auf eine richterliche Genehmigung kann mit nachträglichen Rechtsmitteln kompensiert werden. Die gerichtliche Beurteilung sollte zudem, im Interesse einer möglichst klaren Zuständigkeitsregelung, durch den (Haft-) Richter erfolgen.

6.3.2 Absatz 2

Keine Bemerkungen.

7. Kosten und Gebühren

ICT und ePower verlangen die Kosten für Überwachungsmassnahmen generell zu senken und die Gebührenverordnung anzupassen. Das setzt voraus, dass ein digitalisierter „End to End Prozess“ in den technischen Richtlinien des Dienstes abgebildet ist. Rechtssicherheit bedeutet, dass alle an einem System Beteiligten genau wissen, was von ihnen, wann ver-

langt wird. Sie beantragen, diesen Punkt vor der parlamentarischen Behandlung des Geschäftes zu regeln.

7.1. Artikel 30

[1] Die Kosten der für eine Überwachung notwendigen Einrichtungen und die Kosten der einzelnen Überwachung gehen zu Lasten der Personen, die Überwachungen nach diesem Gesetz durchführen.

[2] Die anordnende Behörde bezahlt dem Dienst eine Gebühr. Der Bundesrat setzt die Gebühren für die Dienstleistungen des Dienstes fest.

7.1.1 Absatz 1

Etliche Teilnehmer[126] begrüssen, vornehmlich mit Verweis auf die bestehende entschädigungslose Editionspflicht von Banken, Treuhändern, Versicherungen etc., den Wegfall der Entschädigung für die Anbieterinnen. Sie erachten eine Entschädigung als systemwidrig. ZH verweist überdies darauf, dass bei den Banken auch im Zusammenhang mit der Verhinderung der Geldwäscherei hohe Kosten anfallen, die sie selber tragen bzw. aus ihren Erträgen zahlen müssen. NW, SO, KSBS und SKG heben zudem hervor, dass grössere, gut organisierte Anbieterinnen mit den Fernmeldeüberwachungen in der Vergangenheit erheblich Geld verdient haben.

Eine grosse Anzahl Teilnehmer[127] spricht sich hingegen – aus verschiedenen, nachfolgend dargelegten Gründen – grundsätzlich gegen die vorgesehene Streichung der Entschädigung für die Durchführung von Überwachungsmassnahmen aus.

Die meisten dieser Teilnehmer[128] betonen, dass die Strafverfolgung eine staatliche Aufgabe und daher durch das Gemeinwesen zu tragen ist. Gemäss einigen Teilnehmern[129] vermag insbesondere das Argument, dass eine Entschädigung vor dem Hintergrund der Editionspflicht von Banken, Treuhändern, Versicherungen etc. systemwidrig ist, nicht zu überzeugen. Die SP betont, dass das, was von den Providern verlangt wird, weit mehr ist als die Herausgabe von ohnehin vorhandenen Daten oder Akten. DJS und gr.ch erachten den Vergleich mit der erwähnten Editionspflicht schon deswegen für abwegig, weil nicht spezielle Aufbewahrungs- und sonstige Mitwirkungspflichten für den Bereich des BÜPF postuliert werden müssten, wenn auf die StPO gestützte Editionsbegehren zur Verfügung stehen würden. Gemäss ISSS und MS widerspricht die Bestimmung zudem den anerkannten Grundsätzen der Beteiligung Privater an einem gegen Dritte geführten Strafverfahren, wie bspw. die Entschädigung von Zeugen und Sachverständigen. MS verweist zudem auf Artikel 434 StPO, der ausdrücklich vorsieht, dass Dritte Anspruch auf angemessenen Ersatz ihres nicht auf andere Weise gedeckten Schadens haben, wenn sie bei der Unterstützung von Strafbehörden Schaden erlitten haben. Diese Kosten sind schliesslich gemäss Artikel 422 ff. StPO Bestandteil der Verfahrenskosten, die am Ende zu Lasten des Verurteilten gehen.

---

126 ZH, LU, UR, OW, NW, SO, BL, SG, AG, NE, VD, GL, GR, TG, VS, JU, KKJPD, KKPKS, KSBS, SKG.

127 SP, CVP, FDP, SVP, GPS, PPS, DJS, gr.ch, RD, ISSS, MS, SIUG, SIMSA, INT, asut, Finecom, Orange, Swisscom, Sunrise, Colt, Verizon, Cablecom, SAV, SKS, Swisscable, CP, CCC, Sitrox, economiesuisse, IT(19), SWICO, hp, COG.

128 CVP, FDP SVP, GPS, asut, Finecom, Orange, Swisscom, Sunrise, Verizon, Cablecom, SAV, SKS Swisscable, SIUG, CP, CCC, Sitrox, PPS.

129 SP, DJS, gr.ch, Colt, Cablecom, RD.

Für eine grössere Teilnehmergruppe[130] hat die Entschädigung von Fernmeldedienstanbieterinnen auch einen disziplinierenden bzw. kostendämmenden Effekt, weil mit einer Entschädigungspflicht die Überwachungsanordnungen nicht zu überborden drohen.

Manche Teilnehmer[131] betonen, dass eine teure Infrastruktur und einiges Know-how notwendig ist, um den Anforderungen des Gesetzes Genüge zu tun und im Fall eines Auftrages durch den Dienst zeitgerecht die notwendigen technischen Massnahmen ergreifen zu können. Für kleinere Betriebe stellen schon die für die Überwachung erforderlichen Investitionskosten ein erhebliches Problem dar bzw. sind gemäss der GPS untragbar, da mit einem erheblichen Anstieg gerechnet werden muss. Colt sieht zudem den Grundsatz der Verhältnismässigkeit verletzt, wenn solche Ausrüstungen angeschafft und diese dann selten oder gar nie gebraucht werden. Für den Fall, dass die Investitionen trotzdem zu Lasten der Fernmeldedienstanbieterinnen gehen, dürfen diese gemäss Colt nicht gezwungen werden, Ausrüstungen zu beschaffen, solange keine Überwachung umgesetzt werden muss. Weiter ist es den Fernmeldedienstanbieterinnen zu überlassen, ob sie auch im wiederholten Überwachungsfall auf eine externe Ausrüstung allenfalls unter Kostenfolge zurückgreifen wollen. Die SP verweist darauf, dass die Auflagen marktverzerrend zugunsten der grossen Anbieter mit ohnehin schon fast monopolartiger Stellung sind. Sie postuliert daher für die Entschädigung der Anbieterinnen eine differenziertere Lösung, welche der wirtschaftlichen Tragbarkeit der Massnahmen, abhängig von der Unternehmensgrösse, Rechnung trägt.

Eine grössere Anzahl Teilnehmer[132] schlägt daher eine Formulierung vor, wonach die anordnende Behörde dem Dienst eine Gebühr bezahlt, welche die Entschädigungen zugunsten der Anbieterinnen enthält.

economiesuisse will unter Vorlage eines Formulierungsvorschlags, dass die Investitionen zwar durch die Anbieterinnen getragen werden, die Nutzung jedoch in Rechnung gestellt werden kann. Die CVP möchte die Kosten, welche die Provider zur Aufrüstung ihrer Systeme einsetzen, damit die geforderten Überwachungen durchgeführt werden können, entschädigen.

ZG befürchtet, dass wenn die Entschädigung für die Anbieterinnen wegfällt, der Bund irgendwie sicherstellen muss, dass die Anbieterinnen die Daten weiterhin rasch und zuverlässig zur Verfügung stellen.

7.1.2 Absatz 2

ZH, LU und ZG weisen darauf hin, dass obwohl die Kosten formell als Aufwand den Verurteilten oder kostenpflichtigen Personen überbunden werden können, diese in vielen Fällen den Verfahrensparteien nicht auferlegt werden können (Notsuche, Fahndung nach verurteilten Personen, bei Freisprüchen, in Rechtshilfeverfahren) oder unbezahlt bleiben, weil die betroffenen Personen zahlungsunfähig sind, und folglich zulasten der anordnenden Behörden gehen. Etliche Teilnehmer[133] beantragen, die Tarife der Verordnung vom 7. April 2004 über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs[134] adäquat anzusetzen bzw. erheblich zu senken. SZ verweist darauf, dass der Dienst

---

130 SVP, GPS, asut, Finecom, Orange, Swisscom, Sunrise, Verizon, Cablecom, SAV, SKS, Swisscable, SIUG, CP, CCC, Sitrox, PPS, economiesuisse.
131 SP, Colt, SIUG, SIMSA, INT, ISSS, PPS, GPS.
132 asut, Finecom, Orange, Swisscom, Sunrise, Verizon, Cablecom, Swisscable, IT(19), SWICO, hp, COG.
133 ZH, LU, ZG, BL, AG, TI, GL, GR, TG, VS, JU, SZ, OW, KKJPD, KKPKS.
134 SR 780.115.1

in diesem Zusammenhang nicht unnötige Schnittstellenfunktionen übernehmen soll wie bspw. die Überwachung der Aufbewahrungsdauer von Daten und die Vermittlung von Auskünften über Fernmeldeanschlüsse. LU und ZG beantragen, zur Gebührenverordnung zur gegebenen Zeit Stellung nehmen zu können. FR will, dass die Frage der Gebühren, welche die Kantone an den Dienst zu entrichten haben, auf der Basis einer noch durchzuführenden Evaluation zu prüfen ist. VD vermutet, dass die Beibehaltung der Gebühren beim Dienst zu einem Kostenüberschuss führen dürfte. NE verlangt zu prüfen, ob die Gebühren für die anordnenden Behörden nicht ganz gestrichen werden können. Gemäss der SP ist darauf zu achten, dass die Gebühren für die Strafverfolgungsbehörden nicht prohibitiv hoch sind, damit wichtige Ermittlungen nicht an zu hohen Fallpauschalen scheitern.

8. Strafbestimmungen

8.1. Artikel 31 Übertretungen

[1] Mit Busse bis zu 100 000 Franken wird bestraft, wer vorsätzlich:

a. den Weisungen des Dienstes nicht Folge leistet;

b. der Pflicht zur Aufbewahrung der Daten nach Artikel 19 Absatz 2 und Artikel 23 nicht nachkommt.

[2] Versuch und Gehilfenschaft sind strafbar.

[3] Handelt der Täter fahrlässig, so beträgt die Busse bis zu 40 000 Franken.

[4] Artikel 102 Absätze 1, 3 und 4 StGB und 112 StPO sind sinngemäss anwendbar. Die Busse beträgt höchstens 1 Million Franken.

SO sowie CP sind mit der Strafbestimmung grundsätzlich einverstanden. Für CP setzt dies jedoch voraus, dass das Gesetz eine Entschädigung sowie eine kostenfreie Zertifizierung für die Verpflichteten vorsieht.

GPS und SKS erachten die Strafbestimmung als eindeutig zu strikt. Dies insbesondere deshalb, weil diejenigen, welche Überwachungen durchführen, kaum Mittel haben, sich zu wehren. Aufgrund dessen und der Tendenz immer mehr Überwachungen durchzuführen, führt die Strafbestimmung dazu, dass die Fernmeldedienstanbieterinnen willkürlich den Anordnungen unterworfen sind. Zudem wird das Strafmass gerade kleinere Provider existenziell bedrohen. Sie verlangen daher eine deutlich abgeschwächte Bestimmung.

Diverse Teilnehmer[135] weisen in diesem Zusammenhang auf die unklar geregelten Pflichten hin. Die FDP hält vor diesem Hintergrund die Strafbestimmung zumindest für heikel. SIMSA ist der Meinung, dass eindeutige Tatbestandsmerkmale fehlen, welche eine strafrechtliche Sanktion rechtfertigen. Gemäss einigen Teilnehmern[136] verletzt die Bestimmung daher nicht nur das Bestimmtheitsgebot, sondern stellt insofern eine Zumutung dar, als aufgrund von Artikel 15 Buchstabe a VE-BÜPF der Dienst selbst dann noch Weisungen zu erteilen und Verfügungen zu erlassen hat, wenn er selber nicht hinter diesen stehen kann.

Orange und Colt halten es zudem für nicht sachgerecht, dass auch natürliche Personen der Bestimmung unterliegen. Sie beantragen daher, den Adressatenkreis des BÜPF und entsprechend auch die Strafbestimmungen auf juristische Personen zu beschränken.

---

135 FDP, SIMSA, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

136 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

8.1.1 Absatz 1

Etliche Teilnehmer[137] sprechen sich für eine Verschärfung der Bestimmung aus. OW zweifelt zumindest an der beabsichtigten Wirkung der Bestimmung. Für NW und KSBS ist die Ausgestaltung der Bestimmung als Übertretung angesichts der im Fernmeldeverkehr generierten Gewinne im Verhältnis zum Überwachungsaufwand unangemessen und nicht abschreckend, da die für eine Pflichtverletzung vorgesehene Busse (CHF 100'000.-) durch damit gesparte Aufwendungen in gewissen Fällen mehr als nur neutralisiert wird. Einige Teilnehmer[138] verlangen daher, den Betrag von CHF 100'000.- zu erhöhen. Eine Mehrheit dieser Teilnehmer[139] schlägt eine Erhöhung auf CHF 1 Million vor.

Buchstabe a

Acht Teilnehmer[140] erachten die Formulierung „wer vorsätzlich den Weisungen des Dienstes nicht Folge leistet“ unter Hinweis auf das Bestimmtheitsgebot von Artikel 1 StGB für rechtsstaatlich bedenklich.

Buchstabe b

VD, BL und AG möchten die Bestimmung auch auf Verstösse gegen Artikel 20 VE-BÜPF angewendet wissen; AG zusätzlich auf Artikel 22 VE-BÜPF.

8.1.2 Absatz 2

UNIZH erachtet die Strafbarkeit von Versuch und Gehilfenschaft als systemwidrig, da es sich um Übertretungen, und nicht um Vergehen oder Verbrechen handelt.

8.1.3 Absätze 3 und 4

Keine Bemerkungen.

8.2. Artikel 32 Gerichtsbarkeit

Die Verfolgung und Beurteilung der Straftaten nach Artikel 31 obliegt den Kantonen.

KKPKS begrüsst die kantonale Zuständigkeit ausdrücklich, da sie dem Grundsatz folgt, wonach die Kantone für die Verfolgung und Beurteilung einer Straftat zuständig sind.

Einige Teilnehmer[141] wollen für die örtliche Zuständigkeit eine Regelung vorsehen, die darauf abstellt, wo die fehlbare Anbieterin ihre Dienstleistung erbringt. Erstreckt sich diese auf mehrere Kantone, so ist eine Bundesgerichtsbarkeit vorzusehen.

Gemäss BL und KSBS ist nicht einzusehen, warum die Gerichtsbarkeit bei den Kantonen liegen soll. Sie beantragen eine generelle Bundeszuständigkeit. BL verweist darauf, dass es in Artikel 31 VE-BÜPF um Übertretungen in Bereichen geht, in denen der Dienst und damit grundsätzlich der Bund zuständig ist. Hinzu kommt, dass die fraglichen Verfehlungen der

---

137 ZH, LU, AG, GL, GR, TG, VS, JU, NW, KKJPD, KSBS.
138 ZH, AG, LU, GL, GR, TG, VS, JU, KKJPD.
139 AG, LU, GL, GR, TG, VS, JU, KKJPD.
140 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
141 ZH, LU, SG, GL, GR, TG, VS, JU, KKJPD.

Anbieterinnen in aller Regel mehrere Kantone betreffen. Gemäss KSBS ist gegen Verfügungen des Dienstes die Beschwerde nach den Regeln über die Bundesrechtspflege zulässig, sodass auch für Strafverfahren die Regeln über das Verwaltungsstrafrecht anwendbar sein sollten.

9. Aufsicht und Rechtsschutz

9.1. Artikel 33 Aufsicht

[1] Der Dienst wacht über die Einhaltung der Gesetzgebung betreffend die Überwachung des Post- und Fernmeldeverkehrs.

[2] Stellt er eine Rechtsverletzung fest, so kann er sinngemäss die Massnahmen nach Artikel 58 Absatz 2 Buchstabe a des Fernmeldegesetzes vom 30. April 1997 ergreifen. Er kann vorsorgliche Massnahmen anordnen.

Gemäss mehreren Teilnehmern[142] steht die Formulierung „Der Dienst wacht über die Einhaltung der Gesetzgebung“ in Absatz 1 in Widerspruch zu Artikel 15 Buchstabe a VE-BÜPF, wonach der Dienst die rechtliche Korrektheit einer Überwachungsanordnung eben gerade nicht prüfen darf. Artikel 33 VE-BÜPF ist demnach so zu verstehen, dass der Dienst nicht die Einhaltung der Gesetzgebung generell sicherstellen soll, sondern nur einseitig die Einhaltung der Gesetzesbestimmungen durch die Fernmeldedienstanbieterinnen. Darauf deutet auch der Wortlaut von Absatz 2 hin. Der Dienst sollte an sich die Rolle der dazwischen stehenden Verwaltung einnehmen, das Gesetz anwenden und in strittigen Fällen auch entscheiden, was er aber zurzeit nicht kann. Er sieht sich jedoch nicht in dieser Rolle, sondern handelt je länger je mehr so, wie wenn er selber eine Überwachungsinstanz wäre. Der Dienst beschränkt sich in den technischen Richtlinien sowie in den organisatorischen und administrativen Vorschriften, welche er als reine Ausführungsvorschriften zu erlassen hat, nicht darauf zu regeln, wie die Fernmeldedienstanbieterinnen gewisse Daten zu liefern haben, sondern erlässt immer mehr auch Vorschriften, welche regeln, was sie alles zu leisten haben. Weiter wird bemängelt, dass mitunter in einem gewissen Übereifer gar Leistungen vorsorglich verlangt werden, welche weiter gehen als die Begehren der Untersuchungsbehörden. Diese Entwicklung eines sich verselbständigenden und durch keine Rechtmittel- oder Aufsichtsinstanz kontrollierbaren Dienstes wird als besorgniserregend empfunden. Die Teilnehmer, die sich zu Artikel 33 VE-BÜPF äussern, kommen zum Schluss, dass vor dem Hintergrund des insgesamt unklaren und nicht zufriedenstellenden Gesetzes Artikel 33 zu überdenken ist, da der Dienst selber sich nicht als Hüter des Rechts sieht, sondern eher als Instanz, welche versucht, soviel Überwachung wie irgendwie möglich sicherzustellen. Vor diesem Hintergrund ist er als Aufsichtsbehörde nicht geeignet.

Cablecom kritisiert, dass mit der vorliegenden Formulierung der Dienst seine eigene Tätigkeit überwachen muss. Sie schlägt vor, das Bundesamt für Kommunikation (BAKOM) als Aufsichtsbehörde einzusetzen.

KFG will mit Verweis auf die Fichenaffäre die Kontrolle des Dienstes sichergestellt wissen. Es beantragt die Einführung einer Kontrollstelle, welche regelmässig die Ausgaben des Dienstes sowie die Verhältnismässigkeit und die Rechtmässigkeit der angeordneten Massnahmen kontrolliert.

[142] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, SWICO, hp, COG.

9.2. Artikel 34 Rechtsschutz

[1] Verfügungen des Dienstes unterliegen der Beschwerde nach den allgemeinen Bestimmungen über die Bundesrechtspflege.

[2] Mit der Beschwerde gegen die Verfügung des Dienstes kann die Rechtmässigkeit der Anordnung der Überwachung nicht geltend gemacht werden. Dagegen kann geltend gemacht werden, die Überwachung könne aus technischen oder aus organisatorischen Gründen nicht durchgeführt werden.

9.2.1 Absatz 1

Keine Bemerkungen.

9.2.2 Absatz 2

Neun Teilnehmer[143] betonen, dass die vorgeschlagene Bestimmung einem praktischen Bedürfnis entspricht. Gemäss KSBS ist der generelle Ausschluss der Rechtmässigkeitsprüfung jedoch zu weitgehend. Die Fernmeldedienstanbieterinnen sollen die Möglichkeit haben zu rügen, dass angeordnete Massnahmen gesetzlich nicht vorgesehen sind, da die Genehmigungsbehörde nicht über die nötigen technischen Kenntnisse verfügt.

Eine Vielzahl von Teilnehmern[144] verlangt, dass entgegen dem vorgeschlagenen Absatz 2 generell die Möglichkeit bestehen muss, die Rechtmässigkeit einer Überwachungsanordnung überprüfen zu lassen.

Einige Teilnehmer[145] weisen darauf hin, dass eine unrechtmässig angeordnete Überwachung, bspw. die Verfolgung einer Straftat, welche nicht im Katalog von Artikel 269 Absatz 2 Buchstabe a StPO vorgesehen ist oder eine Überwachungsmassnahme, welche gesetzlich nicht vorgesehen ist, nicht nur die Rechte der betroffenen Person beschlägt, sondern auch ein öffentliches Interesse daran besteht, eine fehlerhafte Anordnung vor dem Hintergrund der Schwere des Grundrechtseingriffes rügen zu können. Schliesslich verweisen sie darauf, dass in dringenden Fällen die Strafverfolgungsbehörden die Überwachung während des Beschwerdeverfahrens im Sinne einer vorsorglichen Massnahme beantragen können bzw. einer allfälligen Beschwerde die aufschiebende Wirkung entzogen werden kann.

Für BE ist es stossend, wenn sich die Personen, welche vom Dienst fälschlicherweise als zur Überwachung Verpflichtete bezeichnet werden, sich nicht dagegen zur Wehr setzen können.

Acht Teilnehmer[146] verweisen auf den Umstand, dass gemäss den allgemeinen Regeln die Beschwerdeinstanz keine umfassendere Kognition als die erste Instanz haben kann. Da der Dienst keine materiellen Prüfungskompetenzen hat bzw. die Überwachungsanordnungen einfach übernimmt, bedeutet dies, dass auch die Beschwerdeinstanzen nicht prüfen werden, was bereits die Vorinstanz nicht geprüft hat. Im Ergebnis führt dies dazu, dass die Verfügungen des Dienstes gar nicht anfechtbar sind. Sie fordern daher entsprechende Prüfungskompetenzen des Dienstes (vgl. auch die Ausführungen in III. Ziff. 3.2.1 zu Art. 15 Bst. a VE-BÜPF).

Gemäss Cablecom widerspricht Absatz 2 den Bestimmungen der Bundesrechtspflege und

---

143 LU, NW, GL, GR, TG, VS, JU, KKJPD, KSBS.

144 ZG, BE, BL, AR, FDP, SP, economiesuisse, SSV, privatim, SSV, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom, Swisscable, SKS, SIUG, VSPF, SWICO, hp, COG, IT(19), ISSS.

145 ZG, privatim, SP, FDP, economiesuisse, SSV.

146 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SKS.

ist daher ersatzlos zu streichen. Swisscable hält fest, dass ein Pflichtenheft nichts nützt, wenn es keine Grundlage gibt, um die darin festgehaltenen Rechte und Pflichten nötigenfalls einzufordern. Deshalb müssen im Sinne der Rechtssicherheit künftig Rechtsmittel gegen überbordende behördliche Anordnungen bestehen. Dies ist weder im heutigen Gesetz noch im Revisionsvorschlag gegeben und führt zu einer fehlenden Rechtssicherheit.

Eine grössere Teilnehmergruppe[147] schlägt folgende Neuformulierung vor: „Mit der Beschwerde gegen die Verfügung des Dienstes kann nicht geltend gemacht werden, die Anordnung einer Überwachung sei im konkreten Einzelfall unverhältnismässig oder die anordnende Behörde habe ihr Ermessen unrichtig ausgeübt".

BL weist zudem darauf hin, dass wenn die technische und organisatorische Machbarkeit gemäss Absatz 2 ein Beschwerdegrund darstellt, sie folgerichtig vorher geprüft werden muss. Artikel 15 Buchstabe a VE-BÜPF ist entsprechend zu ergänzen (vgl. vorne III. Ziff. 3.2.1 zu Art. 15 Bst. a VE-BÜPF).

AG verlangt, eine andere Kontrollmöglichkeit vorzusehen, falls die Anbieterinnen die fehlende Rechtmässigkeit einer Überwachungsanordnung nicht geltend machen können. Gemäss OW soll die Möglichkeit bestehen, überprüfen zu lassen, ob der Dienst seine Aufgaben gemäss Artikel 15 VE-BÜPF wahrgenommen hat. Es ist unklar, ob dies vorgesehen ist.

10. Schlussbestimmungen

10.1. Artikel 35 Vollzug

Der Bundesrat und im Rahmen ihrer Zuständigkeit die Kantone erlassen die Vollzugsvorschriften.

Keine Bemerkungen.

10.2. Artikel 36 Aufhebung und Änderung bisherigen Rechts

Die Aufhebung und die Änderung bisherigen Rechts werden im Anhang geregelt.

Bemerkungen zu vorgesehenen Änderungen bisherigen Rechts finden sich nachfolgend unter Ziffer 11.

10.3. Artikel 37 Übergangsbestimmung

Für Überwachungen, die vor dem Inkrafttreten dieses Gesetzes angeordnet worden sind, gilt das neue Recht.

Mehrere Teilnehmer[148] aus der Fernmeldedienstbranche fordern angemessene Übergangsfristen für die technische Umsetzung. Sie schlagen folgende Formulierung vor: „Für Überwachungen, die vor dem Inkrafttreten dieses Gesetzes angeordnet worden sind, gilt das *alte* Recht. *Unter dem alten Recht angeordnete Überwachungen dürfen im Zeitpunkt des Inkrafttretens des neuen Rechts nur fortgeführt werden, sofern sie auch nach neuem Recht zulässig sind*". Da der sachliche wie auch der persönliche Anwendungsbereich erweitert wird, beantragen switch und switchplus eine angemessene Übergangsfrist für Personen, die neu zur Durchführung von Überwachungsmassnahmen verpflichtet werden. Sie schlagen deshalb

147 economiesuisse, SWICO, hp, COG, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, IT(19).

148 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

einen neuen Absatz 2 vor: *„Personen, die neu aufgrund des erweiterten sachlichen oder persönlichen Anwendungsbereiches der Pflicht unterstehen, Überwachungsmassnahmen umzusetzen, haben diese innerhalb eines Jahres seit in Kraft Setzung dieses Gesetzes umzusetzen".*

Für BL ist die Bestimmung missverständlich formuliert. Er vermutet, dass bei Inkrafttreten des Gesetzes das neue Recht für alle *laufenden* Überwachungen gelten soll, die vor Inkrafttreten angeordnet wurden, und nicht rückwirkend für alle Überwachungen, die vor Inkrafttreten des Gesetzes angeordnet wurden.

Im selben Zusammenhang wirft SZ die Frage auf, ob die Meldung nach Artikel 11 VE-BÜPF nachgeholt werden muss, wenn das neue Recht auch für abgeschlossene Überwachungen gelten soll.

Für Cablecom ist die in diesem Artikel beschriebene rückwirkende Inkraftsetzung des neuen Rechts bei bereits bestehenden Überwachungen fragwürdig, da bspw. die rückwirkenden Daten eventuell noch gar nicht zwölf Monate zurück verfügbar sein werden. Sie schlägt folgende Formulierung vor: „Für Überwachungen, die vor dem Inkrafttreten dieses Gesetzes angeordnet worden sind, gilt das *alte* Recht. *Für Überwachungen, die nach dem Inkrafttreten dieses Gesetzes angeordnet werden, gilt während einer Übergangszeit von 6 Monaten das alte Recht"*.

Gemäss MS widerspricht die Bestimmung dem Bestimmtheitsgebot, wonach der Bürger wissen muss, welche Konsequenzen mit seinem Verhalten verbunden sind. Deshalb darf das neue BÜPF nur für neue Überwachungen gelten.

Andere Teilnehmer[149] vermuten ein Versehen: Gemeint ist wohl, dass für laufende Überwachungen, die vor Inkrafttreten *verfügt* wurden, ab Inkrafttreten die Regeln dieses Gesetzes gelten. Damit erachten sie jedoch die Bestimmung mit Verweis auf den erläuternden Bericht für unnötig.

10.4. Artikel 38 Referendum und Inkrafttreten

[1] Dieses Gesetz untersteht dem fakultativen Referendum.
[2] Der Bundesrat bestimmt das Inkrafttreten.

Keine Bemerkungen.

11. Aufhebung und Änderung bisherigen Rechts (Anhang; Art. 36 VE-BÜPF)

11.1. Strafprozessordnung vom 5. Oktober 2007 (StPO)[150]

11.1.1 Artikel 269 Absatz 2 Buchstabe a StPO Voraussetzungen

[2] Eine Überwachung kann zur Verfolgung der in den folgenden Artikeln aufgeführten Straftaten angeordnet werden:

[149] GL, GR, TG, VS, JU, KKJPD, KSBS.
[150] AS 2010 1881; in Kraft per 1.1.2011.

a. *StGB: Artikel 111–113; 115; 118 Ziffer 2; 122; 127; 129; 135; 138–140; 143; 144 Absatz 3; 144bis Ziffer 1 Absatz 2 und Ziffer 2 Absatz 2; 146–148; 156; 157 Ziffer 2; 158 Ziffer 1 Absatz 3 und Ziffer 2; 160; 161; 163 Ziffer 1; 180; 181–185; 187; 188 Ziffer 1; 189–191; 192 Absatz 1; 195; 197; 220; 221 Absätze 1 und 2; 223 Ziffer 1; 224 Absatz 1; 226; 227 Ziffer 1 Absatz 1; 228 Ziffer 1 Absätze 1–4; 230bis; 231 Ziffer 1; 232 Ziffer 1; 233 Ziffer 1; 234 Absatz 1; 237 Ziffer 1; 238 Absatz 1; 240 Absatz 1; 242; 244; 251 Ziffer 1; 258; 259 Absatz 1; 260bis–260^{quinquies}; 261bis; 264–267; 271; 272 Ziffer 2; 273; 274 Ziffer 1 Absatz 2; 285; 301; 303 Ziffer 1; 305; 305bis Ziffer 2; 310; 312; 314; 317 Ziffer 1; 319; 322ter, 322^{quater} und 322^{septies};*

Zwölf Teilnehmer[151] begrüssen ausdrücklich die Ausdehnung des Straftatenkatalogs auf Artikel 220 StGB (Entziehen von Unmündigen).

Gemäss SGB schiesst der VE-BÜPF über das Ziel hinaus. So ist der Deliktskatalog zu ausufernd. Bei Tatbeständen wie Sachbeschädigung mit hohem Schaden oder Störung des Eisenbahnverkehrs bspw. „Government Software“ (oft auch „Bundestrojaner“ genannt) einsetzen zu können, ist klar nicht gerechtfertigt.

SIUG und VSPF halten fest, dass der abschliessende Straftatenkatalog bereits heute nicht gilt, falls die Straftat über das Internet begangen worden ist. Gemäss Artikel 20 Absatz 3 VE-BÜPF müssen Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, dem Dienst alle Angaben machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen. Sie fordern, dass die Ausdehnung auf zusätzliche Anlassstraftaten kritisch hinterfragt wird. Zudem hat der Straftatenkatalog auch für den Zugriff auf Daten aus der Vorratsdatenspeicherung zu gelten.

KFG sieht keine Rechtfertigung für die Ausdehnung des Straftatenkatalogs auf Artikel 220 StGB. Der Tatbeststand entspricht keiner „schweren Straftat“ und ist daher zu streichen.

ESBK möchte den Straftatenkatalog mit Artikel 55 Absatz 1 Buchstabe a des Bundesgesetzes vom 18. Dezember 1998 über Glücksspiele und Spielbanken (SBG)[152] ergänzen. Zur Begründung führt sie an, dass immer mehr illegale Spielbanken im Internet betrieben werden. Eine effiziente Strafverfolgung dieser Spielbanken bedingt neue Mittel der Ermittlung. Um die notwendigen Beweismittel sicherzustellen, ist es unerlässlich in das Netz dieser illegalen Spielbanken eindringen zu können und zwar in einer Weise wie dies bei einer Hausdurchsuchung in der realen Welt der Fall ist. In der realen Welt ist eine Hausdurchsuchung gestützt auf Artikel 56 SBG möglich, nicht aber mangels Überwachungsmassnahmen im Sinne des BÜPF in der virtuellen Welt. Solche Überwachungen sind aber bei der Strafverfolgung von im Internet betriebenen, illegalen Spielbanken unerlässlich. ESBK ist der Auffassung, dass Artikel 55 Absatz 1 SBG die Kriterien erfüllt, um in den Katalog von Artikel 269 Absatz 2 StPO aufgenommen zu werden, da es sich um ein Vergehen von besonderer Schwere handelt und es immer mehr mittels Internet begangen wird.

11.1.2 Artikel 270bis StPO Abfangen und Entschlüsselung von Daten *(neu)*

[1] Sind bei einer Überwachung des Fernmeldeverkehrs die bisherigen Massnahmen erfolglos geblieben oder wären andere Überwachungsmassnahmen aussichtslos oder würden die Überwachung unverhältnismässig erschweren, so kann die Staatsanwaltschaft auch ohne Wissen der überwachten Person das Einführen von Informatikprogrammen in ein Datensystem anordnen, um die Daten abzufangen und zu lesen. Die Staatsanwaltschaft gibt in der Anordnung der Überwachung an, auf welche Art von Daten sie zugreifen will.

[2] Die Anordnung bedarf der Genehmigung durch das Zwangsmassnahmengericht.

Vierzehn Teilnehmer[153] begrüssen die neue Bestimmung. Davon weisen einige Teilneh-

151 LU, ZH, OW, NW, GL, GR, TG, VS, JU, KKPKS, KKJPD, KSBS.
152 SR 935.52
153 ZH SZ, NW, OW, GL, GR, TG, VS, JU, KKJPD, KKPKS, KSBS, SPICT, SSV.

mer[154] auf die sich stark ausbreitende Verschlüsselungsproblematik hin. SSV spricht sich überdies gegen die zusätzliche Voraussetzung der sogenannten „doppelten Subsidiarität“ aus, welche zu hoch angesetzt und wenig praktikabel ist. Der Einsatz von „Government Software“ (oft auch „Bundestrojaner“ genannt) stellt keine weitergehendere Massnahme dar als andere Überwachungsmassnahmen, insbesondere auch Artikel 280 StPO. Es überzeugt gemäss SSV nicht, dass unter dem Stichwort „Subsidiarität“ vor dem Abhören der Internettelefonie eines Beschuldigten zuerst dessen Fest- und Mobiltelefone abgehört werden müssen. Die obligate Prüfung der Verhältnismässigkeit im Rahmen von Artikel 269 StPO reicht aus.

Zehn Teilnehmer[155] lehnen die Einführung von Informatikprogrammen in ein fremdes Datensystem gänzlich ab, eine weitere Teilnehmergruppe[156] bringt Vorbehalte an.

GPS, DJS, gr.ch, SKS und SIUG weisen zunächst darauf hin, dass das Einschleusen von Informatikprogrammen nichts anderes ist, als das Einbauen von Schaden anrichtender Software in die Computer von Privatpersonen. Damit verbunden ist ein massiver Eingriff in die Privatsphäre der Betroffenen. Denn mit der betreffenden Überwachungsmethode kann auf das gesamte Datenverarbeitungssystem (Fotos, Briefe, Passwörter, Mikrofon etc.) zugegriffen werden. Sie erachten es als unverständlich bzw. geradezu bezeichnend, dass nirgends auf das Grundsatzurteil des deutschen Bundesverfassungsgericht vom Februar 2008[157] Bezug genommen wird, worin festgestellt wird, dass diese Methode das sich aus dem allgemeinen Persönlichkeitsrecht ergebende Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verletzt. Das deutsche Bundesverfassungsgericht will diese „Online-Durchsuchung“ nur für den Schutz „überragend wichtiger Rechtsgüter“ zulassen. Darunter fallen die wichtigen Rechtsgüter wie Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Ein solches Grundrecht ergibt sich gemäss den erwähnten Teilnehmern aus Artikel 10 BV.

SIUG weist zusätzlich auf den deutschen Bundesgerichtshof hin, der eine solche Massnahme nach geltendem Bundesrecht für Zwecke der Strafverfolgung als unzulässig betrachtet. Er begründete seine Entscheidung[158] u.a. damit, dass diese ohne Wissen der betroffenen Person stattfindet, während das Gesetz für eine herkömmliche Durchsuchung die Anwesenheit von Zeugen bzw. des Inhabers des Durchsuchungsobjektes vorsieht. Gemäss SIUG stellt Artikel 245 StPO (Durchführung der Hausdurchsuchung) eine entsprechende Bestimmung dar.

GPS, DJS, gr.ch und SKS kritisieren ferner, dass die Durchsuchung des Computers nicht etwa auf bestimmte Programme – wie etwa das Mailprogramm – beschränkt werden sollte. Eine lediglich thematische Eingrenzung setzt jedoch zunächst die Durchsuchung der gesamten Festplatte voraus, um die angeblich relevanten Dateien zu finden. Auch die Argumentation der „doppelten Subsidiarität“ vermag nicht zu überzeugen, weil schon die übliche Telekommunikationsüberwachung an die Voraussetzung gebunden ist, dass andere Methoden erfolglos waren oder aussichtslos sind. Tatsächlich heisst das nichts anderes, als dass die Untersuchungsbehörden und das genehmigende Gericht letztlich bei einem Fehlschlag der üblichen Telekommunikationsüberwachung fast automatisch die Grundlage für ein weiteres

---

154 ZH, GL, GR, TG, VS, JU, KKJPD, KKPKS.
155 GPS, DJS, gr.ch, Cablecom, CCC, SKS, SIUG, KFG, PPS, ISSS.
156 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, ZH, BL, AR, LU, SP, SIUG, privatim, economiesuisse, Swisscable.
157 BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333).
158 BGH, Beschluss vom 31.1.2007 – StB 18/06.

Eindringen in den jeweiligen Computer haben. Ein besonderer Deliktkatalog ist zudem auch nicht vorgesehen, weil gemäss dem erläuternden Bericht alle Delikte, welche die „normale“ Telefonüberwachung zulassen könnten, „geeignet sind, im konkreten Fall eine solche Schwere zu erreichen, welche die Anwendung der Überwachungsmassnahme rechtfertigt“. Worin die hier geforderte besondere Schwere bestehen soll, lässt der Bericht indessen offen. Dies macht aus Sicht der erwähnten Teilnehmer deutlich, dass es darum geht, eine möglichst leicht handhabbare Gesetzesgrundlage für eine Methode zu erhalten, die technisch möglich ist. Neben der Frage des Rechtsschutzes stellt sich auch die Frage nach der zu erwartenden Effizienz dieses Mittels. Es ist zu erwarten, dass diejenigen, welche mit derlei Massnahmen überwacht werden sollen, ausweichen. Sie können Vorsichtsmassnahmen treffen oder andere Kommunikationskanäle als ihren eigenen Computer nutzen.

GPS, SKS, KFG und PPS bringen die Befürchtung zum Ausdruck, dass die Methode des Eindringens in private Computer eine Sicherheitslücke schafft, die irgendwann auch von Verbrechern genutzt werden kann. So ist es möglich, dass die Quellsoftware des staatlichen „Bundestrojaners“ im Netz auftaucht und von Verbrechern missbraucht wird.

Gemäss KFG verändert jede Software, welche auf einem System installiert wird, das System selber und kann die Sicherheit des Rechners und des gesamten Netzwerkes gefährden. In diesem Zusammenhang stellt sich zudem das Problem, wie eine Behörde beweisen will, dass das gefundene Beweisstück nicht vom „Bundestrojaner“ selbst hochgeladen oder versendet wurde. Denn so wie Daten gelesen werden können, können sie auch abgefangen, geschrieben oder verändert werden. Eine Beweisführung wird damit verunmöglicht.

PPS weist darauf hin, dass die Interaktion des Überwachungstrojaners mit anderen Elementen des Datensystems vorgängig nicht exakt bestimmt werden kann. Es stellt sich somit die Frage, wer für den Schaden eines „Bundestrojaners“ aufkommt.

Für CCC ist es gewagt, dass der Staat selber trojanerartige Software einsetzen will, welche in der Schweiz nicht in Umlauf gebracht werden darf. Zudem müssen unbescholtene Dritte mit kompromittierten Rechnern rechnen, denn je nach Kommunikationsnetz werden Dritte miteinbezogen. Der staatliche Einsatz von „Trojanersoftware“ ist anmassend und die Wahrscheinlichkeit, dass (unschuldige) Dritte mit überwacht werden, zu gross.

Auch SIUG weist ausführlich auf diverse technische Schwierigkeiten und Gefahren bei der Installation derartiger Software auf dem gewünschten Rechner hin. Zudem ist SIUG der Ansicht, dass das Risiko einer Verbreitung der Schadsoftware an einen grösseren Personenkreis, auch im Ausland, durch Schweizer Behörden ausgelöst, nicht auf sich genommen werden kann.

Sieben Teilnehmer[159] vermissen eine Regelung betreffend Modalitäten der Löschung der Programme von den betroffenen Systemen. Gemäss ZH, BL, ZG und SP ist auch nicht geregelt, welche Anforderungen in Bezug auf die Sicherheit sowohl der eingesetzten Programme als auch deren Anbieter gelten.

Gemäss FDP, economiesuisse und Swisscable sind die Auswirkungen von „Bundestrojanern“ schwer abschätzbar. Letztere fordern, dass nur Programme eingesetzt werden dürfen, die sich auf die Überwachung der genehmigten Bereiche beschränken und die keine anderen Softwareprogramme in ihrer Funktionalität beeinträchtigen. Weiter muss der Bund für Schäden haften. Beide schlagen konkrete Formulierungen vor.

---

[159] ZH, BL, AR, ZG, SP, SIUG, privatim.

Für die SVP sind entsprechende Eingriffe in die Privatsphäre von Personen und Unternehmen ultima ratio. Anforderungen und Kriterien sind dementsprechend hoch anzusetzen. Die Bestimmung erfüllt die Anforderungen nicht. Sie beantragt Straftatbestände, welche einen Einsatz solcher Instrumente erlauben, im Gesetz explizit festzuhalten. Die CVP meldet gegenüber dem Einsatz von Methoden, die einen grossen „Beifang" verursachen oder ein grösseres Risiko für unbeteiligte Dritte darstellen, gewisse Vorbehalte an.

Auch privatim verweist auf die Schwere des Eingriffs. Aus Sicht der BV hat der Staat in den Informatiksystemen der Rechtsunterworfenen grundsätzlich nichts zu suchen. Eine gesetzliche Grundlage, welche das unbemerkte Einschleusen eines Informatikprogramms in private Informatiksysteme erlaubt, muss daher in Bezug auf die Bestimmtheit den höchsten Ansprüchen genügen. Dies erfüllt die vorliegende Bestimmung nicht in jeder Beziehung. privatim und die SP fordern mit Blick auf das deutsche Bundesverfassungsgericht[160], dass der Deliktskatalog von Artikel 269 Absatz 2 Buchstabe a StPO auf einige wenige, schwerste, gegen Leib und Leben bzw. den Bestand des Staates gerichtete Delikte beschränkt wird. Auch BS und FR beantragen generell eine Einschränkung des Deliktskatalogs für den Einsatz von „Bundestrojanern". FR will derartige Eingriffe sodann nur unter sehr strengen Voraussetzungen angewendet wissen, d.h. nur bei konkreten Indizien einer unmittelbaren Gefahr für ein wesentliches Rechtsgut, und nicht bloss bei einem dringenden Verdacht gemäss Artikel 269 Absatz 1 Buchstabe a StPO. Die Bundesbehörden sollen gemäss FR zudem den Umfang derartiger Massnahmen im Verhältnis zu der Gesamtheit der Überwachungsmassnahmen abschätzen.

BE beantragt eine gesetzliche Klarstellung, ob mit den „Bundestrojanern" eine „elektronische Hausdurchsuchung" erlaubt ist oder nur der Fernmeldeverkehr erhoben werden darf**.**

MS stellt fest, dass mit der Bestimmung jegliche Art von Daten erfasst werden kann und beantragt deshalb, sie in Artikel 280 StPO zu integrieren. Zudem geht aus dem Wortlaut nicht klar hervor, dass die Bestimmung auf den Deliktskatalog von Artikel 269 Absatz 2 Buchstabe a StPO beschränkt ist.

UNISG und UNIZH haben grundsätzliche Bedenken zu dieser Art von Überwachung und verweisen auf die besondere Herausforderung organisatorischer und personeller Natur, welche diese Art von Überwachung mit sich bringt.

ISSS legt Wert auf die Feststellung, dass der Einsatz solcher Informatik-Programme geeignet sein wird, das in der Schweiz erreichte Niveau von Datenschutz und Informationssicherheit erheblich zu beeinträchtigen.

11.1.3 Artikel 270ter StPO Einsatz von Ortungsgeräten *(neu)*

[1] Die Staatsanwaltschaft kann den Einsatz von Geräten durch die Polizei anordnen, mit denen spezifische Kennzeichen von Mobiltelefongeräten und ihr Standort ermittelt werden können. Die Geräte müssen vorgängig von der zuständigen Behörde bewilligt worden sein.

[2] Die Anordnung bedarf der Genehmigung durch das Zwangsmassnahmengericht.

Eine grössere Anzahl Teilnehmer[161] begrüsst die neue Bestimmung grundsätzlich.

Einige dieser Teilnehmer[162] beantragen statt von „Mobiltelefongeräten" von „mobilen Kommunikationsmitteln" zu sprechen, um neue technologische Entwicklungen (bspw. Notebooks mit SIM-Karten) abzudecken. KKPKS schlägt zudem vor, einen neuen Absatz 3 vorzusehen,

[160] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333).
[161] ZH, LU, SZ, OW, NW, SG, BL, GL, GR, TG, VS, JU, KKJPD, KKPKS, KSBS.
[162] ZH, LU, KKJPD, GL, GR, TG, VS, JU, KKPKS.

welcher den Einsatz der Ortungsgeräte für die Notsuche vorsieht. Andere[163] verweisen darauf, dass es sich bei den erwähnten Ortungsgeräten um technische Überwachungsgeräte handelt, die von der Polizei, und nicht vom Dienst eingesetzt werden. Sie beantragen daher, die Bestimmung in Artikel 280 StPO einzuordnen und ein entsprechendes Genehmigungsverfahren vorzusehen.

GPS, DJS, gr.ch, SKS und SIUG lehnen die Bestimmung ab und verweisen darauf, dass der Einsatz dieser sogenannten „IMSI[164]-Catcher" nicht nur einen bestimmten Mobilfunkteilnehmer betrifft, sondern dass bei allen Personen im Umkreis – verdächtige und unverdächtige – der Mobilfunkverkehr umgeleitet bzw. gestört wird, ohne dass sie davon erfahren. Schliesslich zeigen ausländische Erfahrungen mit dem „IMSI-Catcher", dass das Gerät vor allem dazu geeignet ist, in bestimmten Situationen „spontan" zu erfahren, wer sich an einem bestimmten Ort aufhält, oder um gezielt den Telefonverkehr zu stören. Für GPS, DJS und gr.ch stellt sich zudem die Frage, ob der Einsatz dieser Geräte überhaupt in den Bereich des Strafprozessrechts gehört. Gemäss dem erläuternden Bericht soll die Polizei nämlich zwar auf Anordnung der Staatsanwaltschaft solche Geräte einsetzen dürfen – jedoch mit dem Ziel, „die öffentliche Sicherheit zu gewährleisten". Letzteres ist gemäss den erwähnten Teilnehmern eine polizeirechtliche Aufgabe, für die der Bund keine Gesetzgebungskompetenz hat. Artikel 270ter StPO gibt überdies weder Kriterien dafür an, wann ein solcher Einsatz gerechtfertigt wäre, noch formuliert er Eingriffsvoraussetzungen, die über die Genehmigung durch das Zwangsmassnahmengericht hinausgehen. Das Gericht hat damit auch keine Leitlinien, anhand derer es den Einsatz genehmigen oder untersagen kann.

Gemäss TI ist im Gesetz zu präzisieren, dass die Zuständigkeit für die Bewilligung derartiger Geräte beim BAKOM liegt, damit nicht missverständlicherweise angenommen wird, dass die in Absatz 2 genannte Genehmigungsbehörde diese erteilt. Weiter ist klarzustellen, ob die besagte Genehmigung des BAKOM die Zulässigkeit eines bestimmten Gerätetyps beinhaltet oder ob eine Genehmigung für jeden Einsatz eingeholt werden muss. Auch NW verlangt, dass das Genehmigungsverfahren im Gesetz geregelt wird.

Mehrere Teilnehmer aus der Fernmeldedienstbranche[165] geben zu bedenken, dass beim Betrieb von solchen „IMSI-Catchern" bei den Fernmeldedienstanbieterinnen automatisch nach „IMSI" oder gar „TIMSI"[166] nachgefragt wird. Die Herausgabe der „IMSI" ist jedoch fragwürdig, da IMSI ein Sicherheitselement des Fernmeldenetzes ist. Solange die Polizeiorgane selbständig nach Standorten suchen, können sie damit leben, aber sobald Unterstützung in Form von speziellen Karten gefragt ist, wird es sehr teuer, da eine solche Unterstützung nur von sehr wenigen Spezialisten erbracht werden kann.

MS betont, dass der „IMSI-Catcher" auch den Zugriff zum Inhalt der Gespräche erlaubt. Dies muss unbedingt erwähnt werden und auch in der Marginalie zum Ausdruck kommen, um zu vermeiden, dass damit Daten im Sinne von Artikel 269 StPO gesammelt werden.

11.1.4 Artikel 271 Absatz 1 und 2 StPO Schutz von Berufsgeheimnissen

1 Bei der Überwachung einer Person, die einer in den Artikeln 170–173 genannten Berufsgruppe angehört, wird der direkte Zugang der Strafverfolgungsbehörde zu den aus der Überwachung gewonnenen Informationen unterbunden. Informationen, die mit dem Gegenstand der Ermittlungen und dem Grund, aus dem diese Person überwacht wird, nicht in Zusammenhang stehen, werden unter der Leitung eines Gerichtes ausgesondert. Dabei dürfen der Strafverfolgungsbehörde keine Berufsgeheimnisse zur Kenntnis gelangen.

---

163 LU, NW, BL, SG, GL, GR, TG, VS, JU, KKJPD, KSBS.
164 International Mobile Subscriber Identity.
165 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
166 Temporary International Mobile Subscriber Identity.

2 Von der Aussonderung wird abgesehen, wenn:

a. der dringende Tatverdacht gegen die Trägerin oder den Träger des Berufsgeheimnisses selber besteht; und

b. besondere Gründe es erfordern.

OW hält die Anpassung bzw. Ergänzung der Bestimmung für angebracht und richtig.

NW, BL, SG und KSBS vermissen die Regelung der Konstellation, bei der der Berufsgeheimnisträger als Gesprächspartner der überwachten Person auftritt. Die Bestimmung ist diesbezüglich zu ergänzen. Wenn der Berufsgeheimnisträger als Dritter überwacht wird, dann sollte sich die Überwachung gemäss SG und KSBS zudem auf Gespräche mit der beschuldigten Person (oder auf Gespräche der beschuldigten Person, welche den Anschluss des Berufsgeheimnisträgers benützt) beschränken. Dies ist nicht nur durch eine Triage unter der Leitung des Gerichtes, sondern allenfalls durch eine technische Triage möglich. Diese Möglichkeit sollte im Gesetz vorgesehen werden (z.B. nur Aufzeichnung von Verbindungen zwischen dem überwachten Anschluss und der Zielperson). Es kann jedoch entgegen dem Wortlaut nicht verlangt werden, dass das Gericht die Auswertung der Überwachung nicht einer Strafverfolgungsbehörde überträgt; denn nur diese Behörden besitzen das nötige Know-how zur Auswertung der Überwachung. Die erwähnten Teilnehmer verlangen daher, Absatz 1 wie folgt zu ergänzen: „(…) wird der direkte Zugang der *mit der Voruntersuchung befassten* Strafverfolgungsbehörde (…) unterbunden".

Gemäss SAV enthält der vorgeschlagene Artikel Elemente, die jeglicher Logik entbehren. So ist unverständlich, warum Berufsgeheimnisse durch Aussonderung der Informationen aus den Akten geschützt werden, wenn diese mit dem Gegenstand der Ermittlungen nicht im Zusammenhang stehen und der Träger des Berufsgeheimnisses nur als einfacher Besitzer eines Anschlusses überwacht wird, nicht aber, wenn die Überwachung auf Grund eines dringenden Tatverdachts erfolgt, unter welchem der Träger des Berufsgeheimnisses steht. In beiden Fällen ist das Interesse am Geheimnisschutz der Klienten, Patienten oder Gläubigern das gleiche und es gibt keine Gründe, Informationen, die mit dem Gegenstand der Ermittlungen nicht im Zusammenhang stehen und dem Berufsgeheimnis unterstehen, in den Akten zu belassen.

Gemäss SAV wird in jedem zivilisierten Staat das Berufsgeheimnis bei Überwachungsmassnahmen im Fernmeldeverkehr geschützt, und zwar auf Grund folgender drei Grundsätze: Die Überwachung von Fernmeldeanlagen von Trägern des Berufsgeheimnisses muss die Ausnahme bleiben; die Überwachung muss so erfolgen, dass sie nur Informationen erfasst, die mit dem Gegenstand der Ermittlungen im Zusammenhang stehen und schliesslich hat die Auswertung der so gewonnenen Informationen ein Gericht vorzunehmen, das mit dem Fall nicht befasst ist. Das bedeutet, dass die Überwachung nur bei ausserordentlichen Umständen zu erfolgen hat. Die durch das Berufsgeheimnis geschützten Informationen, welche anlässlich einer Überwachung von Dritten entdeckt werden, sind aus den Akten zu entfernen und sind nicht verwertbar. Gestützt auf diese Grundsätze beantragt der SAV eine Neuformulierung der Bestimmung.

11.1.5 Artikel 273 Absatz 3 StPO Verkehrs- und Rechnungsdaten, Teilnehmeridentifikation

3 Auskünfte nach Absatz 1 können unabhängig von der Dauer der Überwachung und bis 12 Monate rückwirkend verlangt werden.

LU, NW, KSBS und KKJPD verweisen auf ihre Ausführungen zu Artikel 23 VE-BÜPF (III. Ziff. 5.4). OW hält die Anpassung für angebracht.

11.1.6 Artikel 274 Absatz 4 Buchstaben c und d StPO Genehmigungsverfahren *(neu)*

4 Die Genehmigung äussert sich ausdrücklich darüber, ob:
c. Informatikprogramme in ein Datensystem eingeführt werden dürfen, um Daten abzufangen und zu lesen;
d. Geräte von der Polizei eingesetzt werden dürfen, mit denen spezifische Kennzeichen von Mobiltelefongeräten und ihr Standort ermittelt werden können.

OW hält die Ergänzung der Bestimmung für angebracht.

Buchstabe c

BL und AG beantragen, die Modalitäten der Löschung der Informatikprogramme von den betroffenen Systemen in Buchstabe c zu regeln**.** NW möchte das Genehmigungsverfahren für den Einsatz solcher Informatikprogramme geregelt haben.

Buchstabe d

Mehrere Teilnehmer[167] beantragen, den Begriff „mobile Kommunikationsmittel“ anstelle von „Mobiltelefongeräte“ zu verwenden, damit die Überwachbarkeit auch bei zukünftigem technischen Fortschritt gewährleistet bleibt (bspw. Notebooks mit SIM-Karten).

KSBS und KKJPD verweisen auf ihren Antrag den Einsatz solcher Geräte in Artikel 280 StPO aufzunehmen (vgl. Bemerkungen in III. Ziff. 11.1.3 zu Art. 270ter StPO) und beantragen, zusammen mit NW, das entsprechende Genehmigungsverfahren in Artikel 274 StPO zu regeln.

11.1.7 Artikel 278 Absatz 1bis StPO Zufallsfunde

1bis Werden durch die Überwachung nach Artikel 27 und 28 des Bundesgesetzes vom … betreffend die Überwachung des Post- und Fernmeldeverkehrs strafbare Handlungen bekannt, so dürfen die Erkenntnisse unter den Voraussetzungen der Absätze 2 und 3 verwendet werden.

OW hält die Ergänzung der Bestimmung für angebracht.

11.2. Militärstrafprozess vom 23. März 1979 (MStP)[168]

OW hält die vorgeschlagenen Anpassungen und Ergänzungen des MStP für angebracht und richtig.

11.2.1 Artikel 70a^{bis} MStP Abfangen und Entschlüsselung von Daten *(neu)*

1 Sind bei einer Überwachung des Fernmeldeverkehrs die bisherigen Massnahmen erfolglos geblieben oder wären andere Überwachungsmassnahmen aussichtslos oder würden die Überwachung unverhältnismässig erschweren, so kann der Untersuchungsrichter auch ohne Wissen der überwachten Person das Einführen von Informatikprogrammen in ein Datensystem anordnen, um die Daten abzufangen und zu lesen. Der Untersuchungsrichter gibt in der Anordnung der Überwachung an, auf welche Art von Daten er zugreifen will.
2 Die Anordnung bedarf der Genehmigung durch den Präsidenten des Militärkassationsgerichts.

Einige Teilnehmer[169] verweisen auf ihre Bemerkungen zu Artikel 270bis StPO (vgl. III. Ziff. 11.1.2).

---

167 ZH, LU, AG, GL, GR, TG, VS, JU, KKPKS, KKJPD.
168 SR 322.1
169 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

11.2.2 Artikel 70a^ter MStP Einsatz von Ortungsgeräten *(neu)*

[1] Der Untersuchungsrichter kann den Einsatz von Geräten durch die Polizei anordnen, mit denen spezifische Kennzeichen von Mobiltelefongeräten und ihr Standort ermittelt werden können. Die Geräte müssen vorgängig von der zuständigen Behörde bewilligt worden sein.

[2] Die Anordnung bedarf der Genehmigung durch den Präsidenten des Militärkassationsgerichts.

Mehrere Teilnehmer[170] beantragen, den Begriff „mobile Kommunikationsmittel“ anstelle von „Mobiltelefongeräte“ zu verwenden, damit die Überwachbarkeit auch bei zukünftigem technischen Fortschritt gewährleistet bleibt (bspw. Notebooks mit SIM-Karten).

Einige Teilnehmer[171] verweisen auf ihre Bemerkungen zu Artikel 270^ter StPO (vgl. III. Ziff. 11.1.3).

11.2.3 Artikel 70b MStP Schutz von Berufsgeheimnissen

[1] Bei der Überwachung einer Person, die einer in Artikel 75 Buchstabe b genannten Berufsgruppe angehört, wird der direkte Zugang der Strafverfolgungsbehörde zu den aus der Überwachung gewonnenen Informationen unterbunden. Informationen, die mit dem Gegenstand der Ermittlungen und dem Grund, aus dem diese Person überwacht wird, nicht in Zusammenhang stehen, werden unter der Leitung des Präsidenten des Militärgerichts ausgesondert Dabei dürfen der Strafverfolgungsbehörde keine Berufsgeheimnisse zur Kenntnis gelangen.

[2] Von der Aussonderung wird abgesehen, wenn:

- *a. der dringende Tatverdacht gegen die Trägerin oder den Träger des Berufsgeheimnisses selber besteht; und*
- *b. besondere Gründe es erfordern.*

[3] Bei der Überwachung anderer Personen sind Informationen, über welche eine in Artikel 75 Buchstabe b genannte Person das Zeugnis verweigern könnte, aus den Strafverfahrensakten auszusondern und sofort zu vernichten; sie dürfen im Strafverfahren nicht verwendet werden.

Keine Bemerkungen.

11.2.4 Artikel 70d Absatz 3 MStP

[3] Auskünfte nach Absatz 1 können unabhängig von der Dauer der Überwachung und bis 12 Monate rückwirkend verlangt werden.

Einige Teilnehmer[172] verweisen auf ihre Bemerkungen zur Verlängerung der Aufbewahrungsfrist in Artikel 19 Absatz 2 VE-BÜPF (vgl. III. Ziff. 4.1.2) und Artikel 23 VE-BÜPF (vgl. III. Ziff. 5.4).

11.2.5 Artikel 70e Absatz 4 Buchstaben c und d MStP *(neu)*

[4] Die Genehmigung äussert sich ausdrücklich darüber, ob:

- *c. Informatikprogramme in ein Datensystem eingeführt werden dürfen, um Daten abzufangen und zu lesen;*
- *d. Geräte von der Polizei eingesetzt werden dürfen, mit denen spezifische Kennzeichen von Mobiltelefongeräten und ihr Standort ermittelt werden können.*

Einige Teilnehmer[173] verweisen bezüglich des Buchstabens c auf ihre Bemerkungen in III. Ziffer 11.1.2 zu Artikel 270^bis StPO und auf Ziffer 11.1.3 zu Artikel 270^ter StPO bezüglich Buchstaben d.

---

170 ZH, LU, AG, GL, GR, TG, VS, JU, KKPKS, KKJPD.
171 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
172 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
173 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

11.3. Fernmeldegesetz vom 30. April 1997 (FMG)[174]

11.3.1 Art. 6a FMG Zugangssperre zum Fernmeldedienst

Die Anbieterinnen von Fernmeldediensten haben den Zugang zur Mobiltelefonie und zum Internet für Personen zu sperren, welche die Kundenbeziehung nicht über ein Abonnementsverhältnis aufgenommen haben, wenn diese Personen bei der Aufnahme der Kundenbeziehung die Identität einer Person verwendet haben, die nicht existiert oder die der Aufnahme der Kundenbeziehung nicht vorgängig zugestimmt hat.

Zehn Teilnehmer[175] begrüssen die Verankerung einer Zugangssperre bei Missbräuchen ausdrücklich. Die heutige Praxis zeigt, dass Delinquenten, welche die Mobiltelefonie benutzen, entweder gestohlene Geräte benützen oder solche, die auf fremde oder inexistente Personen als Abonnenten lauten. Die Qualität der Überprüfungsprozesse der Identität von Kundinnen und Kunden bei Vertragsabschlüssen mit Mobiltelefonieanbietern lässt erfahrungsgemäss zu wünschen übrig.

Für OW geht die beabsichtigte Anpassung des FMG zu wenig weit. Nur mit einer konsequenten Handhabung der Registrierung der Kundenbeziehung kann der in der Praxis stattfindende Missbrauch der Prepaid-SIM-Karten verhindert werden. Die aktuelle Situation ist für die Strafverfolgungsbehörden unbefriedigend. AG beantragt, die Bestimmung dahingehend zu ergänzen, dass mit der Befugnis der Strafverfolgungsbehörden, allenfalls mit Genehmigung des Zwangsmassnahmengerichts, eine Zugangssperre für „Prepaid-SIM- und Prepaid-Wireless-Karten“ verlangt werden kann, wenn über diese Karten strafbare Handlungen vorgenommen wurden und weiterhin werden.

Orange beantragt, die Formulierung „(…) und zum Internet (…)“ ersatzlos zu streichen.

---

[174] SR 784.10

[175] ZH, NW, KKJPD, GL, GR, TG, VS, JU, KKPKS, KSBS.