

**Bericht und Vorentwürfe
über die Änderung des Schweizerischen Strafge-
setzbuches und des Militärstrafgesetzes**

betreffend

**die strafrechtliche Verantwortlichkeit
der Provider und die Kompetenzen des Bundes bei
der Verfolgung strafbarer
Handlungen mittels elektronischer
Kommunikationsnetze (Netzwerkkriminalität)**

Bern, Oktober 2004

Übersicht	3
1. Ausgangslage	4
1.1 Expertenkommission „Netzwerkkriminalität“	4
1.2 Arbeitsgruppe „Genesis“	5
2. Strafrechtliche Verantwortlichkeit der Provider (Vorentwurf A)	6
2.1 Expertenkommission "Netzwerkkriminalität"	6
2.11 Strafrechtliche Verantwortlichkeit der Provider.....	7
2.12 Bundeskompetenz für die Strafverfolgung.....	8
2.13 Anregungen für andere Rechtsgebiete.....	8
2.2 Stellungnahme und Vorschlag des Bundesrates	9
2.21 Strafrechtliche Verantwortlichkeit der Provider.....	9
2.22 Flankierende Massnahmen.....	11
2.221 Zivilrecht.....	11
2.222 Verwaltungsrecht.....	12
2.223 Weitere gesetzgeberische Massnahmen.....	12
2.3 Erläuterungen der einzelnen Bestimmungen	13
2.31 Strafgesetzbuch.....	13
2.311 Ergänzung des Randtitels im 6. Abschnitt des Zweiten Titels StGB.....	14
2.312 Strafrechtliche Verantwortlichkeit der Provider.....	14
2.32 Militärstrafgesetz.....	19
2.4 Vorentwurf A	20
2.41 Schweizerisches Strafgesetzbuch	20
2.42 Militärstrafgesetz	22
3. Kompetenzen des Bundes bei strafbaren Handlungen mittels elektronischer Kommunikationsnetze (Vorentwurf B)	24
3.1 Vorschläge der Arbeitsgruppe "Genesis"	24
3.11 Strafverfolgung bei Tatbegehung mittels elektronischer Kommunikationsnetze.....	24
3.12 Analyse der Operation „Genesis“.....	24
3.13 Keine Bundeskompetenz zur Strafverfolgung von Netzwerkkriminalität.....	25
3.14 Vorgeschlagenes Modell.....	25
3.15 Variante 1 (Ermittlungskompetenz der Bundesanwaltschaft [BA] gemäss Art. 259 des Bundesgesetzes vom 15. Juni 1934 über die Bundesstrafrechtspflege [BStP] gestützt auf eine Oberaufsicht des Bundes).....	26
3.16 Variante 2 (Ermittlungskompetenz der zuständigen Bundesbehörde).....	26
3.17 Flankierende Massnahmen.....	27
3.2 Stellungnahme und Vorschlag des Bundesrates	27
3.21 Keine Bundeskompetenz zur Strafverfolgung von Netzwerkkriminalität.....	27
3.22 Ermittlungskompetenzen der Bundesbehörden.....	28
3.23 Flankierende Massnahmen.....	29
3.3 Erläuterungen des Artikels 344 VE-StGB (Kompetenzen des Bundes bei strafbaren Handlungen mittels elektronischer Kommunikationsnetze)	30
3.31 Systematische Einordnung und Randtitel des neuen Artikels 344 VE- StGB.....	30
3.32 Absatz 1.....	30
3.33 Absatz 2.....	31
3.4 Militärstrafgesetz	32
3.5 Vorentwurf B Schweizerisches Strafgesetzbuch	32

Übersicht

Die rasante Entwicklung der Informations- und Netzwerktechnologie, wie Internet oder Mobiltelefonie, hat in den letzten Jahren wie kaum ein anderer Faktor die Lebens- und Kommunikationsgewohnheiten der Menschen beeinflusst. Es ist heute möglich von jedem Netzanschluss aus Informationen von überall auf der Welt abzurufen. Diese unbestrittenen Vorzüge der elektronischen Kommunikationsmittel haben aber auch ihre Schattenseiten: strafbare Handlungen können von jedem beliebigen Ort der Welt aus begangen werden. Die so genannte Netzwerkkriminalität nimmt stetig zu und die geltenden Strafgesetzbuch (StGB) und Militärstrafgesetz (MStG) geben auf einzelne Fragen der strafrechtlichen Verantwortlichkeit der Provider, d.h. der verschiedenen Diensteanbieter, welche mit der technischen Infrastruktur an der Begehung dieser Delikte beteiligt sind, nicht immer eine klare Antwort. Bei diesen Providern handelt es sich namentlich um den Content-Provider oder Inhaltsanbieter, der eigene oder von Dritten übernommene Inhalte auf dem Internet zur Nutzung bereithält; den Hosting-Provider, der seinen Kunden, den Content-Providern, einen Speicherplatz zur Verfügung stellt, auf dem diese ihre eigenen Inhalte anbieten können, und schliesslich um den Access-Provider oder Zugangsvermittler, der den Nutzern (Usern) den Zugang ins Internet technisch ermöglicht.

Die Netzwerkkriminalität mit ihrer weltweiten Wirkung stellt auch die Strafverfolgung vor neue Herausforderungen. Die zuständigen kantonalen Strafverfolgungsbehörden stossen bei ihren Ermittlungen in komplexen Fällen namentlich von grenzüberschreitenden Computerdelikten schnell an ihre Grenzen, weil es ihnen vielfach an spezialisierten Kriminalisten und entsprechender Ausrüstung fehlt. Häufig ist zu Beginn der Ermittlungen auch unklar, welche kantonale Strafverfolgungsbehörde überhaupt zuständig ist. Um den Anschluss im Kampf gegen diese moderne Form der Kriminalität nicht zu verlieren, müssen die Rahmenbedingungen für die Zusammenarbeit zwischen Bund und Kantonen verbessert werden.

Der Bundesrat beabsichtigt mit der vorliegenden StGB/MStG-Revision, die gesetzliche Regelung der strafrechtlichen Verantwortlichkeit der Provider zu präzisieren und mit besseren Rahmenbedingungen in der Zusammenarbeit zwischen Bund und Kantonen auch eine effizientere Strafverfolgung von in Netzwerken begangenen Delikten zu ermöglichen. Die Vorlage wurde in der Legislaturplanung 2003-2007 als Richtliniengeschäft angekündigt (BBI 2004 1186).

Um eine differenzierte politische Willensbildung zu ermöglichen, hat der Bundesrat einen Bericht mit zwei Vorentwürfen erstellt. Der Vorentwurf A betrifft die strafrechtliche Verantwortlichkeit der Provider, der Vorentwurf B die Kompetenzen des Bundes bei der Verfolgung strafbarer Handlungen mittels elektronischer Kommunikationsnetze.

1. Ausgangslage

1.1 Expertenkommission „Netzwerkkriminalität“

Im Sommer 1998 stellte die damalige Bundespolizei fest, dass rassistische Inhalte, die in der Schweiz zu Verurteilungen wegen Verstosses gegen Artikel 261^{bis} StGB geführt hatten, im Internet immer noch ungehindert ihre Verbreitung fanden. Die damalige Bundespolizei richtete daraufhin ein Rundschreiben an die schweizerischen Anbieter von Internet-Dienstleistungen (Internet Service Provider, ISP) und bat sie, die Sperrung der betreffenden Internet-Seiten zu prüfen. Diese Intervention bewirkte einige Unruhe in der Providerbranche, was wiederum Auslöser für die Schaffung einer Kontaktgruppe mit Vertreterinnen und Vertretern der interessierten Bundesstellen und der Providerbranche war.

Da innerhalb der Kontaktgruppe die Frage der strafrechtlichen Verantwortlichkeit der Internet-Provider für deliktische Internet-Inhalte umstritten war, wurde das Bundesamt für Justiz (BJ) beauftragt, diese Frage zu begutachten. Das BJ bejahte in seinem Gutachten vom 24. Dezember 1999¹ grundsätzlich die subsidiäre Verantwortlichkeit auch eines reinen Zugangsvermittlers, des Access-Providers, im Sinne des Medienstrafrechts; vorausgesetzt dieser sei von einer Strafverfolgungsbehörde klar auf den illegalen Inhalt aufmerksam gemacht worden. Wo das Medienstrafrecht keine Anwendung finde, könnten die Access-Provider als Gehilfen zur Haupttat bestraft werden.

Die Providerbranche war mit dem Ergebnis des BJ-Gutachtens nicht einverstanden und beauftragte daraufhin die Strafrechtsprofessoren Niggli, Riklin und Stratenwerth, die Verantwortlichkeitsfrage ihrerseits zu prüfen. In ihrem Gutachten vom Oktober 2000² kamen die drei Professoren zu weitgehend anderen Schlussfolgerungen. Sie betonten aber die ihres Erachtens unklare Rechtslage und schlossen auf einen gesetzgeberischen Handlungsbedarf.

Am 14. Dezember 2000 reichte Ständerat Thomas Pfisterer eine Motion (00.3714)³ ein. Ziel der Motion war es, Missbräuche des Internets zu verhindern und die Internetkriminalität strafrechtlich zu erfassen. Um dies zu erreichen, verlangte die Motion vom Bundesrat eine rechtssichere, praktikable, international harmonisierte Regelung im Strafrecht, eventuell in einzelnen weiteren Bestimmungen. In der Begründung empfahl der Motionär eine Anlehnung an die so genannte E-Commerce-Richtlinie der Europäischen Union (EU)⁴ und entwarf zudem einen möglichen Gesetzestext. Die Motion Pfisterer wurde 2001 von beiden Räten angenommen.

Vor dem Hintergrund dieser Entwicklungen setzte die damalige Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements (EJPD) am 22. November 2001 eine Expertenkommission unter dem Vorsitz des damaligen BJ-Vizedirektors Dr. Peter Müller ein. Die aus Vertreterinnen und Vertretern der Rechtswissenschaft, der Provi-

¹ Veröffentlicht in VPB 64 75.

² Abgedruckt in medialex, Sondernummer 1/2000.

³ AB 2001 S 27 f.

⁴ Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“ - „e-commerce Richtlinie“).

derbranche und der Bundesverwaltung zusammengesetzte Kommission hatte den Auftrag zu prüfen, mit welchen Mitteln durch das Internet begangene Rechtsverletzungen verhindert beziehungsweise geahndet werden können und insbesondere wie die strafrechtliche Verantwortlichkeit im Internet zu regeln sei. Die Expertenkommission „Netzwerkkriminalität“ lieferte ihren Bericht im Sommer 2003 ab⁵.

1.2 Arbeitsgruppe „Genesis“

Im Sommer 2002 führten die Polizeikorps der meisten Kantone in Zusammenarbeit mit dem Bundesamt für Polizei (fedpol) unter dem Namen „Genesis“ eine Operation gegen Kinderpornografie im Internet durch. Es handelte sich dabei um eine landesweite Operation von noch nie da gewesenen Ausmass. Die grosse Anzahl und die schweizweite Streuung der gleichzeitig einzuleitenden Verfahren waren in dieser Form für die schweizerischen Ermittlungsbehörden ein Novum. Zur Bewältigung stellte die Bundeskriminalpolizei (BKP) die gesamtschweizerische Koordination dieser Operation sicher, ohne aber über eigentliche Ermittlungsmöglichkeiten in der ersten Verfahrensphase bis zur Bezeichnung der zuständigen kantonalen Strafverfolgungsbehörden und ohne über Weisungskompetenzen zu verfügen. Die Strafverfolgungskompetenz im Bereich der Pornografie (Art. 197 StGB) liegt bei den Kantonen - ob mittels Internet oder auf andere Weise begangen. Die Operation „Genesis“ zeigte erstmals deutlich, dass für das Zusammenwirken von Bund und Kantonen in Fällen, die der kantonalen Gerichtsbarkeit unterstehen und eine Vielzahl von Personen in mehreren Kantonen betreffen, gesetzgeberischer Handlungsbedarf besteht.

Die Operation „Genesis“ stiess in der Öffentlichkeit und in der Politik, welche schon zuvor für die Themen Kinderpornografie im Internet sowie Internetkriminalität im Allgemeinen stark sensibilisiert waren⁶, auf grosses Interesse. Am 26. September 2002 reichte die damalige Nationalrätin Regine Aeppli Wartmann eine parlamentarische Initiative (02.452) ein, mit der sie für die Strafverfolgung im Bereich der Netzwerkkriminalität eine Bundeskompetenz nach dem Muster der „Effizienzvorlage“ (Art. 340^{bis} StGB) verlangte⁷. Am 11. Dezember 2003 gab der Nationalrat der Initiative Folge.

Vor diesem Hintergrund erteilte die damalige Vorsteherin des EJPD im Herbst 2002 fedpol den Auftrag, die rechtlichen und organisatorischen Rahmenbedingungen der Operation „Genesis“ im Hinblick auf künftige ähnliche Fälle zu analysieren und Vorschläge für eine verbesserte Zusammenarbeit zwischen Bund und Kantonen auszuarbeiten. Zur Erfüllung dieses Auftrages wurde die Arbeitsgruppe „Genesis“ ins Leben gerufen; sie setzte sich aus Vertreterinnen und Vertretern von Polizei und Justizbehörden, der Konferenz der Kantonalen Polizeikommandanten der Schweiz

⁵ Bericht der Expertenkommission „Netzwerkkriminalität“, Eidgenössisches Justiz- und Polizeidepartement, Bern, Juni 2003.

⁶ Vgl. dazu folgende parl. Vorstösse: Motion Aeppli Wartmann Regine (01.3196), Internet-Kriminalität. Wirksamere Bekämpfung mit effizientem Verfahren; Motion Kommission für Rechtsfragen N (01.3012), Bekämpfung der Pädophilie; Interpellation Tillmanns Pierre (00.3235), Bekämpfung der Pädophilie; Motion Kommission 00.16-N (00.3206), Grossverbrechen. E-Kriminalität; Interpellation Freund Jakob (00.3059), Internetaktivitäten des Bundes im Rahmen der Strafverfolgung; Kt.IV. Genf (00.314), Bekämpfung der Pädophilie; Motion von Felten Margrith (98.3467), Internetkriminalität. Verantwortlichkeit der Provider; Motion Jeanprêtre Francine (97.3487), Bekämpfung der Kinderpornographie auf Datennetzen; Postulat Kommission für Rechtsfragen N (96.3005), Kinderpornographie im Internet.

⁷ AB 2003 N 1967.

(KKPKS), der Konferenz der Strafverfolgungsbehörden der Schweiz (KSBS) sowie von Bundesstellen (fedpol, Bundesanwaltschaft und BJ) zusammen. Die Arbeitsgruppe "Genesis" lieferte ihren Bericht im November 2003 ab⁸.

Anfang 2003 - also rund ein halbes Jahr nach dem Beginn der Operation „Genesis“ - nahm die „Nationale Koordinationsstelle zur Bekämpfung der Internet-Kriminalität“ (KOBIK) ihre Arbeit auf. Diese von Bund und 25 Kantonen (ohne Zürich) gemeinsam finanzierte Stelle ist fedpol angegliedert. Sie unterstützt die Strafverfolgungsbehörden der Kantone und des Bundes beim Erkennen strafbarer Internet-Missbräuche (Monitoring), der Prüfung und Zuweisung eingegangener Verdachtsmeldungen (Clearing) sowie der Analyse der Internet-Kriminalität. Die Ermittlungskompetenzen und -pflichten der Strafverfolgungsbehörden bleiben jedoch unabhängig von der Tätigkeit von KOBIK im aktuellen Umfang bestehen, was bedeutet, dass sie in den meisten Fällen bei den Kantonen liegen. KOBIK hat zudem keine Weisungsbefugnis gegenüber den zuständigen Strafverfolgungsbehörden.

2. Strafrechtliche Verantwortlichkeit der Provider (Vorentwurf A)

2.1 Expertenkommission "Netzwerkkriminalität"

In ihrem Bericht legt die Expertenkommission „Netzwerkkriminalität“ dar, dass das seit dem 1. April 1998 geltende Medienstrafrecht nicht auf das Internet passt⁹. Nach den Bestimmungen des Medienstrafrechts (Art. 27, 27^{bis} und 322^{bis} StGB) gilt nämlich, dass die strafbare Handlung durch eine Veröffentlichung in einem Medium begangen wird und sie sich zugleich in dieser Veröffentlichung erschöpfen muss. Grundsätzlich macht sich dabei nur der Autor strafbar (Art. 27 Abs. 1 StGB). Kann dieser nicht ermittelt oder in der Schweiz nicht vor Gericht gestellt werden (Art. 27 Abs. 2 StGB), ergibt sich aus Artikel 322^{bis} StGB eine subsidiäre, exklusive Strafbarkeit des verantwortlichen Redaktors oder, wo ein solcher fehlt, der für die Veröffentlichung verantwortlichen Person (so genannte Kaskadenhaftung). Die geltende Regelung des Medienstrafrechts ist auf ein Zusammenwirken von Autoren, Redaktoren und anderen für die Publikation Verantwortlichen ausgerichtet.

Diese Regelung passt nicht generell auf den Hosting-Provider, der in der Regel lediglich die technische Infrastruktur zum Bereithalten der Informationen betreibt und deshalb keine für die Veröffentlichung verantwortliche Person ist. Das Gleiche gilt auch für den Access-Provider, sofern sich dessen Dienstleistung darauf beschränkt, einen Zugang zum Internet zur Verfügung zu stellen.

Auch im Zusammenhang mit der Anwendung der allgemeinen Zurechnungsregeln von Täterschaft und Teilnahme des StGB erkennt die Expertenkommission für den Hosting- wie auch für den Access-Provider eine Reihe von ungelösten Fragen. Ob z.B. der Hosting-Provider Täter oder nur Gehilfe ist, hängt von der Beschreibung der Tathandlung in der jeweiligen Strafnorm ab. Die Abgrenzung zwischen diesen beiden Rollen ist aber gerade bei den im Internet in Frage kommenden Tatbeständen über

⁸ Bericht „Modell für eine effiziente Strafverfolgung bei kantonsübergreifenden und/oder internationalen Fällen von Netzwerkkriminalität“ der Arbeitsgruppe „Genesis“, Bern, 12. November 2003.

⁹ Bericht der Expertenkommission „Netzwerkkriminalität“, op. cit., S. 59 ff.; 65 f.

weite Strecken verwischt. Nach Artikel 197 Ziffer 1 StGB genügt z.B. das blosses Zugänglichmachen von pornografischen Schriften an Personen unter 16 Jahren, was den Hosting-Provider zum Täter machen würde. Der Hosting-Provider beschränkt sich aber in der Regel darauf, seinem Kunden ein bestimmtes Quantum an Speicherplatz auf seinen Rechnern einzuräumen. Welche Informationen sich auf seinen Rechnern befinden, weiss der Hosting-Provider somit oft gar nicht. Dieses Wissen kann er nur dadurch erlangen, dass er entweder auf eine Information aufmerksam gemacht wird, oder indem er präventiv selbst Kontrollen durchführt.

Schliesslich ist nach einem 1999 ergangenen Bundesgerichtsurteil¹⁰ nicht alles, was sich medial veröffentlichen lässt und sich in der Veröffentlichung ausschöpft, auch immer ein Mediendelikt. Das Bundesgericht erwähnt in diesem Urteil explizit die Gewaltdarstellungen (Art. 135 StGB), die harte Pornografie (Art. 197 Ziff. 3 StGB) und das Leugnen von Völkermord (insbesondere durch die „Auschwitzlüge“ im Sinne von Art. 261^{bis} Abs. 4 StGB), die nicht zu den Mediendelikten zu zählen seien. Begründet hat dies das Bundesgericht im Wesentlichen damit, dass der Gesetzgeber bei diesen Delikten die Veröffentlichung der strafbaren Inhalte verhindern wollte und deshalb kaum einer bestimmten Gruppe von Tatbeteiligten eine privilegierende Stellung gemäss Medienstrafrecht, Artikel 27 StGB, einräumen wollte. Zudem sei die Schweiz im Hinblick auf die Rassendiskriminierung durch die Ratifikation des internationalen Übereinkommens gegen die Rassendiskriminierung¹¹ völkerrechtlich verpflichtet, jede Verbreitung rassistischer Äusserungen ohne Ausnahme zu verfolgen. Diesem Urteil ist zwar von Seiten der Lehre viel Kritik erwachsen¹². Diese in Lehre und Rechtsprechung unklare Situation zeigt laut Expertenkommission aber auf, dass eine gesetzliche Regelung der strafrechtlichen Verantwortlichkeit der an der Netzwerkkriminalität beteiligten Provider nötig ist.

Im Zentrum des Expertenberichts stehen zwei Themenbereiche (vgl. unten Ziff. 2.11 und 2.12), zu denen ausformulierte Vorschläge erarbeitet wurden; ausserdem hat die Expertenkommission Anregungen zu anderen Rechtsgebieten gemacht (unten Ziff. 2.13).

2.11 Strafrechtliche Verantwortlichkeit der Provider

In Anlehnung an ausländische Vorschriften, welche die E-Commerce-Richtlinie der EU umsetzen, schlägt die Expertenkommission vor, das StGB mit einer neuen speziellen Regelung der strafrechtlichen Verantwortlichkeit der Provider zu ergänzen (neue Art. 27 und 322^{bis} VE-StGB). Diese Regelung enthält zusammengefasst den Grundsatz, dass die allgemeinen Bestimmungen über Täterschaft und Teilnahme

¹⁰ BGE 125 IV 206 ff.

¹¹ BBI 1992 III 269 ff.

¹² Franz Riklin, Kaskadenhaftung – quo vadis? *Medialex* 2000, 208; Franz Riklin/Günter Stratenwerth, Medienstrafrecht/Kaskadenhaftung, in: Niggli/Riklin/Stratenwerth (Hrsg.), *Die strafrechtliche Verantwortlichkeit von Internet-Providern*, *medialex Sonderausgabe* 2000, S. 13 ff.; Dorrit Schleiminger / Christoph Mettler, Strafbarkeit der Medienverantwortlichen im Falle der Rassendiskriminierung, Art. 27, Art. 261^{bis} Abs. 4 StGB, *Bemerkungen zu BGE 125 IV 206 ff.*, *AJP* 2000, S. 1039 ff.; Jörg Rehbberg/ Andreas Donatsch, *Strafrecht I, Verbrechenslehre*, 7. Auflage, Zürich 2001, S. 166; Christian Schwarzenegger, *E-Commerce – Die strafrechtliche Dimension*, in: Arter/Jörg (Hrsg.), *Internet-Recht und Electronic Commerce Law*, Lachen und St. Gallen 2001, S. 349 ff.; Franz Riklin, *Strafrecht, Allgemeiner Teil*, 2. Auflage, Zürich 2002, S. 245; Franz Zeller, in: Niggli/Wiprächtiger, *Basler Kommentar, StGB I*, Basel 2003, zu Artikel 27, N 32.

des StGB auf die Provider anwendbar sind, wenn sie sich aktiv an den strafbaren Handlungen beteiligen. Der Provider ist aber straflos, wenn er sich darauf beschränkt den automatisierten Zugang zum Internet zu ermöglichen, und er macht sich strafbar, wenn er im Nachhinein erfährt oder feststellt, dass er einen strafbaren Inhalt bereithält und es unterlässt, die Nutzung dieser Information zu verhindern¹³.

2.12 Bundeskompetenz für die Strafverfolgung

Über die seit Anfang 2003 vom Bund in Zusammenarbeit mit den Kantonen betriebene nationale Koordinationsstelle KOBIK (vgl. oben Ziff. 1.2) hinaus schlägt die Expertenkommission - nach dem Vorbild der so genannten Effizienzvorlage¹⁴ (Art. 340^{bis} StGB) - in bestimmten Fällen Bundesgerichtsbarkeit vor: So namentlich, wenn mehrere Kantone von der mittels elektronischer Kommunikationsnetze begangenen strafbaren Handlung betroffen sind und ein eindeutiger örtlicher Schwerpunkt fehlt oder wenn ein koordiniertes Ermittlungsverfahren in mehreren Kantonen notwendig ist. Ausserdem soll der Bundesanwalt auf Ersuchen kantonaler Strafverfolgungsbehörden ein Ermittlungsverfahren eröffnen und damit Bundesgerichtsbarkeit begründen können.

Dieser Vorschlag der Expertenkommission orientiert sich an der parlamentarischen Initiative Aepli Wartmann (vgl. oben Ziff. 1.2).

2.13 Anregungen für andere Rechtsgebiete

Die Expertenkommission hält unter anderem auch neue verwaltungsrechtliche Massnahmen für eine denkbare Möglichkeit, um - ergänzend zum Strafrecht – Rechtsverletzungen in elektronischen Kommunikationsnetzen vorzubeugen. Sie erinnert aber daran, dass solche Massnahmen oft mit verfassungsrechtlichen Schranken kollidieren, namentlich mit dem Grundrecht auf freie Kommunikation und dem Grundsatz der Verhältnismässigkeit behördlicher Eingriffe.

Die Expertenkommission erachtet es zudem als wünschenswert, bestimmte zivilrechtliche Haftungsfragen im Zusammenhang mit der Netzwerkkriminalität gesetzgeberisch zu klären.

Die Expertenkommission äussert sich in ihrem Bericht auch zu weiteren (damals) laufenden Gesetzgebungsverfahren im Bereich der Netzwerkkriminalität und gibt dazu Empfehlungen ab¹⁵.

¹³ Bericht der Expertenkommission „Netzwerkkriminalität“, op. cit. , S. 90 ff.

¹⁴ Ziel der Effizienzvorlage ist die Verbesserung der Effizienz und der Rechtsstaatlichkeit in der Strafverfolgung in all jenen Fällen, in welchen die Tat zum wesentlichen Teil im Ausland oder in mehreren Kantonen begangen wurde (BBI 1998 1529 ff.); in Kraft seit 1. Januar 2002 (AS 2001 3071 3076).

¹⁵ Bericht der Expertenkommission „Netzwerkkriminalität“, op.cit., S. 136 ff.

2.2 Stellungnahme und Vorschlag des Bundesrates

Es ist unbestritten, dass sich die rasante Entwicklung der Informations- und Netzwerktechnologie auch auf die Kriminalität auswirkt. Auf der einen Seite erleichtern die neuen technischen Möglichkeiten die Begehung „klassischer“ Straftaten wie Ehrverletzungen, Gewaltdarstellungen, Pornografie oder Rassendiskriminierung. Auf der anderen Seite bieten Computertechnologie und Netzwerke Möglichkeiten für neue Kriminalitätsformen wie unbefugte Datenbeschaffung oder Datenbeschädigung durch die Verbreitung von Computerviren.

Im Sinne der bereits erwähnten parlamentarischen Vorstösse (insbesondere Motion Pfisterer und parlamentarische Initiative Aeppli Wartmann; vgl. oben Ziff. 1.1 und 1.2) ist eine wirkungsvolle Bekämpfung und eine effiziente Strafverfolgung der Netzwerkkriminalität auch für den Bundesrat ein Richtliniengeschäft seiner Legislaturplanung 2003-2007. Er erklärt sich darin bereit, gesetzliche Regelungen zu prüfen, um auf Bundesebene Ermittlungskompetenzen einzuführen und für die Provider strafrechtliche Verantwortlichkeiten festzulegen.

Wie bei Revisionen des bürgerlichen Strafgesetzbuches üblich, ist auch das Militärstrafgesetz entsprechend zu ändern, sofern sich dieselbe Vorschrift in beiden Gesetzen findet.

2.21 Strafrechtliche Verantwortlichkeit der Provider

Die geltenden StGB bzw. MStG enthalten keine ausdrückliche Regelung der Verantwortlichkeit der Provider im Zusammenhang mit illegalen Internet-Inhalten. Wegen der Parallelität¹⁶ zum Medienstrafrecht galt es zunächst abzuklären, ob die Sachverhalte der Netzwerkkriminalität nicht unter die geltenden Artikel 27 und 322^{bis} StGB bzw. 26a MStG fallen oder, ob sie nicht nach den allgemeinen Regeln des StGB/MStG, d.h. insbesondere jenen über die Gehilfenschaft (Art. 25 StGB; Art. 23 MStG) zu beurteilen sind.

Nach einer Auslegeordnung der geltenden strafrechtlichen Möglichkeiten und unter Berücksichtigung der bestehenden Lehrmeinungen und der bundesgerichtlichen Rechtsprechung kommt die Expertenkommission „Netzwerkkriminalität“ zum Schluss, dass die Anwendbarkeit des Medienstrafrechts wie auch die der allgemeinen Teilnahmeregel bei der Netzwerkkriminalität umstritten und deshalb eine gesetzliche Regelung mit Blick auf die gewünschte Rechtssicherheit angezeigt ist.

Der Bundesrat teilt diese Einschätzung der Expertenkommission und schlägt eine ausdrückliche Regelung der strafrechtlichen Verantwortlichkeit der Internet-Provider im StGB/MStG vor.

Die von der Expertenkommission übernommene Regelung sieht vor, dass die Provider für die im elektronischen Kommunikationsnetz zirkulierenden strafbaren Informationen grundsätzlich nach den allgemeinen Bestimmungen des StGB/MStG über die

¹⁶ Es geht auch bei den Netzwerkdelikten um Veröffentlichung (Bereitstellen), Verbreitung und Konsum (Nutzung) von Informationen. Ausserdem sind eine Vielzahl von Personen an der Veröffentlichung und Verbreitung beteiligt.

Täterschaft und Teilnahme strafbar sind. Der Content-Provider oder Inhaltsanbieter, der eigene oder von Dritten übernommene Inhalte auf dem Internet zur Verfügung stellt, ist als Autor der illegalen Information als Täter strafbar. Der Access-Provider oder Zugangsvermittler ist als Mittäter, Anstifter oder Gehilfe strafbar, wenn er sich aktiv an den strafbaren Handlungen des Content-Providers beteiligt und sich nicht auf die automatisierte Zugangsvermittlung beschränkt. Ebenso strafbar ist der Hosting-Provider, der z.B. von allem Anfang an weiss, dass der Content-Provider auf dem ihm zur Verfügung gestellten Speicherplatz strafbare Informationen aufschalten wird.

Gegenüber dieser grundsätzlichen Strafbarkeit der Provider sieht die neue Regelung aber folgende Vorbehalte vor:

- Ist der Content-Provider Autor oder Redaktor im Sinne des geltenden Medienstrafrechts, d.h. begeht er eine strafbare Handlung in einer Online-Publikation z.B. auf einer im Internet publizierten Tageszeitung, so ist der geltende Artikel 27 StGB bzw. Artikel 26a MStG (neu Art. 27^{bis} VE-StGB; neu Art. 26b VE-MStG) anwendbar.
- Weiss der Hosting-Provider im Zeitpunkt in dem er dem Content-Provider den Speicherplatz überlässt nicht, welche Art von Informationen dieser ins Netz stellen will und wird, bleibt er straflos. Erfährt oder stellt der Hosting-Provider aber im Nachhinein fest, dass auf seinem Rechner gespeicherte Daten strafbare Informationen beinhalten, und unterlässt er es, die Nutzung dieser Information zu verhindern, obschon ihm dies technisch möglich und zumutbar ist, so ist er strafbar. Ebenso macht er sich strafbar, wenn er es unterlässt von Dritten an ihn gerichtete und bei ihm eingegangene Hinweise auf strafbare Informationen an die Strafverfolgungsbehörden weiterzuleiten. Dem Hosting-Provider gleichgestellt werden die Anbieter von automatisierten Suchmaschinen wie google.com, altavista.com etc.
- Der Access-Provider, der lediglich den automatisierten Zugang zum Internet ermöglicht, ist nicht strafbar. Diese Straflosigkeit des Access-Providers beruht auf der Tatsache, dass sich seine Zugangsvermittlung auf rein technische Vorgänge beschränkt. Straflos ist auch eine durch eine Nutzerabfrage verursachte, automatische und kurzzeitige Zwischenspeicherung.

Bei dieser Regelung ist entscheidend, dass die Strafbarkeit bzw. die Straflosigkeit nicht ausschliesslich vom Status der Provider abhängt, sondern von ihrer Funktion, die sie im einzelnen Kommunikationsvorgang einnehmen. Allein die Tatsache z.B. Access-Provider zu sein ist noch kein zwingender Strafbefreiungsgrund.

Die neue Regelung stützt sich auf die geltenden Bestimmungen des StGB bzw. MStG. Es versteht sich aber von selbst, dass nach Inkrafttreten der Änderung des StGB (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) vom 13. Dezember 2002 (BBI 2002 8240) bzw. des MStG vom 21. März 2003 (BBI 2003 2808) die Artikelnummerierung angepasst wird. Die vorgeschlagenen Artikel 27, 27bis und 27ter VE-StGB werden zu Artikel 28, 28a und 28b nStGB, bzw. die vorgeschlagenen Artikel 26a, 26b und 26c VE-MStG werden zu Artikel 27, 27a und 27b nMStG.

Gestützt auf die Vernehmlassungsergebnisse zum inzwischen sistierten neuen Bundesgesetz über die Lotterien und Wetten, ist der Bundesrat auch überzeugt, dass die Frage der strafrechtlichen Verantwortlichkeit der Provider im StGB/MStG zu regeln ist und nicht etwa in einem anderen Bundesgesetz. Die im Entwurf des neuen Lotteriegengesetzes vorgesehene Strafbestimmung, die die Provider, welche nicht bewilligte Spiele vermitteln, mit Gefängnis bis zu einem Jahr oder mit Busse bis zu 1 Million Franken bestraft hätte - in schweren Fällen gar mit einer Zuchthausstrafe bis zu fünf Jahren oder Gefängnis nicht unter einem Jahr -, wurde von den Vernehmlassern klar verworfen. Sie wiesen vielmehr darauf hin, dass sie eine Regelung der strafrechtlichen Verantwortlichkeit der Internet-Provider im Sinne der Expertenkommission „Netzwerkkriminalität“ im StGB befürworteten.

Mit der vorliegenden StGB/MStG-Revision schlägt der Bundesrat eine differenzierte gesetzliche Lösung vor, die den technischen Besonderheiten des Internet Rechnung trägt und sich auch an die entsprechenden Vorschriften anderer Länder, namentlich der Nachbarstaaten anlehnt. Dazu gehört auch die E-Commerce-Richtlinie der EU, die einen rechtlichen Rahmen zur Sicherstellung des freien Verkehrs von Diensten der Informationsgesellschaft schaffen will. Zusammenfassend handelt es sich bei der vorliegenden Revision des StGB/MStG - wie von der Motion Pfisterer verlangt - um eine rechtssichere, praktikable und mit dem Recht der Nachbarstaaten harmonisierte Regelung. Die dabei vorgeschlagene Festlegung der strafrechtlichen Verantwortlichkeit entspricht der Vielfältigkeit der durch die Provider im Internet wahrgenommenen Funktionen.

2.22 Flankierende Massnahmen

Neben dieser strafrechtlichen Regelung hat der Bundesrat auch folgende flankierende Massnahmen verwaltungs- oder zivilrechtlicher Natur geprüft.

2.221 Zivilrecht

Die Expertenkommission "Netzwerkkriminalität" beurteilt in ihrem Bericht die haftungsrechtliche Situation für Hosting- und Access-Provider in der Schweiz als lückenhaft und unklar¹⁷. Sie leitet daraus im Interesse einer raschen Verwirklichung von Rechtssicherheit einen gesetzgeberischen Handlungsbedarf ab. Als Ort einer gesetzlichen Regelung, die sich von der Richtlinie der EU über den elektronischen Geschäftsverkehr inspirieren lassen soll, schlägt die Expertenkommission das Bundesgesetz über den elektronischen Geschäftsverkehr oder das Bundesgesetz über die Revision und Vereinheitlichung des Haftpflichtrechts (Haftpflichtgesetz) vor.

Der Bundesrat teilt diese Einschätzungen der Expertenkommission nicht. Die zivilrechtliche Regelung der Providerhaftung ist weder lückenhaft noch unklar. Einschlägig ist vielmehr Artikel 50 Obligationenrecht (OR). Danach haften Anstifter, Urheber und Gehilfen solidarisch für den von ihnen angerichteten Schaden. Wie in den übrigen Fällen möglicher Verantwortlichkeit bleibt es der Praxis überlassen zu beurteilen, welche Voraussetzungen konkret erfüllt sein müssen, damit ein Provider namentlich zum Gehilfen im Sinn dieser Bestimmung wird. Das Gleiche gilt auch für die Beurtei-

¹⁷ Bericht der Expertenkommission "Netzwerkkriminalität", op. cit., S. 83.

lung von verschuldensunabhängigen Beseitigungs- und Unterlassungsansprüchen, beispielsweise bei der Beurteilung einer Persönlichkeitsverletzung durch einen ins Internet gestellten oder zu stellenden Text (Art. 28 Zivilgesetzbuch).

Anders als im Strafrecht hat sich der Gesetzgeber gegen ein besonderes Medienzivilrecht ausgesprochen. Dieses Regime hat sich, wie die Expertenkommission selber einräumen muss, grundsätzlich bewährt und zu keinen stossenden Ergebnissen geführt. Einen zusätzlichen Beitrag zur Rechtssicherheit braucht der Gesetzgeber nach Meinung des Bundesrates nicht zu leisten; die Expertenkommission hat denn auch diesbezüglich keine konkreten Vorschläge gemacht. Anders wäre höchstens dann zu entscheiden, wenn das politische Anliegen darin bestünde, das Verhalten von Providern in bisher nicht gekanntem Ausmass zu entschuldigen. Dies kann und darf aber nicht das Ziel einer Vorlage sein, die sich primär dem Kampf gegen die Netzwerkkriminalität verschrieben hat.

Der Bundesrat erinnert im Übrigen daran, dass die Arbeiten zur Revision des Haftpflichtrechts sistiert worden sind und dass das künftige Bundesgesetz über den elektronischen Geschäftsverkehr hauptsächlich Konsumentenschutzanliegen aufgreift. Für eine Regelung der Providerhaftung wäre daher im Bundesgesetz über den elektronischen Geschäftsverkehr auch dann kein Platz, wenn privatrechtlicher Handlungsbedarf bestünde.

2.222 Verwaltungsrecht

Bezüglich allfälliger verwaltungsrechtlicher Massnahmen teilt der Bundesrat die Ausführungen der Expertenkommission in ihrem Bericht¹⁸. In der Tat würden flankierende, insbesondere präventive Massnahmen des Verwaltungsrechts mit dem Zensurverbot in Konflikt geraten. Auf Grund der Meinungsäusserungsfreiheit könnten den Providern verwaltungsrechtlich auch nicht mehr Pflichten auferlegt werden als jene, die indirekt aus den vorgeschlagenen Artikeln 27 und 322^{bis} VE-StGB bzw. Artikel 26a VE-MStG hervorgehen. Mit der vorgeschlagenen Regelung wird der Hosting-Provider bestraft, der „sicher weiss“, dass ein Dritter mit der Benützung seiner Infrastruktur eine strafbare Handlung begeht. Er wird nicht verpflichtet, ständig darüber zu wachen, ob ein Dritter strafbare Handlungen begeht.

2.223 Weitere gesetzgeberische Massnahmen

Auch bezüglich weiterer gesetzgeberischer Aufgaben im Bereich der Netzwerkkriminalität teilt der Bundesrat die Auffassung der Expertenkommission „Netzwerkkriminalität“, wonach sich die Europaratskonvention über die Cyberkriminalität zu einem wichtigen Instrument im Kampf gegen diese Art der Delinquenz entwickeln kann. Es liegt grundsätzlich im Interesse der Schweiz und der internationalen Rechtshilfe, dass möglichst viele Länder einen gleichen Standard zur Bekämpfung dieser Art der Kriminalität erreichen. Voraussetzung hierfür wird jedoch sein, dass das Übereinkommen international auf breiter Ebene umgesetzt wird, was zum heutigen Zeitpunkt angesichts der komplexen Materie, seiner Interpretationsbedürftigkeit sowie des ausgesprochen weiten Anwendungsbereichs der prozessualen Bestimmungen nicht

¹⁸ Bericht der Expertenkommission "Netzwerkkriminalität", op. cit., S. 76 ff.

der Fall ist. Die Frage des Anpassungsbedarfs im schweizerischen Recht wird mittelfristig massgeblich davon abhängen, inwieweit von der Möglichkeit von Vorbehalten und Erklärungen zum Konventionstext Gebrauch gemacht wird. In jedem Fall muss eine gegenseitige Abstimmung mit den Arbeiten an der Schweizerischen Strafprozessordnung erfolgen.

Nicht erforderlich ist aber die von der Expertenkommission in ihrem Bericht¹⁹ verlangte Ergänzung des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)²⁰, da gemäss einer veröffentlichten Entscheid der Rekurskommission des Eidgenössischen Departements für Umwelt, Verkehr, Energie und Kommunikation vom 27. April 2004²¹ der Gesetzgeber mit Artikel 14 Absatz 4 BÜPF eine Spezialnorm geschaffen hat, welche bei jeder über das Internet begangenen strafbaren Handlung in einem vereinfachten Verfahren eine umfassende Auskunftspflicht zur Identifikation der Urheberschaft vorsieht. Diese Auskunftspflicht gilt unabhängig davon, ob die Daten unter das Fernmeldegeheimnis fallen. Auskunftsgesuche im Sinne von Artikel 14 Absatz 4 BÜPF gelten demnach auch dann nicht als Überwachungsmassnahmen, wenn sie sich auf eine dynamisch zugeteilte IP-Adresse beziehen und Randdaten bzw. Daten zur Teilnehmeridentifikation zum Gegenstand haben. Im Einklang mit dem Wortlaut ist der Zweck von Artikel 14 Absatz 4 BÜPF somit darin zu sehen, dass der Internet-Provider bei jeder über das Internet begangenen strafbaren Handlung und damit unabhängig vom Strafkatalog von Artikel 3 BÜPF zur Auskunft verpflichtet und diese Auskunftspflicht nicht auf bestimmte Daten beschränkt ist.

2.3 Erläuterungen der einzelnen Bestimmungen²²

2.31 Strafgesetzbuch

Wie bereits erwähnt, ist eine gewisse Parallelität der vorgeschlagenen Regelung mit dem geltenden Medienstrafrecht gegeben. Die vorgeschlagenen Normtexte sind aber in mehrfacher Hinsicht nicht einfach das Spiegelbild der geltenden Artikel 27 und 322^{bis} StGB bzw. 26a MStG. Die neue Regelung erfasst jedes Netzwerkdelikt und ist somit nicht wie das Medienstrafrecht auf die Mediendelikte beschränkt. Im Medienstrafrecht ist eine strafrechtliche Haftung des verantwortlichen Redaktors bzw. der für die Veröffentlichung verantwortlichen Person an die Voraussetzung geknüpft, dass der Autor nicht ermittelt oder in der Schweiz nicht vor Gericht gestellt werden kann (Kaskadenhaftung). Diesen Ausschluss der Strafbarkeit gibt es bei Straftaten mittels elektronischer Kommunikationsnetze nicht. Auch wenn der Autor oder Content-Provider ermittelt oder in der Schweiz vor Gericht gestellt werden kann, bleibt die Strafbarkeit des Hosting-Providers gemäss Artikel 322^{bis} VE-StGB bestehen. Zudem ist bei den Netzwerkdelikten im Gegensatz zu den Mediendelikten (Art. 322^{bis} Satz 2 StGB) die fahrlässige Begehung straflos.

¹⁹ Bericht der Expertenkommission "Netzwerkriminalität", op. cit., S. 142 f.

²⁰ SR 780.1

²¹ Der Entscheid der Rekurskommission UVEK vom 27.4.2004 kann abgerufen werden unter: http://www.reko-inum.admin.ch/de/display_file.php?fname=114010669724120&query=.

²² Für weitere Erläuterungen vgl. Bericht Expertenkommission „Netzwerkriminalität“, insbesondere S. 93 ff.

2.311 Ergänzung des Randtitels im 6. Abschnitt des Zweiten Titels StGB

Die vorgeschlagene Ergänzung des Randtitels im 6. Abschnitt des Zweiten Titels des StGB mit dem Begriff „in elektronischen Kommunikationsnetzen“ ist technologieunabhängig und bezieht sich bewusst nicht ausschliesslich auf das Internet; unter den Begriff „Kommunikationsnetz“ fallen nicht nur der Zusammenschluss von Computern, sondern auch andere Telekommunikationsmittel. So kann z.B. eine ehrverletzende Äusserung oder ein pornografisches Bild sowohl via Internet (E-Mail, WWW), Mobiltelefonnetz (SMS, MMS) oder ein geschlossenes lokales Firmennetz (LAN), das sich nicht unbedingt der Internet-Technologie bedienen muss, übertragen werden. Es ist auch unerheblich, ob die fraglichen Informationen über Leitungen oder drahtlos erfolgen oder andere Übertragungsstrukturen verwendet werden (Telefon- oder Stromleitungen). Es spielt keine Rolle, ob die Informationen einseitig (wie z.B. im Rahmen traditioneller Radio- und Fernsehsendungen) oder auf zweiseitigem Datenaustausch basieren (wie z.B. beim Telefongespräch oder dem Versenden und Empfangen elektronischer Post).

Mit dem Begriff „in elektronischen Kommunikationsnetzen“ sollen sämtliche durch die Übermittlung, das Bereitstellen oder Bereithalten von Informationen in Telekommunikationsnetzen begangene Straftaten erfasst werden. Für die „klassischen“ Medien delikte gilt nach wie vor das geltende Medienstrafrecht, das in die neue Regelung integriert wird (als Art. 27^{bis} und als Ziff. 2 von Art. 322^{bis} VE-StGB).

2.312 Strafrechtliche Verantwortlichkeit der Provider

Artikel 27 VE-StGB Strafbarkeit in elektronischen Kommunikationsnetzen

Wie bereits dargelegt, ist der Begriff der elektronischen Kommunikationsnetze umfassender als derjenige der Medien. Deshalb wird die neue Vorschrift über die Strafbarkeit in elektronischen Kommunikationsnetzen an den Anfang der ganzen Regelung gestellt, während die geltende medienstrafrechtliche Norm als Artikel 27^{bis} VE-StGB folgt. Mit der gleichen Begründung erfolgt im Übrigen die entsprechende Umstellung beim neuen Artikel 322^{bis} VE-StGB. Der geltende Artikel 322^{bis} StGB wird als Ziffer 2 übernommen. Der geltende Artikel 27^{bis} (Quellenschutz) StGB wird zum neuen Artikel 27^{ter} VE-StGB.

Absatz 1 Content-Provider

Der neue Artikel 27 VE-StGB statuiert in Absatz 1, dass primär für die Internet-Provider die allgemeinen Regeln des StGB, d.h. die Regeln über Täter-, Mittäter-, Gehilfenschaft und Anstiftung gelten. Dieser Grundsatz gilt für den Content-Provider als Autor der illegalen Information. Er gilt aber ebenso für den Access- oder den Hosting-Provider, der sich aktiv an der Bereitstellung oder Bereithaltung von illegalen Informationen beteiligt. Die Strafbarkeit oder die Straflosigkeit des Providers hängt somit nicht von seinem Status, sondern von seiner Funktion ab, die er im einzelnen Kommunikationsvorgang einnimmt. Dieser Grundsatz gilt unter Vorbehalt der nachfolgenden Bestimmungen in den Absätzen 2 - 4.

„Übertragung, Bereitstellen und Bereithalten“ sind drei aus netzwerkspezifischer Sicht grundlegende Operationen. Übertragen meint das elektronische Senden und

Empfangen von Informationen über Leitungen und Funk; Bereitstellen ist das Aufladen von Informationen auf ein öffentliches, durch elektronische Kommunikationsnetze zugängliches Speichermedium und das Bereithalten bedeutet das Unterhalten eines Speichermediums, auf dem Informationen abgespeichert sind. Das letzte Glied in diesem Kommunikationsprozess wäre das Abrufen durch den Nutzer, das nicht strafbar ist. Strafbar ist aber im Sinne von Artikel 197 Ziffer 3^{bis} StGB seit dem 1. April 2002 das Abspeichern bzw. Herunterladen (so genanntes „Download“ oder „Downloading“) von Dateien mit pornografischem Inhalt.

„Informationen“ ist ein breiter Begriff, der insbesondere auch Computerprogramme einschliesst. Dieser wird im Fernmeldegesetz²³ wie auch in der E-Commerce-Richtlinie verwendet. Damit ist die vorgeschlagene Regelung nicht auf „Äusserungsdelikte“, wie z.B. Gewaltdarstellungen (Art. 135 StGB), Pornografie (Art. 197 StGB) oder Rasendiskriminierung (Art. 261^{bis} StGB) im Internet beschränkt, sondern sie geht weiter. Sie erfasst auch die übrige Computerkriminalität wie z.B. Anleitungen zur Herstellung von Computer-Viren (Art. 144^{bis} StGB) oder betrügerische Angebote auf dem WWW (Art. 146 StGB) und urheberstrafrechtliche Delikte, wie z.B. Musikpiraterie (Art. 67 und 69 Urheberrechtsgesetz URG²⁴).

Absatz 2 Abgrenzung zum Medienstrafrecht

Ist der Content-Provider Autor oder Redaktor im Sinne des Medienstrafrechts von Artikel 27 StGB bzw. Artikel 27^{bis} VE-StGB, d.h. wird eine strafbare Handlung durch Veröffentlichung in einem Online-Medium, wie z.B. einer im Internet publizierten Tageszeitung begangen, so findet die in Artikel 27^{bis} VE-StGB vorgesehene Regelung Anwendung. Allerdings nennt der Vorbehalt nur die Autoren und die Redaktoren und nicht die im geltenden Artikel 27 Absatz 2 StGB erfassten „für die Veröffentlichung verantwortlichen Personen“. Dies deshalb, weil bei strafbaren Handlungen, die mittels automatisierter Prozesse in elektronischen Kommunikationsnetzen begangen werden, die für die Veröffentlichung verantwortlichen Hosting- und Access-Provider unter Ausschluss der Autoren und Redaktoren der vorliegenden Neuregelung unterstellt werden sollen. Die Beschränkung des Vorbehaltes zugunsten des Medienstrafrechtes auf Autoren und Redaktoren soll dies gewährleisten.

Absatz 3 Hosting-Provider

Absatz 3 unterscheidet zwischen dem Regelfall der automatisiert ablaufenden Datentransfers, deren Inhalt der Hosting-Provider nicht kennt, und jenen Fällen, in denen er im Nachhinein die strafrechtliche Relevanz der Informationen erkennt oder davon erfährt. Im ersteren Fall ist er straflos; im zweiten Fall ist er gemäss Artikel 322^{bis} Ziffer 1 VE-StGB strafbar.

Viele Internet-Nutzer beginnen ihre Nachforschungen über eine so genannte Suchmaschine (wie z.B. google.ch oder altavista.com). Neu soll der Betreiber derartiger Suchmaschinen in strafrechtlicher Hinsicht den Hosting-Providern gleichgestellt werden. Diese Ergänzung in Absatz 3, Satz 2 ist notwendig, weil die Informationen, die der Index der Suchmaschine enthält, nicht mehr "fremd" im Sinne von Satz 1 sind. Es

²³ Vgl. dazu die Legaldefinition in Art. 3 lit. a des Fernmeldegesetzes vom 30. April 1997 (FMG; SR 784.10): "Informationen: für Menschen, andere Lebewesen oder Maschinen bestimmte Zeilen, Signale, Schriftzeichen, Bilder, Leute und Darstellungen jeder anderen Art."

²⁴ SR 231.1

ist nicht irgendein Content-Provider, der seine Informationen auf dem Rechner des Suchmaschinenbetreibers bereitstellt, sondern der Betreiber der Suchmaschine selbst, der automatisiert eine Datenbank erstellt. Was in diesem Index steht, ist eigener Inhalt und wäre folglich nach Artikel 27 Absatz 1 VE-StGB zu beurteilen.

Absatz 4 Access-Provider

Wie bereits erwähnt und erläutert, ist bei Anwendung der allgemeinen Bestimmungen des StGB nicht auszuschliessen, dass der Access-Provider z.B. als Gehilfe zur Haupttat des Content-Providers bestraft wird. Im Normalfall beschränkt sich aber die Dienstleistung des Access-Providers auf das zur Verfügung Stellen eines Zugangs zum Internet. Wenn sich die Beteiligung des Access-Providers auf die reine Zugangsvermittlung beschränkt, ist diese nach Absatz 4 straflos. Der Nutzer bedient sich der verschiedenen Internetdienste zur Kommunikation oder Informationsbeschaffung und benötigt dafür einen Netzzugang.

Nach dieser Bestimmung ist auch die automatische kurzzeitige Zwischenspeicherung von fremden Informationen als Zugangsvermittlung zu verstehen. Entgegen der E-Commerce-Richtlinie der EU²⁵ schlägt der Bundesrat vor, nicht zwischen der technisch bedingten Zwischenspeicherung und dem so genannten Proxy-Caching, d.h. der kurzzeitigen Zwischenspeicherung durch den Access-Provider, die bei häufig abgerufenen Inhalten einen effizienteren Datenabruf für alle Kunden des Access-Providers ermöglicht, zu unterscheiden. Diese flexible Lösung ist einer differenzierteren Regelung vorzuziehen, da eine Abgrenzung in generell-abstrakter Form in einem sich ständig wandelnden technischen Umfeld kaum möglich ist. Von der Straflosigkeit nicht erfasst, wird das so genannte „Mirroring“, d.h. das Überspielen eines bestimmten Internet-Angebotes durch aktive Handlungen eines Anbieters auf einen anderen Rechner, etwa um die Zugriffszeiten auf einen besonders belasteten Rechner zu verkürzen. Erfasst werden nur die Fälle, in denen es sich um eine automatische, durch Nutzerabfrage bedingte Zwischenspeicherung handelt.

Artikel 27^{bis} VE-StGB Strafbarkeit der Medien

Artikel 27^{bis} VE-StGB übernimmt die Regelung des geltenden Artikels 27 StGB mit der Änderung, dass in Absatz 2 neu auf Artikel 322^{bis} Ziffer 2 VE-StGB verwiesen wird.

Artikel 322^{bis} VE-StGB Nichtverhindern strafbarer Handlungen in elektronischen Kommunikationsnetzen und in Medien

Ziffer 1 Absatz 1

Absatz 1 regelt die im neuen Artikel 27 Absatz 3 VE-StGB statuierte Strafbarkeit des Hosting-Providers. Dabei handelt es sich um ein echtes Sonderdelikt: Täter kann nur sein, wer fremde Informationen automatisiert in einem Kommunikationsnetz bereithält. Gemeint sind die Hosting-Provider, auf deren Rechnern die Kunden, d.h. die Content-Provider Informationen aufschalten, ohne dass die Hosting-Provider darauf einen Einfluss hätten.

²⁵ Vgl. Art.12 Abs. 2 und Art.13 der E-Commerce-Richtlinie .

Ziffer 1 Absatz 1 verankert ein echtes Unterlassungsdelikt: Der Vorwurf an den Hosting-Provider geht dahin, dass er - obwohl es ihm technisch möglich und zumutbar war - die Nutzung einer Datei, von der er sicher weiss, dass sie z.B. rassendiskriminierende, pornografische oder gewaltverherrlichende Inhalte aufweist, nicht verhindert. Der Unrechtskern ist somit nicht die Beteiligung am Hauptdelikt, sondern das Untätigbleiben mit Blick auf die weitere Verbreitung der illegalen Information.

Verlangt wird, dass mittels der fremden Information eine strafbare Handlung begangen wird. Zum einen kommen diejenigen Strafnormen in Betracht, die klassischerweise zur Netzwerkkriminalität gezählt werden, wie die Gewaltdarstellungen (Art. 135 StGB), die Pornografie (Art. 197 StGB) oder die Rassendiskriminierung (Art. 261^{bis} StGB). Zum anderen gehören aber auch sämtliche Straftaten dazu, zu deren Begehung der Einsatz elektronischer Kommunikationsmittel denkbar ist, also etwa die so genannten Computerdelikte, aber auch die klassischen Vermögensdelikte (z.B. Betrug, Art. 146 StGB) und die Delikte des Nebenstrafrechts, v.a. jene im Zusammenhang mit dem Unlauteren Wettbewerb oder dem Urheber- und Markenschutz.

Ziffer 1 Absatz 2

Ziffer 1 Absatz 1 verlangt sicheres Wissen, um die Strafbarkeit der Unterlassung des Hosting-Providers zu begründen. Daraus ergibt sich die Frage, was mit demjenigen Hosting-Provider zu geschehen hat, der solches sicheres Wissen nicht erlangt, weil z.B. die Hinweise, die bei ihm eingehen, mangelhaft sind. Bleibt der Hosting-Provider in einem solchen Fall passiv, vermag er das von Absatz 1 verlangte nötige Wissen nie zu erlangen und bliebe straflos. Das will der neue Absatz 2 verhindern. Die Strafbarkeit des Hosting-Providers ist nach Absatz 2 deshalb auch gegeben, wenn er es unterlässt, Hinweise von Dritten auf Informationen, mittels deren eine strafbare Handlung begangen wird, den Strafverfolgungsbehörden zur Kenntnis zu bringen. Wichtig ist dabei, dass diese Weiterleitungspflicht allein durch individuell an den Hosting-Provider gerichtete Meldungen ausgelöst wird, nicht aber durch allgemein zugängliche Informationen, wie etwa solche aus Presse, Radio oder Fernsehen.

Zudem ist der Hosting-Provider nur weiterleitungspflichtig bezüglich der Hinweise auf Dateien, die er selber „hostet“. Diese Weiterleitungspflicht trifft also nur den Hosting-Provider, der solch sicheres Wissen nicht erlangen kann und trotz unvollständiger oder mangelhafter Hinweise passiv bleibt. In diesem Sinne handelt es sich nicht um eine generelle Anzeigepflicht, auch wenn ein vorsichtiger Hosting-Provider sämtliche eingehenden Hinweise an die Strafverfolgungsbehörden weiterleiten wird.

Mit den Absätzen 1 und 2 ist der rechtspolitische Zweck der Inpflichtnahme der Hosting-Provider erfüllt. Man kann von ihnen nicht verlangen, Straftaten ihrer Kunden, d.h. der Content-Provider, welche diese durch die Publikation auf dem Internet-Server begangen haben, ganz zu verhindern; denn sie haben ja auf den Vorgang der Aufschaltung der konkreten Inhalte keinen Einfluss. Hingegen kann man sie – und darin liegt ja das eigentliche gesetzgeberische Ziel – sehr wohl dazu anhalten, solche Straftaten in ihren Folgen zu begrenzen, dass sie die Kenntnisnahme der entsprechenden Inhalte dadurch verunmöglichen, indem sie die Nutzung technisch verunmöglichen oder im Sinne von Absatz 2 die eingegangenen Hinweise an die Strafverfolgungsbehörde weiterleiten.

Sowohl Absatz 1 als auch Absatz 2 sehen als Strafen Gefängnis (drei Tage bis drei Jahre; Art. 36 StGB) oder Busse (bis zu 40'000 Franken; Art. 48 StGB) vor²⁶. Dies ist eine angemessene Strafdrohung, wie ein Blick auf die Haupttaten zeigt. So drohen die Artikel 135, 197 und 261^{bis} StGB ebenfalls Gefängnis oder Busse an. Die vorgeschlagene Strafdrohung ist aber auch gerechtfertigt, wenn man sich den rechtspolitischen Zweck der Inpflichtnahme des Hosting-Providers vor Augen hält: Begrenzung der Folgen der Straftat seines Kunden, des Content-Providers, indem er die Kenntnisnahme des entsprechenden illegalen Inhaltes verunmöglicht.

Ziffer 1 Absatz 3

Handelt es sich bei der strafbaren Handlung im Internet um ein Antragsdelikt, sieht Absatz 3 vor, dass die Tat auch nur verfolgt wird, wenn ein Antrag auf Verfolgung der strafbaren Handlung vorliegt. Fehlt ein solcher Antrag bezüglich der Haupttat, wird auch kein Verfahren gegen den Hosting-Provider eingeleitet. Eine analoge Regelung kennt das StGB schon bei der Hehlerei (Art. 160 StGB). Wenn ein Hinweis auf ein Antragsdelikt beim Hosting-Provider eingeht, wird dieser häufig nicht wissen, ob ein Antrag vorliegt. Er wird deshalb im Zweifel die Meldungen unabhängig vom Antragsanfordernis weiterleiten. Absatz 3 soll das stossende Ergebnis verhindern, dass der Hosting-Provider wegen unterlassener Weiterleitung nach Absatz 2 bestraft wird, obwohl derjenige, der von der angeblich strafbaren Handlung betroffen ist, deren Verfolgung und damit auch die Bestrafung ablehnt.

Ziffer 1 Absatz 4

Nach welchem Recht ist zu entscheiden, ob eine strafbare Handlung vorliegt? Die Antwort auf diese Frage gibt der neue Absatz 4: „Ob mittels einer Information eine strafbare Handlung begangen wird, beurteilt sich nach schweizerischem Recht“. Der Zugriff auf den Hosting-Provider soll auf diese Weise auch in denjenigen Fällen möglich sein, in denen die beanstandete Handlung nach dem Recht des Ortes ihrer Ausführung nicht strafbar ist.

Von praktischer Bedeutung könnten in diesem Zusammenhang z.B. Äusserungen aus dem angloamerikanischen oder australischen Rechtskreis sein, die dort wegen der Meinungsäusserungsfreiheit straflos sind, in der Schweiz aber als rassendiskriminierend gelten würden. Mit der Strafbarkeit des Hosting-Providers in den vorgeschlagenen Absätzen 1 und 2 soll verhindert werden, dass die strafrechtlich relevante Information weiterhin von einem schweizerischen Server abgerufen werden kann. Ein Interesse an solcher Verhinderung besteht aber nur, wenn die betreffende Datei nach schweizerischem Recht illegale Informationen enthält.

²⁶ Bei Inkrafttreten der Änderung des StGB (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) vom 13. Dezember 2002 (BBl 2002 8240) wird der Ausdruck „Gefängnis oder Busse“ durch „Freiheitsstrafe bis zu drei Jahren oder Geldstrafe“ ersetzt. Da die Geldstrafe neu nach dem Tagessatzsystem bemessen wird, erhöht sich der Maximalbetrag der Geldstrafe neu auf Fr. 1'080'000.- (360 Tagessätze à Fr. 3000.-; vgl. Art. 34 nStGB).

Ziffer 1 Absatz 5

Gemäss Absatz 5 werden Informationen im Sinne der Absätze 1 und 2, d.h. solche, mittels deren eine strafbare Handlung begangen wurde, gelöscht. Die Löschung der Information als Pendant zur Einziehung (Art. 58 StGB) ist wie diese materiell-rechtlicher Natur. Sie wird vom Gericht im Urteil angeordnet. Absatz 5 verkörpert keine prozessuale Bestimmung analog der Beschlagnahme, mittels deren schon die Strafverfolgungsbehörde die Information vorläufig sperren könnte. Eine solche ist der Strafprozessgesetzgebung vorbehalten. Im Vordergrund steht hier eine Sperrverfügung; diese hat sich als prozessuale Zwangsmassnahme auf entsprechende Bestimmungen zu stützen.

Nach der Löschung dürfen die illegalen Inhalte nicht mehr rekonstruierbar sein. Die Löschung der Informationen wird - wie bereits erwähnt - vom Gericht angeordnet, wenn es zu einer Verurteilung des Hosting-Providers kommt. Inwiefern eine Löschung auch im Falle eines Freispruchs oder bei prozessualer Erledigung der Sache in Betracht fällt, ist im Sinne der Expertenkommission wie folgt zu lösen: Scheitert eine Verurteilung des Hosting-Providers beispielsweise daran, dass sich ihm kein sicheres Wissen um die Strafbarkeit der Information, sondern nur allenfalls Eventualvorsatz nachweisen lässt, so kann die Löschung vom Gericht trotzdem angeordnet werden. Die Löschung erfolgt zudem auch „ungeachtet schweizerischer Hoheit“. Es wäre nämlich eine rechtspolitisch unbefriedigende Situation, wenn zwar in dem den Hosting-Provider freisprechenden Urteil festgestellt würde, ein Content-Provider habe einen tatbestandsmässig rechtswidrigen Inhalt auf dessen Rechner geladen, eine Löschung der entsprechenden Information sei jedoch nicht möglich, weil für die Tat des Content-Providers keine schweizerische Strafhöhe bestehe. Es kommt demnach für die Löschung nicht darauf an, ob für die Tat des Content-Providers schweizerische Strafhöhe vorliegt. Auch wenn dies nicht der Fall ist, werden die Informationen auf dem Internet-Server des Hosting-Providers gelöscht.

Ziffer 2

Ziffer 2 übernimmt die Regelung des geltenden Artikels 322^{bis} StGB mit der Änderung, dass neu auf Artikel 27^{bis} VE-StGB verwiesen wird.

2.32 Militärstrafgesetz

Wie bei Revisionen des bürgerlichen Strafgesetzbuches üblich, ist auch das Militärstrafgesetz entsprechend zu ändern, sofern sich dieselbe Vorschrift in beiden Gesetzen findet (vgl. unten Ziff. 2.42).

2.4 Vorentwurf A

2.41 Schweizerisches Strafgesetzbuch

(neuer Titel) 6. Strafbarkeit in elektronischen Kommunikationsnetzen und in Medien ²⁷

Artikel 27 VE-StGB

Strafbarkeit in elektronischen Kommunikationsnetzen ²⁸

¹ Wird eine strafbare Handlung mittels Übertragung, Bereitstellen oder Bereithalten von Informationen in einem elektronischen Kommunikationsnetz begangen, so gelten die allgemeinen Bestimmungen dieses Gesetzes über Täterschaft und Teilnahme. Vorbehalten bleiben die nachfolgenden Bestimmungen:

² Ist der Täter Autor oder Redaktor im Sinne von Artikel 27^{bis}, so richtet sich die Strafbarkeit nach dieser Bestimmung.

³ Wer fremde Informationen zur Nutzung in einem elektronischen Kommunikationsnetz automatisiert bereithält, macht sich unter den Voraussetzungen von Artikel 322^{bis} Ziffer 1 strafbar. Das Bereithalten eines Verzeichnisses, in welches fremde Informationen automatisiert aufgenommen werden, gilt als Bereithalten fremder Informationen.

⁴ Wer lediglich den Zugang zu einem elektronischen Kommunikationsnetz vermittelt, ist nicht strafbar. Eine automatische und kurzzeitige Speicherung fremder Informationen infolge Nutzerabfrage gilt als Zugangsvermittlung.

Artikel 27 StGB wird zu Artikel 27^{bis} VE-StGB ***Strafbarkeit der Medien*** ²⁹

¹ ...

² Kann der Autor nicht ermittelt oder in der Schweiz nicht vor Gericht gestellt werden, so ist der verantwortliche Redaktor nach Artikel 322^{bis} Ziffer 2 strafbar. Fehlt ein verantwortlicher Redaktor, so ist jene Person nach Artikel 322^{bis} Ziffer 2 strafbar, die für die Veröffentlichung verantwortlich ist.

³ ...

⁴ ...

²⁷ Bei Inkrafttreten der Änderung des StGB (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) vom 13. Dezember 2002 (BBI 2002 8240) ersetzt der Titel 6. Strafbarkeit in elektronischen Kommunikationsnetzen und in Medien den Titel 6. Strafbarkeit der Medien.

²⁸ Bei Inkrafttreten der Änderung des StGB (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) vom 13. Dezember 2002 (BBI 2002 8240) wird Artikel 27 zu Artikel 28.

²⁹ Bei Inkrafttreten der Revision vom 13. Dezember 2002 des Allgemeinen Teils des StGB (BBI 2002 8240) wird Artikel 27^{bis} zu Artikel 28a.

**Artikel 27^{bis} StGB wird unverändert zu Artikel 27^{ter} VE-StGB
Quellenschutz³⁰**

Artikel 322^{bis} VE-StGB

Nichtverhindern strafbarer Handlungen in elektronischen Kommunikationsnetzen und in Medien

1. Wer in einem elektronischen Kommunikationsnetz fremde Informationen automatisiert bereithält, mittels deren, wie er sicher weiss, eine strafbare Handlung begangen wird, und es unterlässt, die Nutzung dieser Informationen zu verhindern, obwohl es ihm technisch möglich und zumutbar ist, wird mit Gefängnis oder Busse bestraft³¹.

Wer in einem elektronischen Kommunikationsnetz fremde Informationen automatisiert bereithält, mittels deren eine strafbare Handlung begangen wird, und es unterlässt, von Dritten an ihn gerichtete und bei ihm eingegangene Hinweise auf solche Informationen an die Strafverfolgungsbehörden weiterzuleiten, wird mit Gefängnis oder Busse bestraft.

Handelt es sich bei der strafbaren Handlung um ein Antragsdelikt, so wird die Tat nur verfolgt, wenn ein Antrag auf Verfolgung der strafbaren Handlung vorliegt.

Ob mittels einer Information eine strafbare Handlung begangen wird, beurteilt sich nach schweizerischem Recht.

Informationen im Sinne der Absätze 1 und 2 werden ungeachtet schweizerischer Strafhoheit gelöscht.

2. Wer als Verantwortlicher nach Artikel 27^{bis} Absätze 2 und 3 eine Veröffentlichung, durch die eine strafbare Handlung begangen wird, vorsätzlich nicht verhindert, wird mit Gefängnis oder Busse bestraft. Handelt der Täter fahrlässig, so ist die Strafe Haft oder Busse.

³⁰ Bei Inkrafttreten der Änderung des StGB (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) vom 13. Dezember 2002 (BBI 2002 8240) wird Artikel 27^{ter} zu Artikel 28b

³¹ Bei Inkrafttreten der Änderung des StGB (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) vom 13. Dezember 2002 (BBI 2002 8240) wird der Ausdruck „Gefängnis oder Busse“ durch „Freiheitsstrafe bis zu drei Jahren oder Geldstrafe“ ersetzt. Da die Geldstrafe neu nach dem Tagessatzsystem bemessen wird, erhöht sich der Maximalbetrag der Geldstrafe neu auf Fr. 1'080'000.- (360 Tagessätze à Fr. 3000.-; vgl. Art. 34 n StGB).

2.42 Militärstrafgesetz

(neuer Titel) 8. Strafbarkeit in elektronischen Kommunikationsnetzen und in Medien³²

Artikel 26a VE-MStG

Strafbarkeit in elektronischen Kommunikationsnetzen³³

¹ Wird eine strafbare Handlung mittels Übertragung, Bereitstellen oder Bereithalten von Informationen in einem elektronischen Kommunikationsnetz begangen, so gelten die allgemeinen Bestimmungen dieses Gesetzes über Täterschaft und Teilnahme. Vorbehalten bleiben die nachfolgenden Bestimmungen:

² Ist der Täter Autor oder Redaktor im Sinne von Artikel 26b, so richtet sich die Strafbarkeit nach dieser Bestimmung.

³ Wer fremde Informationen zur Nutzung in einem elektronischen Kommunikationsnetz automatisiert bereithält, macht sich unter den Voraussetzungen von Artikel 322^{bis} Ziffer 1 des Strafgesetzbuches strafbar. Das Bereithalten eines Verzeichnisses, in welches fremde Informationen automatisiert aufgenommen werden, gilt als Bereithalten fremder Informationen.

⁴ Wer lediglich den Zugang zu einem elektronischen Kommunikationsnetz vermittelt, ist nicht strafbar. Eine automatische und kurzzeitige Speicherung fremder Informationen infolge Nutzerabfrage gilt als Zugangsvermittlung.

Artikel 26a MStG wird zu Artikel 26b VE-MStG

Strafbarkeit der Medien³⁴

¹ ...

² Kann der Autor nicht ermittelt oder in der Schweiz nicht vor Gericht gestellt werden, so ist der verantwortliche Redaktor nach Artikel 322^{bis} Ziffer 2 des Strafgesetzbuches strafbar. Fehlt ein verantwortlicher Redaktor, so ist jene Person nach Artikel 322^{bis} Ziffer 2 des Strafgesetzbuches strafbar, die für die Veröffentlichung verantwortlich ist.

³ ...

⁴ ...

³² Bei Inkrafttreten der Änderung des MStG (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) vom 21. März 2003 (BBI 2003 2808) wird der Titel 8. Strafbarkeit in elektronischen Kommunikationsnetzen und in Medien durch den Titel 6. Strafbarkeit in elektronischen Kommunikationsnetzen und in Medien ersetzt.

³³ Bei Inkrafttreten der Änderung des MStG (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) vom 21. März 2003 (BBI 2003 2808) wird Artikel 26a zu Artikel 27.

³⁴ Bei Inkrafttreten der Änderung des MStG (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) vom 21. März 2003 (BBI 2003 2808) wird Artikel 26b zu Artikel 27a

**Artikel 26b MStG wird unverändert zu Artikel 26c VE-MStG
Quellenschutz³⁵**

³⁵ Bei Inkrafttreten der Änderung des MStG (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) vom 21. März 2003 (BBl 2003 2808) wird Artikel 26c zu Artikel 27b

3. Kompetenzen des Bundes bei strafbaren Handlungen mittels elektronischer Kommunikationsnetze (Vorentwurf B)

3.1 Vorschläge der Arbeitsgruppe "Genesis"

Die Arbeitsgruppe "Genesis" befasste sich vorwiegend mit rechtlichen Verbesserungsvorschlägen, die nach eingehender Analyse der Operation „Genesis“ nötig erscheinen und eine Effizienzsteigerung in der Strafverfolgung von Netzwerkkriminalität bringen sollen.

3.11 Strafverfolgung bei Tatbegehung mittels elektronischer Kommunikationsnetze

In ihrem Bericht³⁶ legt die Arbeitsgruppe "Genesis" dar, weshalb Ermittlungen im Bereich der Netzwerkkriminalität, sowohl in personeller als auch in technischer Hinsicht eine grosse Herausforderung darstellen. Die Schwierigkeiten sind vielschichtig. Erwähnt seien in diesem Zusammenhang etwa die personalintensive und technisch sehr aufwändige Sicherstellung von Beweismaterial, da es den Tätern ein Leichtes ist, in dieser virtuellen Welt der elektronischen Kommunikationsnetze anonym zu bleiben oder nach begangener Tat die Spuren zu verwischen. Es handelt sich in der Regel auch um komplexe Fälle mit Bezügen zum Ausland, die sich unter Umständen - wie im Fall „Genesis“ - auf mehrere Kantone verteilen können. Schliesslich sind die technische Ausrüstung und die personelle Aus- und Weiterbildung für die Ermittlung besonders kostenintensiv.

3.12 Analyse der Operation „Genesis“

Die Operation „Genesis“ hat diese spezielle Problematik bei der Kriminalitätsbekämpfung im Internet deutlich zutage gefördert. Gleichzeitig stellte der Umfang des sicher gestellten Beweismaterials sowie die Tatsache, dass 25 Kantone (ohne Appenzell Innerrhoden) für die Strafverfolgung zuständig waren, die schweizerischen Ermittlungsbehörden vor eine völlig neue Situation.

Die Analyse der Arbeitsgruppe „Genesis“ kommt zum Schluss, dass in der Zusammenarbeit zwischen Bund und Kantonen Handlungsbedarf besteht und zwar in den Bereichen der Vorbereitung von „Genesis“-ähnliche Operationen, der technischen Auswertung des Beweismaterials, der Ausbildung sowie der Medienarbeit. Dazu gesellt sich als entscheidender Mangel, dass der Bund keine gesetzliche Möglichkeit hat, z.B. die Kundendaten bei den Kreditkartenfirmen zentral abzuklären. Eine solche Befugnis hätte es den Bundesbehörden bei der Operation "Genesis" ermöglicht, die kantonalen Zuständigkeiten rascher abzuklären und den betroffenen Kantonen die entsprechenden Fälle speditiver zuzuteilen. Mangels gesetzlicher Grundlage konnte der Bund ferner auf die zeitlichen Abläufe in den betroffenen 25 Kantonen keinen Einfluss nehmen. Die Koordination durch fedpol wurde dadurch stark erschwert.

³⁶ Bericht der Arbeitsgruppe "Genesis", op. cit., S. 32 f.

Die beiden letztgenannten Mängel, die zu einem bedeutenden Effizienzverlust führten, sind in der ersten Verfahrensphase zu lokalisieren. Beim grössten Teil der mittels elektronischer Kommunikationsmittel begangenen Delikte liegt die Strafverfolgungskompetenz bei den Kantonen³⁷, und der Bund hat in diesen Fällen einzig die Möglichkeit, interkantonale und internationale Ermittlungen zu koordinieren³⁸. Der gesetzliche Rahmen erlaubt jedoch den Bundesbehörden weder selbst Ermittlungshandlungen vorzunehmen noch die Kantone zu solchen aufzufordern.

Für eine effiziente Bekämpfung der Netzwerkkriminalität genügen aber diese vorhandenen Möglichkeiten nicht, da das Deliktspotenzial des elektronischen Kommunikationsmittels zunimmt, je mehr Leute über dieses verfügen und dessen technische Möglichkeiten ausschöpfen können. Zudem haben bereits weitere grosse Fälle gezeigt, dass durch dieses Tatmittel auch in Zukunft vermehrt mit einer grösseren Zahl von gleichartigen Fällen, verteilt auf mehrere Kantone, zu rechnen ist. Die Arbeitsgruppe „Genesis“ hält deshalb in ihrem Bericht³⁹ fest, dass in der ersten Phase des Verfahrens eine Ermittlungsmöglichkeit des Bundes angezeigt ist.

3.13 Keine Bundeskompetenz zur Strafverfolgung von Netzwerkkriminalität

Eine allgemeine Zentralisierung der Strafverfolgung von in Netzwerken begangenen Delikten beim Bund, wie dies die parlamentarische Initiative Aeppli Wartmann (vgl. oben Ziff. 1.2) und die Expertenkommission „Netzwerkkriminalität“ (vgl. oben Ziff. 2.12) vorschlagen, lehnt die Arbeitsgruppe indessen ab.

Diese Forderung geht zu weit und ist auch sachlich nicht gerechtfertigt⁴⁰. So würde beispielsweise die verfassungsmässig verankerte Aufgabenteilung in der Strafverfolgung (kantonale Kompetenz als Regel, Bundesgerichtsbarkeit als Ausnahme) in Frage gestellt, weil die Kantone einen nicht geringen Teil ihrer Kompetenzen an den Bund abgeben müssten. Zudem wurde bei der Analyse der Operation „Genesis“ festgestellt, dass sich die Hauptprobleme im ersten Verfahrensabschnitt stellen, so dass eine Durchführung des gesamten Verfahrens durch den Bund nicht nötig ist⁴¹.

3.14 Vorgeschlagenes Modell

in Anlehnung an das Betäubungsmittelrecht⁴² hat die Arbeitsgruppe „Genesis“ ein Modell entwickelt, das eine Zentralisierung der Strafverfolgung beim Bund in der ersten Phase des Verfahrens ermöglicht, ohne jedoch die kantonalen Strafverfolgungskompetenzen anzutasten. Diese Idee hat sie in der Folge in ihrem Bericht in zwei Varianten konkretisiert (vgl. unten Ziff. 3.15 und 3.16)⁴³. Vorgeschlagen wird eine Ergänzung im StGB, weil so den Strafverfolgungsbehörden ein Ermittlungs-

³⁷ Vgl. Art. 343 StGB.

³⁸ Vgl. Art. 2 lit. b des Bundesgesetzes über die kriminalpolizeilichen Zentralstellen (ZentG; SR 360) und Art. 3 der Verordnung über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei vom 30. November 2001 (SR 360.1).

³⁹ Bericht der Arbeitsgruppe „Genesis“, op. cit., S. 5 ff.

⁴⁰ Bericht der Arbeitsgruppe „Genesis“, op.cit., S. 7 ff.

⁴¹ Bericht der Arbeitsgruppe „Genesis“, op. cit., S. 24 f.

⁴² Bundesgesetz vom 3. Oktober 1951 über die Betäubungsmittel und die psychotropen Stoffe (Betäubungsmittelgesetz, BetmG); SR 812.121

⁴³ Bericht der Arbeitsgruppe „Genesis“, op.cit., S. 9 ff. und 20 ff.

strument zur Verfügung gestellt wird, das mit wenig Aufwand und verhältnismässig rasch umgesetzt werden kann.

3.15 Variante 1 (Ermittlungskompetenz der Bundesanwaltschaft [BA] gemäss Art. 259 des Bundesgesetzes vom 15. Juni 1934 über die Bundesstrafrechtspflege [BStP]⁴⁴ gestützt auf eine Oberaufsicht des Bundes)

Die Ausgestaltung des vorgeschlagenen Modells lehnt sich – wie bereits erwähnt - an die Regelung im BetmG an (vgl. Art. 29 Abs. 4 BetmG in Verbindung mit Art. 259 BStP). Sie weist folgende Grundzüge auf:

Gestützt auf Artikel 259 BStP kann die BA einzelne, dringend notwendige Ermittlungen anordnen, wenn die strafbaren Handlungen - wie bei der Operation „Genesis“ - ganz oder teilweise im Ausland oder in mehreren Kantonen begangen wurden. Für die Anwendung des Artikels 259 BStP wird jedoch ein Oberaufsichtsrecht des Bundes bei der Verfolgung der betroffenen strafbaren Handlungen vorausgesetzt. Da ein solches Oberaufsichtsrecht sowohl im Spezialbereich der Pornografie (Art. 197 StGB) als auch generell im Bereich der Netzwerkkriminalität fehlt, müsste es eingeführt werden.

Die Arbeitsgruppe schlägt deshalb die Schaffung eines neuen Artikels 343^{bis} VE-StGB vor, der bei der Verfolgung von strafbaren Handlungen, die mittels elektronischer Kommunikationsnetze begangen wurden, eine Oberaufsicht des Bundes begründet.

Mit der Einführung einer solchen Oberaufsicht wäre neben der Anwendung von Artikel 259 BStP auch diejenige von Artikel 258 BStP möglich. Gestützt auf letztere Bestimmung hätte der Bund gegenüber den kantonalen Strafverfolgungsbehörden in dem Sinne eine Weisungsbefugnis, dass diese verpflichtet werden könnten, ein Verfahren einzuleiten und durchzuführen.

3.16 Variante 2 (Ermittlungskompetenz der zuständigen Bundesbehörde)

Die von der Arbeitsgruppe „Genesis“ vorgeschlagene Variante 2 verzichtet auf die Einführung eines besonderen, allgemeinen Oberaufsichtsrechts des Bundes; sie verfolgt aber das gleiche Ziel wie die Variante 1.

Die zuständigen Bundesbehörden sollen in Fällen von Netzwerkkriminalität, bei welchen die strafbaren Handlungen ganz oder teilweise im Ausland oder in mehreren Kantonen begangen wurden, einzelne, dringend notwendige Ermittlungen anordnen können, ohne dass eine Bundesgerichtsbarkeit begründet wird. Der Bund könnte auch nach dieser Variante den Kantonen zur Koordination der interkantonalen und internationalen Ermittlungen Weisungen erteilen.

Vorgeschlagen wird zu diesem Zweck die Schaffung eines Artikels 343^{bis} VE-StGB, der diese Ermittlungs- und Weisungsmöglichkeiten der zuständigen Bundesbehörde begründet.

⁴⁴ SR 312.0

3.17 Flankierende Massnahmen

Als flankierende Massnahme empfiehlt die Arbeitsgruppe "Genesis" zudem eine Ergänzung des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)⁴⁵. Die Provider sollen durch diese Ergänzung verpflichtet werden den zuständigen Bundesbehörden auch ausserhalb eines formellen Strafverfahrens über bestimmte Randdaten Auskunft zu geben. Damit würde eine speditivere Zuweisung der Fälle an die zuständigen kantonalen Strafverfolgungsbehörden gewährleistet⁴⁶.

3.2 Stellungnahme und Vorschlag des Bundesrates

Die Operation „Genesis“ hat unbestrittenermassen gezeigt, dass in Fällen, in denen eine Vielzahl von Personen und mehrere Kantone betroffen sind, bei der Zusammenarbeit zwischen Bund und Kantonen gesetzgeberischer Handlungsbedarf besteht. Konkret stellte sich im Fall „Genesis“ für den Bund das Problem der fehlenden Kompetenzen in der ersten Ermittlungsphase, wo es insbesondere um die Identifizierung der einzelnen Personen mit Blick auf die Zuweisung an die zuständigen kantonalen Strafverfolgungsbehörden, die Erhebung und Sicherstellung des Beweismaterials und generell um die Aufbereitung der Fälle ging. Wegen Fehlens einer Weisungskompetenz konnten zudem die Ermittlungen nicht gleichzeitig eingeleitet werden, was dazu führte, dass die Öffentlichkeit zu verschiedenen Zeitpunkten orientiert wurde, so dass einige der Zielpersonen bereits gewarnt wurden und dadurch einschlägiges Beweismaterial beseitigen konnten. Die von der Arbeitsgruppe „Genesis“ in ihrem Bericht vorgenommene Analyse hat den Bundesrat vom gesetzgeberischen Handlungsbedarf überzeugt.

Wie bereits erwähnt (vgl. oben Ziff. 2.2), ist eine wirkungsvolle Bekämpfung und eine effiziente Strafverfolgung der Netzwerkkriminalität auch für den Bundesrat ein erklärtes Ziel seiner Legislaturplanung 2003-2007.

3.21 Keine Bundeskompetenz zur Strafverfolgung von Netzwerkkriminalität

Der Bundesrat hat die beiden Vorschläge *Bundeskompetenz* gemäss Expertenkommission "Netzwerkkriminalität" (vgl. oben Ziff. 2.12) beziehungsweise *Ermittlungsmöglichkeiten des Bundes in der ersten Verfahrensphase* gemäss den Vorschlägen der Arbeitsgruppe "Genesis" (vgl. Ziff. oben 3.14 - 3.16) gegeneinander abgewogen. Eine Bundeskompetenz im Sinne einer Bundesgerichtsbarkeit lehnt der Bundesrat aus folgenden Gründen ab:

Die verfassungsmässig verankerte Aufgabenteilung in der Strafverfolgung (kantonale Kompetenz als Regel, Bundesgerichtsbarkeit als Ausnahme) würde mit einer solchen Bundeskompetenz in Frage gestellt, weil die Kantone dadurch einen nicht geringen Teil ihrer Kompetenzen abgeben müssten. Gleichzeitig würde eine Zuweisung der Kompetenz nach Tatmittel zu einem Ermittlungsparallelismus im selben Tatbestand führen. So wären z.B. bei der Pornografie, die im Kino oder mittels der Printmedien

⁴⁵ SR 780.1

⁴⁶ Bericht der Arbeitsgruppe "Genesis", op.cit., S. 27 f.

verbreitet wird, ausschliesslich die Kantone zuständig, bei jener aber, die mittels elektronischer Kommunikationsmittel verbreitet wird, wäre der Bund zuständig. Eine solche Ineffizienz in der Strafverfolgung gilt es zu vermeiden. Zudem handelt es bei diesen Ermittlungen um klassische Polizeiarbeit im Einzeldeliktbereich (Einvernahmen, Beschlagnahmungen usw.), in der die Kantone mehr Erfahrungen haben. Die Ermittlungsbehörden des Bundes wären deshalb vor allem auch bei grossen Operationen auf eine personelle und logistische Unterstützung der Kantone angewiesen, was zu einer übermässigen Beanspruchung der Kantone in einem Bereich führen würde, in dem sie keine Kompetenz mehr hätten. Schliesslich wurde bei der Analyse der Operation „Genesis“ festgestellt, dass sich die Hauptprobleme auf den ersten Verfahrensabschnitt konzentrierten, so dass eine Durchführung des gesamten Verfahrens durch den Bund nicht nötig ist. Die Umsetzung einer Bundeskompetenz würde zudem wegen der tief greifenden Änderungen im Strafverfolgungssystem länger dauern und eine Reorganisation der entsprechenden Bereiche des Bundes bedingen. Es wäre auch eine beträchtliche Aufstockung der personellen und finanziellen Ressourcen des Bundes in ähnlichem Umfang wie bei der Effizienzvorlage nötig, was angesichts der heutigen Finanzlage des Bundes nicht zu verkraften wäre.

3.22 Ermittlungskompetenzen der Bundesbehörden

Der Bundesrat teilt die Einschätzung der Arbeitsgruppe „Genesis“, dass im heutigen Strafverfolgungssystem im Bereich der Netzwerkkriminalität eine Lücke besteht, die durch die Schaffung einer Ermittlungsmöglichkeit der Bundesbehörden in der ersten Verfahrensphase geschlossen werden kann.

Der Bundesrat hat die beiden von der Arbeitsgruppe „Genesis“ vorgeschlagenen Varianten (vgl. oben Ziff. 3.15 und 3.16) eingehend geprüft:

Beide Varianten verfolgen das gleiche Ziel, nämlich dem Bund in den Fällen, in denen eine Vielzahl von Personen und vermutlich mehrere Kantone betroffen sind, Ermittlungs- und Weisungskompetenzen einzuräumen. Sie beschreiten aber dazu unterschiedliche Wege:

Variante 1 geht den Weg über ein *Oberaufsichtsrecht* des Bundes wie im Betäubungsmittelrecht (BetmG). Im BetmG bezieht sich jedoch die Oberaufsicht des Bundes auf den ganzen Erlass und nicht nur auf die strafrechtlichen Bestimmungen. Eine Oberaufsicht, die sich, wie von der Arbeitsgruppe „Genesis“ vorgeschlagen, ausschliesslich auf die Verfolgung bestimmter strafbarer Handlungen im StGB beschränkt, wäre ein Novum. Eine solche Oberaufsicht wäre wenig bestimmt. Der Bundesrat verkennt nicht, dass bei dieser Variante die Verfahrensabläufe den Strafverfolgungsbehörden aus dem BetmG zwar bekannt wären und sich diese dort auch bewährt haben, doch bestehen Unterschiede zur Netzwerkkriminalität, da in diesem Bereich eine Oberaufsicht bezüglich einer unbestimmten Anzahl von Strafbestimmungen des StGB und des Nebenstrafrechts begründet würde. Aus all diesen Gründen lehnt der Bundesrat diese Variante ab.

Variante 2 der Arbeitsgruppe „Genesis“ ermöglicht einen direkteren Weg um ans gleiche Ziel zu gelangen. Die neuen Kompetenzen des Bundes werden direkt und

abschliessend im StGB definiert. Der Wortlaut der Variante 2⁴⁷ entspricht allerdings nicht durchwegs den im StGB geforderten Kriterien der sprachlichen und inhaltlichen Klarheit und Bestimmtheit, was bei den rechtsanwendenden Behörden zu Unsicherheiten führen kann. Ferner werden durch den Passus „...oder in mehreren Kantonen...“ all jene Fälle ausgeschlossen, in denen es zwar mehrere Verdächtige gibt, aber nur ein Kanton betroffen ist. Ebenso fiele auch der Fall, in dem es nur eine verdächtige Person gibt, aber mehrere Kantone betroffen sind, nicht unter den vorgeschlagenen Normtext der Variante 2. Eine solche Regelung wäre deshalb wenig sinnvoll.

Ausgehend von dieser Variante 2 schlägt der Bundesrat einen neuen Artikel 344 VE-StGB vor (vgl. unten Ziff. 3.3). Gemäss diesem neuen Artikel können BA und BKP in Fällen, in denen eine der kantonalen Gerichtsbarkeit unterstehende strafbare Handlung mittels elektronischer Kommunikationsnetze begangen wurde und der zuständige Kanton noch nicht bekannt ist, erste, dringend notwendige Ermittlungen durchführen. Durch diese Ermittlungskompetenzen der BA und der BKP in der ersten Phase des Verfahrens wird keine Bundesgerichtsbarkeit begründet (vgl. unten Ziff. 3.4). Zudem kann die BKP durch Weisungen die Durchführung der Ermittlungen koordinieren.

Auch wenn dieser Vorschlag die Ermittlungskompetenzen des Bundes nur sehr massvoll ausweitet, braucht es personelle und finanzielle Mittel für die Umsetzung. Eine erste Schätzung kommt zum Schluss, dass ca. 13 zusätzliche Bundesstellen nötig wären. Bei dieser Schätzung gilt es zu berücksichtigen, dass sie auf bisherigen Erfahrungswerten aus der Koordination von Verfahren im Bereich Kinderpornografie beruht. Die einzusetzenden Ressourcen der Ermittlungsbehörden werden sich jedoch in einem gewissen Mass auch am wachsenden Deliktspotenzial in diesem Gesellschaftsumfeld orientieren müssen.

Der Bundesrat ist sich bewusst, dass die vorgeschlagenen Kompetenzen des Bundes im Bereich der kantonalen Gerichtsbarkeit liegen und dass diese deshalb gesetzgeberisch eigentlich in der vereinheitlichten schweizerischen Strafprozessordnung zu regeln wären. Da es aber bis zu deren voraussichtlichen Inkrafttreten noch mehrere Jahre dauern wird, im Bereich der Netzwerkkriminalität jedoch Handlungsbedarf besteht, wird eine Ergänzung des StGB als schneller umsetzbarer Weg gewählt.

Aus der Sicht des Bundesrates ist der vorgeschlagene Artikel 344 VE-StGB eine notwendige und sachgerechte Regelung, welche die Zusammenarbeit zwischen Bund und Kantonen verbessert und die Verfolgung der Netzwerkkriminalität dadurch effizienter gestaltet.

3.23 Flankierende Massnahmen

Aus den bereits genannten Gründen (vgl. oben Ziff. 2.223) hält der Bundesrat die auch von der Arbeitsgruppe „Genesis“ (vgl. oben Ziff. 3.17) empfohlene Ergänzung des BÜPF⁴⁸ für nicht erforderlich.

⁴⁷ Bericht der Arbeitsgruppe „Genesis“, op. cit., S. 21

⁴⁸ SR 780.1

3.3 Erläuterungen des Artikels 344 VE-StGB (Kompetenzen des Bundes bei strafbaren Handlungen mittels elektronischer Kommunikationsnetze)

Der vorgeschlagene Artikel 344 VE-StGB trägt den Besonderheiten der Strafverfolgung bei Fällen von Netzwerkkriminalität Rechnung, die zwar der kantonalen Gerichtsbarkeit unterstehen, in denen die Bundesbehörden (BA und/oder BKP) auf Grund der vorhandenen Informationen aber noch nicht wissen, welche Strafverfolgungsbehörden in welchen Kantonen zuständig sind. Es kann dabei u.a. auch um Fälle gehen, in denen die Bundesbehörden aus dem Ausland, Informationen erhalten, wonach für eine Vielzahl von Personen in mehreren Kantonen ein Verdacht besteht, dass sie eine strafbare Handlung begangen haben. Denkbar ist aber auch, dass die Information aus dem Inland stammt und für die Tatverdächtigen die Strafverfolgungsbehörde eines einzigen Kantons zuständig ist, die aber in dieser Phase des Verfahrens noch nicht bekannt ist. Es macht keinen Sinn - und das hat die Analyse der Operation „Genesis“ klar aufgezeigt - in solchen Fällen diese Informationen unverarbeitet an alle Kantone weiterzuleiten, damit jeder einzelne Kanton für sich die gleichen Ermittlungen durchführt, unter anderem um abzuklären, ob er für die Strafverfolgung zuständig ist. In dieser Phase der Vorabklärungen liegt das eigentliche Problem.

3.31 Systematische Einordnung und Randtitel des neuen Artikels 344 VE-StGB

Die systematische Einordnung als neuer Artikel 344 VE-StGB mit der Randziffer 3., nach dem geltenden Artikel 343 StGB mit dem Randtitel „2. Kantonale Gerichtsbarkeit“, soll signalisieren, dass mit dieser Norm keine neue Bundesgerichtsbarkeit geschaffen wird. Um jegliche diesbezügliche Unklarheiten auszuschliessen, wird dies in Absatz 1 mit dem Passus „... eine der kantonalen Gerichtsbarkeit unterstehende strafbare Handlung ...“ nochmals ausdrücklich präzisiert. Der Begriff „Kompetenzen“ im Randtitel deutet darauf hin, dass es nicht nur um Ermittlungs-, sondern, wie im Absatz 2 von Artikel 344 VE-StGB ausdrücklich festgehalten, auch um Weisungs- und Koordinationskompetenzen geht.

3.32 Absatz 1

Der neue Artikel 344 VE-StGB soll namentlich bei Fällen zur Anwendung kommen, deren Komplexität zum einen darin besteht, dass die Meldung aus dem In- oder Ausland strafbare Taten betrifft, die von einer Vielzahl von Personen in mehreren Kantonen begangen worden sind, zum anderen darin, dass in der virtuellen Welt der elektronischen Kommunikationsnetze andere und wegen des technischen Fortschritts sich ständig verändernde Ermittlungsmethoden angewendet werden müssen als in der realen Welt. Der vorgeschlagene Normtext ist aber so allgemein gefasst, dass die Strafbehörden des Bundes in jedem der kantonalen Gerichtsbarkeit unterstehenden Fall, in dem eine strafbare Handlung mittels elektronischem Kommunikationsnetz begangen wurde, die Ermittlungen aufnehmen kann, wenn der zur Strafverfolgung zuständige Kanton noch nicht feststeht. Um die ersten notwendigen Ermittlungen durchführen zu können, brauchen BA und BKP eine gesetzliche Kompetenz, die ihnen nach geltendem Recht fehlt. Die Ermittlungen von BA und BKP erfol-

gen nach Massgabe der Artikel 100 ff. BStP. Der BA obliegt die Leitung über die gerichtliche Polizei (Art. 15/17 BStP). Die BKP besorgt die in der neuen Norm verankerte Hauptarbeit – sprich den Kontakt zu den Kantonen sowie die Auswertung und Aufbereitung der eingegangenen Informationen. In dieser ersten Phase, in der sich das Verfahren beim Bund befindet, bildet auch die kantonale Polizei einen Teil der gerichtlichen Polizei des Bundes, soweit sie bei den ersten Ermittlungen mithilft (Art. 17 BStP). Nach Vornahme der ersten dringend notwendigen Ermittlungen leitet ihr die BA gestützt auf Artikel 107 BStP den Fall weiter.

Mit „erste dringend notwendige Ermittlungen“ sind sowohl Ermittlungen zur Feststellung der zuständigen kantonalen Strafverfolgungsbehörde als auch alle Sofortmassnahmen zur Beweissicherung gemeint. Gestützt auf die bisherigen Erfahrungen geht es dabei insbesondere um Ermittlungen technischer Natur zur Identifizierung von Kreditkarteninhabern bei den Banken und Kreditkarteninstituten und zur Identifizierung der verdächtigen Inhaber von E-Mail-Adressen bei den Schweizer Providern. Wegen des sich ständig und rasch entwickelnden technischen Umfeldes können aber die aufgezählten Massnahmen nicht als abschliessend betrachtet werden.

3.33 Absatz 2

In Absatz 2 wird der BKP für die Verfahren im Sinne von Absatz 1 ein direktes Weisungsrecht an die Adresse der kantonalen Strafverfolgungsbehörden eingeräumt. Damit soll u.a. sichergestellt werden, dass die Ermittlungen gleichzeitig angehoben werden und die Öffentlichkeit gleichzeitig informiert wird, um zu vermeiden, dass - wie in der Operation „Genesis“ geschehen – einige der Zielpersonen gewarnt werden und wertvolles Beweismaterial beseitigen können.

Es geht im Absatz 2 um Weisungen im Einzelfall und nicht um die sonst als Aufsichtsmittel gebräuchlichen generellen Weisungen. Adressaten sind auch nicht die kantonalen Regierungen, sondern die kantonalen Strafverfolgungsbehörden. Solche Weisungen der Bundesbehörden an bestimmte kantonale Behörden sind im Gegensatz zu den generellen Weisungen zur Durchsetzung des Bundesrechts etwa in Form von Kreisschreiben an die Adresse der Kantone, unüblich, da sie einen Eingriff in die innerkantonale Zuständigkeitsordnung darstellen. Sofern sich aber eine solche Weisungsbefugnis aus sachlichen Gründen als notwendig erweist, ist sie wenn immer möglich auf Gesetzesstufe vorzusehen. Absatz 2 legt deshalb eine solche Befugnis fest.

Mit Blick auf den begrifflichen Charakter der Weisung und der Tatsache, dass es an der Durchsetzungsmöglichkeit fehlt, ist das Adjektiv „verbindlich“, wie in der Variante 2 der Arbeitsgruppe "Genesis" vorgesehen⁴⁹, nicht nötig. Eine Weisung ist immer verbindlich, sonst würde sie zur Empfehlung.

⁴⁹ Bericht der Arbeitsgruppe "Genesis", op. cit., S. 21.

3.4 Militärstrafgesetz

Eine analoge Regelung des Vorentwurfes B ist im MStG nicht nötig, da militärspezifische Fälle in diesem Bereich nur schwer vorstellbar sind. Zudem sieht das MStG vor, solche Fälle an die zuständigen zivilen Behörden abzutreten (vgl. Art. 221 MStG).

3.5 Vorentwurf B Schweizerisches Strafgesetzbuch

Artikel 344 VE-StGB

3. Kompetenzen des Bundes bei strafbaren Handlungen mittels elektronischer Kommunikationsnetze

¹ Besteht der Verdacht, dass eine der kantonalen Gerichtsbarkeit unterstehende strafbare Handlung mittels elektronischer Kommunikationsnetze begangen wurde, und steht der zur Strafverfolgung zuständige Kanton noch nicht fest, so können Bundesanwaltschaft und Bundeskriminalpolizei erste, dringend notwendige Ermittlungen durchführen. Sie wenden dabei das Bundesgesetz vom 15. Juni 1934 über die Bundesstrafrechtspflege an.

² Die Bundeskriminalpolizei kann durch Weisungen an die kantonalen Strafverfolgungsbehörden die Durchführung der Ermittlungen koordinieren.