

Eidg. Justiz- und Polizeidepartement  
Herr Bundesrat Christoph Blocher  
Bundeshaus West  
3003 Bern

29. April 2005

**Bericht und Vorentwürfe über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes betreffend die strafrechtliche Verantwortlichkeit der Provider und die Kompetenzen des Bundes bei der Verfolgung strafbarer Handlungen mittels elektronischer Kommunikationsnetze (Netzwerkriminalität)**

Sehr geehrter Herr Bundesrat  
Sehr geehrte Damen und Herren

Mit Schreiben vom 10. Dezember 2004 haben Sie uns eingeladen, zum Bericht und den Vorentwürfen über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes betreffend die strafrechtliche Verantwortlichkeit der Provider und die Kompetenzen des Bundes bei der Verfolgung strafbarer Handlungen mittels elektronischer Kommunikationsnetze Stellung zu nehmen. Für die gebotene Gelegenheit zur Meinungsäusserung danken wir Ihnen bestens.

**Zusammenfassung**

Die Wirtschaft unterstützt den wirkungsvollen Kampf gegen die Netzwerkriminalität. Unternehmen können dabei als Opfer, als Täter oder als Drittpersonen betroffen sein. Vermögens- und Wirtschaftsdelikte sind dabei im Gegensatz zur verbreiteten Auffassung bedeutender als Pornographie und Rassismus.

economiesuisse lehnt aber die Delegation von Aufgaben der Strafverfolgung an die Unternehmen ab. Eine effiziente Strafverfolgung darf die Entwicklung der neuen Informationstechnologien nicht verhindern. Die im Entwurf vorgeschlagene Erfassung der „Hosting Provider“ und der Suchmaschinenanbieter ist überschüssig und wird entschieden zurückgewiesen. Die Vorlage ist in diesem Sinne zu überarbeiten.

## Allgemeine Bemerkungen

Die Wirtschaft ist an einer effizienten Strafverfolgung interessiert. Unternehmen können dabei sowohl Opfer, Täter wie Dritte sein. Die heutige Rechtsunsicherheit wird durch die unterschiedlichen Gutachten offensichtlich und wirkt sich in jeder Beziehung störend aus, indem die subsidiäre Anwendung der generellen Strafnormen der besonderen Situation bei den elektronischen Kommunikationsnetzen nicht Rechnung trägt. Eine explizite rechtliche Regelung erscheint daher dringlich. Allerdings sind neben strafrechtlichen auch zivilrechtliche Aspekte einzubeziehen. Soll die notwendige Rechtssicherheit geschaffen werden, sind aber klare Abgrenzungen notwendig. Dies gilt betreffend der allenfalls mit Pflichten Belastenden (etwa Bereitstellung von elektronischen Marktplätzen) oder die erfassten Netze (offene und geschlossene Netze; Berücksichtigung der Konvergenz).

Jede Regelung im Bereiche der Informationsgesellschaft muss darauf ausgerichtet sein, dass die Schweiz eine Spitzenstellung einnehmen kann. Nur so kann wirtschaftliches Wachstum erzielt werden. Im konkreten Zusammenhang bedeutet dies, dass einerseits die Netzwerkkriminalität wirksam zu bekämpfen ist, die Entwicklung der Informationsgesellschaft und die Bereitstellung entsprechender Angebote aber nicht gelähmt werden darf. Grundsätzlich sind die verschiedenen Beteiligten mit Ausnahme der „Content Provider“ als Vermittler von Infrastruktur anzusehen, wie etwa Transportunternehmen. Der Grundsatz der freien Kommunikation und die Entwicklung der Informationsgesellschaft müssen im Zweifelsfalle Priorität haben.

Wie im Bericht treffend ausgeführt, erschliessen die neuen Informationstechnologien nicht nur Chancen für eine universelle Informationsbearbeitung für Private, Unternehmen und Behörden sondern ermöglichen auch die Begehung von Straftaten mit diesen Mitteln von jedem beliebigen Ort der Welt aus. Dabei werden in den Medien, aber auch im Bericht der Expertengruppe Netzwerkkriminalität, die Tatbestände der Kinderpornographie, der Gewaltdarstellung und des Rassismus in den Vordergrund gestellt. Gemäss einer FBI-Statistik im Jahre 2004 waren aber über 95% aller durch das Internet verübten Delikte vermögens- und wirtschaftsrechtlicher Natur. Wichtige Tatbestände sind dabei Betrug im Allgemeinen, „Phishing“ im Besonderen, Marken- und Copyrightverletzung, Unlauterer Wettbewerb, Datendiebstahl und Rufschädigung. Sowohl Gesetzgebung wie auch Strafverfolgung müssen sich vermehrt an diesen häufigen Tatbeständen ausrichten.

Der Vorentwurf delegiert einen Teil der staatlichen Aufgaben bei der Ermittlung und Verfolgung von Straftaten an private Unternehmen, indem besondere Überwachungs- und Anzeigepflichten eingeführt werden, mit Strafsanktionen bei Nichterfüllung. Dieses Vorgehen kollidiert aber eklatant mit den Anforderungen des Datenschutzes und Geheimnispflichten, setzt die Verpflichteten privatrechtlichen Haftungsklagen aus (nämlich im Falle einer unberechtigten Meldung) und ist praktisch nur schwer umsetzbar, indem die Illegalität der zu meldenden Inhalte seitens der Ver-

pflichteten nicht rechtssicher festgestellt oder technisch durchgesetzt werden können. Inhaltskontrollen können und dürfen nicht die Aufgabe von Vermittlern von Infrastruktur sein und die Möglichkeiten der technischen Entwicklung dürfen nicht behindert werden. Ein besonderes Augenmerk ist dabei dem internationalen Verhältnis zu widmen.

Sachlich erscheint die strafrechtliche Regelung im Rahmen des 6. Randtitels des StGB als angemessen, ebenfalls die grundsätzliche Erfassung nach den allgemeinen Bestimmungen des StGB über Täterschaft und Teilnahme mit speziellen Bestimmungen für einzelne Provider oder Anbieter.

### **Bemerkungen zu den einzelnen Artikeln**

Die nachfolgenden Bemerkungen gelten für die vorgeschlagenen Änderungen im MStGB sinngemäss.

#### Art. 27 VE-StGB Strafbarkeit in elektronischen Kommunikationsnetzen

Der Begriff des elektronischen Kommunikationsnetzes geht weit über das gemäss Begleitberichten vorwiegend anvisierte Internet hinaus und umfasst etwa auch geschlossene Informatiknetze oder Telekommunikationsnetze. Vermehrt bieten etwa Fernmeldedienstanbieter auf der eigenen Netzwerk-Infrastruktur geschlossene Netze für Dritte an. Eine Inhaltskontrolle in diesen Netzen würde etwa im Bank- oder Gesundheitsbereich mit den entsprechenden Geheimnisverpflichtungen kollidieren. Auch die Individualkommunikation mit beispielsweise E-Mail, Telefonie oder „voice over IP“ wäre wohl erfasst. Dies würde nicht nur eine technisch unzumutbar aufwendige Überwachung mit entsprechenden Risiken bedingen sondern auch mit dem Fernmeldegeheimnis kollidieren.

Die Definition des elektronischen Kommunikationsnetzes ist auf **öffentlich zugängliche oder zum öffentlichen Zugang bestimmte** Netze zu beschränken.

#### *Abs. 1 (Content-Provider)*

Die strafrechtliche Erfassung des Content Provider erscheint als angemessen.

#### *Abs. 2 (Medienstrafrecht)*

Der Vorbehalt des Medienstrafrechts erscheint als sachgerecht. Leider sind aber die Auswirkungen auf die heutige Situation multimedialer Anbieter nicht klar dargelegt, da sich der Vorentwurf auf die Provider ausrichtet. Hier sind für die definitive Vorlage weitere Abklärungen notwendig.

### *Abs. 3 (Hosting-Provider und Suchmaschinen)*

Die strafrechtliche Erfassung von Hosting-Providern lehnen wir ab. Wir verweisen auf die entsprechenden Ausführungen zu Art. 322<sup>bis</sup> VE-StGB.

Völlig verfehlt ist es, Suchmaschinen-Anbieter den Hosting-Providern gleichzustellen. Diese nehmen nicht Inhalte auf, sondern Verweise auf dieselben. Analoges gilt für die Anbieter von elektronischen Marktplätzen. Solchen Anbietern kommt in der Informationsgesellschaft eine Schlüsselrolle zu, indem sie mit ihrer Infrastruktur die Erschliessung von Informationen erleichtern, ohne aber auf den Inhalt dieser Informationen Einfluss zu nehmen. Diese Anbieter arbeiten im Rahmen des Rechtsvollzugs mit den Behörden zusammen, sie mit Strafsanktionen zu bedrohen ist aber verfehlt. Der vorgeschlagene Absatz würde vielmehr dazu führen, dass der Standort Schweiz gerade für Suchmaschinen und für elektronische Marktplätze Nachteile schaffen würde. Die vorgeschlagene Formulierung des „automatisierten“ Bereithaltens könnte sich je nach Interpretation gar kontraproduktiv auswirken (siehe dazu unten).

Der heutige Absatz 3 ist zu streichen und das (automatisierte) Bereithalten von fremden Informationen zur Nutzung in elektronischen Kommunikationsnetzen in Absatz 4 – im Sinne der Straffreiheit – zu erfassen.

Für die detaillierten Begründungen verweisen wir auch auf die Ihnen direkt zugegangenen Stellungnahmen von simsa, eBay und Swisscom, deren entsprechende Schlussfolgerungen wir ausdrücklich unterstützen.

### *Abs. 4 (Access-Provider)*

Die rechtliche Klarstellung, wonach die Verschaffung des reinen Zugangs zu einem elektronischen Kommunikationsnetz nicht zur Strafbarkeit führt (Abweichung von den allgemeinen Regeln zur Täterschaft und Teilnahme), ist richtig. Entgegen dem Begleitbericht muss aber auch ein automatisiertes „Mirroring“ zur Steigerung der Leistungsfähigkeit des Netzwerkes straflos sein. Hingegen sollte Abgrenzung zur Gehilfenschaft exakter gezogen werden, um Anwendungsprobleme zu vermeiden.

Abs. 4 ist zur Klarstellung der Abgrenzung zur Gehilfenschaft etwa wie folgt zu ergänzen:  
Strafbarkeit nach den allgemeinen Regeln der Teilnahme bleibt vorbehalten, sofern der Zugangsvermittler die Übermittlung der Informationen veranlasst, sofern er die Adressaten der übermittelten Informationen auswählt oder sofern er die übermittelten Informationen auswählt oder verändert.

Art. 322<sup>bis</sup> VE-StGB Strafbarkeit in elektronischen Kommunikationsnetzen

Die Übertragung eines Ermittlungs- und Verfolgungsmonopols des Staates an die Hosting-Provider (und auch die Anbieter von Suchmaschinen o.ä.) lehnen wir grundsätzlich ab. Trotz der einschränkenden Bemerkungen im Begleitbericht wird in der Praxis ein Anbieter eigene – praktisch aber nur schwer umzusetzende – Abklärungen vornehmen müssen, will er sein strafrechtliches Haftungsrisiko vermeiden. Wir halten nochmals fest, dass keineswegs nur Gewaltdarstellungen, Pornografie oder Rassen-diskriminierungen klassischerweise zur Netzwerkkriminalität gehören. Vielmehr sind die übrigen – im Bericht gleichsam am Rande erwähnten Bereiche – gerade für die Wirtschaft von grosser Bedeutung.

Der Begriff des „automatisierten“ Bereithaltens würde je nach Auslegung Provider härter erfassen, wenn sie über Filtertechniken oder mit Nachforschungen über die gesetzlichen Pflichten hinaus gegen illegale Inhalte vorgehen. Hier muss eine präzisere Fassung gefunden werden, damit nicht ein kontraproduktiver Effekt erzielt wird.

Entscheidend ist auch die Definition der „fremden“ Information gerade im Konzernverbund. Würde nämlich dieser Begriff zivilrechtlich eng ausgelegt, wären bereits die Informationen von verbundenen Unternehmen als „fremd“ zu betrachten.

Es ist klarzustellen – ob im Gesetz oder mindestens unmissverständlich in den Materialien – dass Informationen von verbundenen Unternehmen auf Netzwerkinstallationen innerhalb des Verbundes nicht als „fremd“ gelten.

*Ziff. 1 Abs. 1 (Einschreiten des Hosting-Providers)*

Der Begriff des „sicheren Wissens“ ist unklar und nach strafrechtlichen Kriterien zu wenig bestimmt. Das Einschreiten des Hosting-Providers muss sich nach objektiven Kriterien messen und jegliche Pflicht zu eigenem Nachforschen muss ausgeschlossen sein. Zu beachten ist, dass ein Hosting-Provider bei einem sich nachträglich als ungerechtfertigt herausstellenden Blockieren von Informationen gegenüber seinen Kunden schadenersatzpflichtig werden kann. Die Beurteilung, ob Informationen zu strafbaren Handlungen verwendet werden, setzt in jedem Falle eine – allenfalls nur summarische – juristische Beurteilung voraus. Viele Hosting-Provider verfügen aber gar nicht über entsprechend qualifizierte Mitarbeiter.

Die Pflicht zum Einschreiten ist auf Fälle zu beschränken, in denen eine zuständige Behörde dem Hosting-Provider mitgeteilt hat, dass derartige Informationen zur Begehung eines von Amtes wegen zu verfolgenden Vergehens oder Verbrechens genutzt werden.

*Ziff. 1 Abs. 2 (Pflicht zur Weiterleitung)*

Die Pflicht zur Weiterleitung irgendwelcher Informationen an die Strafbehörden ist einzigartig. Die Weiterleitung einer solchen Meldung wäre gar dann notwendig, wenn die Haupttat gar keinen Bezug zur Schweiz aufweist. Eine eigene Beurteilung durch den Hosting-Provider würde aber wiederum eigene Abklärungen und Beurteilungen voraussetzen. Faktisch würde dies dazu führen, dass alle Informationen an die Strafverfolgungsbehörden übermittelt würden. Richtig ist es, Dritte anzuhalten, selbst direkt die Strafverfolgungsbehörden einzuschalten. Die möglicherweise so entstehende Schwelle wäre im Sinne einer Verhinderung von leichtfertigen Anzeigen zu begrüssen.

Ziff. 1 Abs. 2 ist ersatzlos zu streichen.
--

*Ziff. 1 Abs. 4 (Anwendbares Recht)*

Die Beurteilung der Strafbarkeit nach Schweizer Recht kann zu grossen Problemen Anlass geben, namentlich wenn etwa unterschiedliche Rechte des Geistigen Eigentums in Frage stehen. Der vorgeschlagene Artikel würde zu einer unerwünschten extraterritorialen Anwendung des Schweizer Rechts führen. Damit wäre der Schweizer Standort für internationale Anbieter in diesem Bereich gefährdet. Leider fehlen dazu die notwendigen Abklärungen, welche nachzuholen sind. Die Anwendbarkeit ist auf Informationen zu beschränken, welche auf die Schweiz ausgerichtet sind.

Abs. 4 ist wie folgt zu ergänzen:
-----------------------------------

Die Strafbarkeit setzt voraus, dass die Information speziell auf die Schweiz ausgerichtet ist.
--

*Art. 344 VE-StGB (Kompetenzen des Bundes)*

Die Schaffung einer Kompetenz des Bundes im vorgeschlagenen Sinne heissen wir gut.

**Weitere Bemerkungen**

Die Frage der Links muss – mindestens in der Botschaft – in dem Sinne klargestellt werden, dass ein Verweis auf eine nicht offensichtlich illegale Seite zulässig ist, selbst wenn auf Unterseiten oder mit weiteren Links im Verlaufe des Abrufens auf illegale Inhalte gelangt werden kann.

Besonders wichtig erscheint uns, die internationale Zusammenarbeit zu verbessern. Tatsächlich werden die inkriminierten Handlungen oft über Installationen im Ausland vorgenommen. Mit der fortschreitenden Technologie wird diese Problematik noch zunehmen.

Zusammenfassend unterstützen wir die Bestrebungen zur Schaffung von Rechtssicherheit in diesem heiklen Gebiet. Wir erachten aber den vorgeschlagenen Entwurf noch als ungenügend. Auch das Bestreben einer effizienten Strafverfolgung rechtfertigt die Schaffung derart weitgehender Verpflichtungen für Hosting-Provider und gleich behandelte Anbieter nicht. Die Auswirkungen auf den Standort Schweiz als Ort einer zukunftsgerichteten Informationsgesellschaft müssen bei einer Regelung genau beachtet und im Zweifelsfall höher bewertet werden als Erleichterungen für die Ermittlungsbehörden.

Sie finden in der Beilage die Stellungnahmen der Aargauischen Industrie- und Handelskammer, der Chambre vaudoise du commerce et de l'industrie, der Zürcher Handelskammer und der UBS im vollen Wortlaut. Weitere Stellungnahmen besonders betroffener Mitglieder wurden Ihnen direkt zugestellt.

Für die Berücksichtigung unserer Anliegen bei der notwendigen substantiellen Überarbeitung der Vorlage danken wir Ihnen. Gerne steht Ihnen der Rechtsunterzeichnende für weitere Informationen zur Verfügung.

Mit freundlichen Grüßen  
economiesuisse

Dr. Rudolf Ramsauer  
Vorsitzender der Geschäftsleitung

Thomas Pletscher  
Mitglied der Geschäftsleitung