Vernehmlassungsantwort zur Änderung des Bundesgesetzes über die Wahrung der inneren Sicherheit (BWIS)

Swiss Internet User Group (SIUG)

29. Mai 2003

Die SIUG ist eine Non-Profit-Organisation, die sich aus Internetexperten verschiedener Stufen zusammensetzt. Dazu gehören Akademiker aus verschiedenen Fachgebieten, Experten aus dem ISP-Bereich, selbständige Informatiker und Anwender. Das Ziel der SIUG ist es, sich für eine vernünftige Anwendung, Entwicklung und Reglementierung des Internets und verwandter Technologien einzusetzen, ohne dabei den ursprünglichen offenen Geist und die Tradition des Mediums übermässig einzuschränken.

Swiss Internet User Group (SIUG)
Postfach 1908
8021 Zürich
Mail siug@siug.ch
Web http://www.siug.ch/

Kontakt:

Matthias Leisi
Zürichweg 5, 8153 Rümlang
Telefon 043 211 03 55, Fax 043 211 03 56
Mail matthias.leisi@siug.ch

1 Allgemeiner Teil

Die Swiss Internet User Group (SIUG) als Expertengruppe im Bereich Internet und Kommunikation bezieht sich in dieser Vernehmlassungsantwort nur auf Massnahmen, welche die Kommunikationstechnologien und damit zusammenhängende Fragen betreffen.

2 Besonderer Teil

2.1 Bundesgesetz über die Wahrung der inneren Sicherheit (BWIS) Art. 13bis, Abs. 5

Dieser Absatz sieht vor, dass das Bundesamt Internet Providern die Sperrung von ausländischen Internetsites empfehlen kann.

Der im Entwurf des Gesetzes verwendete Begriff "Internet-Provider" ist ungenau. Dem Bericht entnehmen wir, dass damit "Access-Provider" gemeint sind, also Telekommunikationsanbieter, die Zugang zum Internet vermitteln.

Die Zugangsvermittler bieten lediglich Zugang zum Internet an und können in keiner Art und Weise für die durch sie transportieren Inhalte verantwortlich gemacht werden. Analog müsste das Bundesamt den Betreibern von öffentlichen Telefonen Sperrungen von ausländischen Anschlüssen empfehlen.

Es kann jedoch nicht Sache des Bundesamts sein, den Schweizer Internetprovidern zu empfehlen, was deren Kundschaft sehen darf und was nicht. Dies ist die alleinige Sache der Internet-Nutzenden. Rechtliche Klarheit in diesem Bereich versucht die Motion Pfisterer[1] zu schaffen.

Das alleinige Beschaffen von Information von öffentlich zugänglichen Quellen ist durch Art. 16 Abs. c der Bundesverfassung explizit geschützt und kann somit auf Gesetzesebene nicht verboten werden. Das Bundesamt hat deshalb keine Empfehlung auszusprechen für eine Freiheit, die durch die Verfassung gewährleistet ist. Das Aussprechen einer Empfehlung zur Webseiten-Sperrung ist im weiteren auch bedenklich was die Art. 6 (Eigenverantwortung) und Art. 13 (Schutz der Privatsphäre) angeht. Das Abrufen einer Webseite ist ein rein privater Vorgang (allenfalls im Gegensatz zum Anbieten einer Webseite) und darf durch die Provider nicht gestört werden. Entsprechend hat das Bundesamt die Provider nicht zur Störung des durch die Verfassung garantierten persönlichen Fernmeldeverkehrs zu verleiten.

Eine offizielle Empfehlung des Bundesamtes an Provider, gewisse ausländische Internetseiten zu sperren, führt höchstens zu einer Verunsicherung unter den Providern, da die Empfehlung den Eindruck eines amtlichem Charakter erweckt. Es ist zudem zu befürchten, dass die Provider in einem vorauseilenden Gehorsam die Seiten sperren werden, bevor ein Gericht darüber entschieden hat, ob der darauf verbreitete Inhalt in der Schweiz überhaupt illegal wäre.

Wir anerkennen das Problem des Rassismus als ernstes gesellschaftliches Problem. Die SIUG ist aber der Ansicht, dass durch technische Massnahmen nicht gesellschaftliche Probleme gelöst werden können. Gerade in Kreisen, die dem rassistischen Gedankengut zugeneigt sind, werden bei Sperrungen in Kürze Anleitungen zu deren Umgehung kursieren.

[1] 00.3714: Netzwerkkriminalit. Änderung der rechtlichen Bestimmungen, AB 2001 S 27 und AB 2001 N 1087

Sperrungen von Webseiten und anderen Angeboten im Internet sind zudem leicht zu überwinden und somit kaum zweckmässig.

Die SIUG verlangt die ersatzlose Streichung von Absatz 5.

2.2 Bundesgesetz über die Wahrung der inneren Sicherheit (BWIS) Art. 16bis (neu)

Der Artikel regelt in keiner Art und Weise, wie Daten aus der Datenbank wieder *gelöscht* werden.

Da die Aufgabe der "Hooligan-Datenbank" das Verhindern aktueller Gewalttaten ist, muss sicher gestellt werden, dass Einträge periodisch darauf überprüft werden, ob die Daten weiterhin richtig und erheblich sind. Eine solche Regelung steht auch im Einklang mit Art. 21 DSG (SR 235.1).

Es muss verhindert werden, dass diese Datenbank quasi zu einem unkontrollierten parallelen Strafregister ohne Verfahrensgarantien wird.

2.3 Bundesgesetz betreffend die Ueberwachung des Post- und Fernmeldeverkehrs (BÜPF) Art. 3, Abs. 2, Bst. a

Die SIUG hat Bedenken, was die Ausweitung des BÜPF-Deliktkatalogs auf die Artikel StGB 261bis, 261ter und 261quat betrifft. Das BÜPF dient primär zur Überwachung der *privaten* Kommunikation während die StGB-Artikel gegen *öffentliche* Aktionen abzielen. Rassistische Äusserungen in privaten E-Mails sind zwar gesellschaftlich gesehen ein bedenkliches Zeichen. Es ist jedoch unverhältnismässig, den Deliktskatalog des BÜPF in der Form auszuweiten – es genügt zur Strafverfolgung, dass zum Beispiel der Empfänger eines solchen E-Mails dessen Inhalt den Strafverfolgungsbehörden zur Kenntnis bringt.

Die Behauptung im Bericht der Expertengruppe (p. 18), dass "Ermittlungen nur unter Aufhebung des Fernmeldegeheimnisses geführt werden" können, entbehrt jeglicher Grundlage.

Die Ausdehnung des Deliktkatalogs des BÜPF ist daher weder sachlich gerechtfertigt noch notwendig und ist abzulehnen.