Bundesrat **Drucksache 556/06 (Beschluss)**

22.09.06

Stellungnahme
des Bundesrates

Entwurf eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz - ElGVG)

Der Bundesrat hat in seiner 825. Sitzung am 22. September 2006 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Abs. 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. Zum Gesetzentwurf allgemein

   Der Bundesrat bittet die Bundesregierung zu prüfen, ob die bereits im UWG normierte "Opt-In"-Regelung, nach der es dem Versender nur bei vorliegender Zustimmung des Empfängers erlaubt ist, Werbung zu versenden, in das ElGVG integriert werden kann mit dem Ziel, dass Verstöße gegen die "Opt-In"-Regelung als Ordnungswidrigkeiten geahndet werden können.

   Begründung:

   Ein Unterlassungs- oder Beseitigungsanspruch gemäß § 8 Abs. 1 UWG ist für den Verbraucher in der Regel das einzige durchsetzbare Rechtsmittel. Diese Ansprüche haben auf den Versender von Spam-Mails jedoch keinen Abschreckungseffekt und stellen, den mit solcher Werbung einhergehenden Gewinn berücksichtigend, keine adäquate Sanktion dar.

   Ein im Einzelfall durch den geschädigten Verbraucher durchzusetzender zivilrechtlicher Anspruch kann den Anforderungen eines umfassenden Verbraucherschutzes vorliegend nicht genügen. Vielmehr bedarf es hier einer hoheitlich schützenden Regelung, welche bei Zuwiderhandlungen auch Sanktionen vorsieht.

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln
Telefon: (02 21) 97 66 83 40, Telefax: (02 21) 97 66 83 44
ISSN 0720-2946

2. Zum Gesetzentwurf allgemein

In der jetzigen Praxis gewähren die Anbieter von Online-Dienstleistungen den Verbrauchern häufig nur Zugang zu diesen Diensten, wenn eine Zustimmung zu einer weit reichenden Datenverwendung erteilt wird. Damit ist in der Regel auch die Zustimmung für den Erhalt unterschiedlichster Werbe-E-Mails verbunden. Der Bundesrat hält die Einführung eines Koppelungsverbotes für sinnvoll und bittet die Bundesregierung um Prüfung, ob ein solches Kopplungsverbot in das ElGVG aufgenommen werden kann.

Begründung:

Aus Verbrauchersicht ist ein uneingeschränktes Koppelungsverbot, dass bei Zuwiderhandlung eine Ordnungswidrigkeit vorsieht, erstrebenswert. Es ist nicht ersichtlich, warum ein Verbraucher dem Anbieter von Online-Diensten als Voraussetzung zur Nutzung dieser Dienste persönliche Informationen zu einer umfangreichen Verwendung zugestehen sollte. Diese Zustimmung erfolgt somit nur, um den angebotenen Dienst nutzen zu können und entspricht nicht der Willensfreiheit des Zustimmenden.

3. Zu Artikel 1 (§ 6 Abs. 2 Satz 2, Satz 3 - neu - TMG)

In Artikel 1 ist § 6 Abs. 2 ist wie folgt zu ändern:

a) Satz 2 ist wie folgt zu fassen:

"Es wird vermutet, dass ein Verschleiern oder Verheimlichen vorliegt, wenn die Kopf- und Betreffzeile so gestaltet sind, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält".

b) Folgender Satz 3 ist anzufügen:

"Dies gilt nicht, wenn der Versender die Verschleierung oder Verheimlichung nicht absichtlich vorgenommen hat."

Begründung:

Nach der bisherigen Fassung des § 6 Abs. 2 Satz 2 TMG-E obliegt es dem Empfänger von Spam-Mails zu beweisen, dass der Versender die Nachricht durch die Kopf- und Betreffzeile absichtlich in verschleiernder, oder verheimlichender Form gefasst hat. Dieser Beweis der absichtlichen Vorgehensweise

wird in der Regel nicht zu erbringen sein. So ist der Empfänger schon räumlich von dem Versender distanziert und hat auch keinen Einblick in dessen Betriebsbereich.

Es ist sachgerechter, dem Versender die Beweislast dafür aufzuerlegen, dass die Verschleierung, oder Verheimlichung der Kopf- oder Betreffzeile nicht absichtlich vorgenommen wurde. Schließlich stammt die Spam-Mail auch aus seinem Betrieb und seinem Machtbereich, so dass ein Einflussnahme und Protokollierung der Vorgänge möglich ist. Schließlich kann der Versender auf die Art und Weise der Gestaltung Einfluss nehmen.

4. Zu Artikel 1 (§ 14 Abs. 2 TMG)

In Artikel 1 sind in § 14 Abs. 2 die Wörter "darf der Diensteanbieter im Einzelfall Auskunft über Bestandsdaten erteilen" durch die Wörter "hat der Diensteanbieter im Einzelfall Auskunft über Bestandsdaten zu erteilen" zu ersetzen.

Begründung:

Die derzeitige Formulierung "darf" erweckt den unzutreffenden Eindruck, dass es im Ermessen des Diensteanbieters liegt, ob er einem Auskunftsersuchen der Sicherheitsbehörden Folge leisten will oder nicht. Ausweislich der Begründung ist dies nicht beabsichtigt:

"Die Vorschrift besagt, dass der Diensteanbieter aus der Aufgabenerfüllung im Bereich der Strafverfolgung sowie der genannten Behörden erwachsende Auskunftsansprüche nicht aus datenschutzrechtlichen Erwägungen zurückweisen können." (vgl. S. 22 zu Nr. 8e)).

Zutreffend wird weiter ausgeführt, dass es entsprechend den allgemeinen datenschutzrechtlichen Grundsätzen nicht Aufgabe des Diensteanbieters ist, die Voraussetzung der Befugnisnorm zu überprüfen, auf die die Sicherheitsbehörde ihr Auskunftsersuchen stützt (vgl. S. 23 zu Nr. 8e)). Dies entspricht auch den Regelungen bei vergleichbaren Eingriffen, z. B. der Telekommunikationsüberwachung nach den Vorschriften der Strafprozessordnung. Tatsächlich besteht daher eine Auskunftspflicht der Diensteanbieter gegenüber den Sicherheitsbehörden. Dies bringt das Wort "hat" deutlicher zum Ausdruck. Die Klarstellung liegt auch im Interesse der Diensteanbieter, da diese gegenüber ihren Kunden die Herausgabe von Daten an Sicherheitsbehörden rechtfertigen müssen. Auch aus der strafrechtlichen Ermittlungspraxis ist für vergleichbare Konstellationen, z. B. die Erteilung von Auskünften durch Banken, bekannt, dass den Unternehmen eine Kooperation mit den Sicherheitsbehörden leichter fällt, wenn sie gegenüber ihren Kunden auf eine eindeutige gesetzliche Verpflichtung verweisen können. Aus den genannten Gründen wurde in der Parallelvorschrift des § 113 Abs. 1 Satz 1 TKG ebenfalls die Auskunftspflicht durch die Formulierung "hat" klar zum Ausdruck gebracht.

5. Zu Artikel 1 (§ 14 Abs. 2 TMG)

In Artikel 1 sind in § 14 Abs. 2 nach den Wörtern "der Strafverfolgung," die Wörter "zur Gefahrenabwehr durch die Polizeibehörden der Länder," einzufügen.

Begründung:

Bestands- und Nutzungsdaten von Telemediendiensten werden auch zur Gefahrenabwehr, die auch die vorbeugende Bekämpfung von Straftaten umfasst, benötigt.

Im Bereich der Gefahrenabwehr wäre ein Bedarfsfall beispielsweise gegeben, wenn auf einer Internetplattform Anleitungen zum Bau von Sprengsätzen, Blankoformulare für Dienstausweise der Polizei oder Zugangsberechtigungen für einen bestimmten Flughafen angeboten werden. Hier kann für die Polizei von Bedeutung sein, zu erfahren, welche Person/Firma sich hinter dem Anbieter verbirgt und ob Informationen über weitere Internetangebote dieser Person/Firma vorliegen.

Die Befugnisse der Behörden der Vollzugspolizeien der Länder nach den jeweiligen Länderpolizeigesetzen gehen ins Leere, solange das datenschutzrechtliche Gegenstück zur Datenerhebung, nämlich die zweckändernde Übermittlungsbefugnis der Diensteanbieter an die Polizeibehörden, nicht bereichsspezifisch im Telemediengesetz, entsprechend den Regelungen für die Strafverfolgungsbehörden, die Verfassungsschutzbehörden des Bundes und der Länder, den Bundesnachrichtendienstes und den Militärischen Abschirmdienstes, geregelt ist. Aus kompetenzrechtlichen Gründen kann eine Durchbrechung der im Telemediengesetz bundesrechtlich festgelegten Verwendungsbeschränkungen auch nicht in den Länderpolizeigesetzen geregelt werden.

In § 14 Abs. 2 TMG-E muss die Öffnungsklausel daher auch die zweckändernde Nutzung der nach dem Telemediengesetz erhobenen Bestands- und Nutzungsdaten zu Zwecken der Gefahrenabwehr vorsehen.

Entsprechend der in § 14 Abs. 2 TMG-E angelegten Systematik, dass sich die Erhebungsbefugnisse nach den jeweiligen Fachgesetzen richten, ergeben sich die Voraussetzungen, unter denen die Polizei Bestands- und Nutzungsdaten bei Diensteanbietern, die eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln, aus den Länderpolizeigesetzen.

Die Erhebung von Bestands- und Nutzungsdaten, die - nicht - wie bei der Telekommunikationsüberwachung - im Rahmen des eigentlichen Übertragungsvorgangs stattfindet, ist ein Eingriff in das Recht auf informationelle Selbstbestimmung (Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG). Ein Eingriff in Artikel 10 GG liegt hingegen auch bei der Erhebung von Nutzungsdaten nicht vor. Das Fernmeldegeheimnis nach Artikel 10 GG schützt den durch Netzbetreiber vermittelten Fernmeldeverkehr und umfasst sowohl den Inhalt

als auch die Umstände desselben. Das Fernmeldegeheimnis bezieht sich nur auf den eigentlichen Übertragungsvorgang. Der Schutzbereich wird durch den Herrschaftsbereich des Betreibers des Fernmeldenetzes umgrenzt. Der Grundrechtschutz des Artikels 10 GG endet daher am Endgerät des Telekommunikationsteilnehmers und gilt nicht im Verhältnis der Kommunikationspartner untereinander. Der Nutzer eines Telemediendienstes und der Diensteanbieter stehen zueinander im Verhältnis von Kommunikationspartner. Soweit die Nutzungsdaten daher nach Abschluss der dem Telemediendienst zu Grunde liegenden Telekommunikation beim Diensteanbieter gespeichert werden, sind sie nicht vom Schutzbereich des Artikels 10 GG umfasst. Soweit die Länderpolizeigesetze die Erhebung von Bestands- und Nutzungsdaten von Telemediendiensten nicht bereichsspezifisch in den Länderpolizeigesetzen geregelt haben, kann die Datenerhebung nur auf die allgemeinen Befugnisnormen zur Datenerhebung gestützt werden.