

Zusammenfassung Telekommunikationsgesetz

Das neue überarbeitete Telekommunikationsgesetz ist am 22.06.2004 in Kraft getreten. Sinn und Zweck dieses Gesetzes ist die technologische Regelung und Förderung der Telekommunikation und Telekommunikations-Infrastruktur. Es soll eine angemessene und ausreichende Dienstleistung gewährleisten.

In diesem Gesetz werden Dinge wie Marktregulierung, Vergabe von Frequenzen, Nummern und Wegerechten, Details der Rundfunkübertragung, Kundenschutz und Missbrauchsaufsicht, Universaldienste sowie Belange der öffentlichen Sicherheit geregelt.

Aufgrund einer Richtlinie 95/46/EG des Europa-Parlamentes vom 29. Mai 2002 sollte das Telekommunikationsgesetz so erweitert werden, dass die Speicherung von Verbindungsdaten für einen gewissen Zeitraum nach deutschem Recht gültig wird. Bisher war nur die Speicherung der Verbindungsnachweise für abrechnungsrelevante Daten zulässig, diese mussten nach der Abrechnung wieder gelöscht werden. Da ein grosser Teil des Datenverkehrs für das Erstellen der Rechnung nicht von Belang ist, konnte kein Profil der Surfgewohnheiten eines einzelnen Nutzers erstellt werden.

Der neue Entwurf sah vor, die Vorratsspeicherung von Verbindungsdaten für einen begrenzten Zeitraum zuzulassen, damit diese Daten von staatlichen Stellen gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG "für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismässig ist, angewendet werden können."

Vor allem diese Leitlinie wurde von Datenschutzbeauftragten des Bundes und der Länder kritisiert, gemäss dem Fernmeldegesetz ist die Vorratsspeicherung nur unter konkretem Tatverdacht zulässig.

Nachdem dieser Gesetzentwurf durch Vermittlungsausschuss gegangen ist, wurden diese Passagen entgegen der EU-Richtlinie aus dem Gesetzestext gestrichen. Das Vorhalten der Verbindungsdaten über einen befristeten Zeitraum ist somit nicht Inhalt des des erlassenen Telekommunikationsgesetzes. Das Verfolgen besuchter Webseiten beziehungsweise das Bilden eines persönlichen Profils bevorzugter Webseiten ist damit nicht zulässig.

Allerdings wurde der Datenschutz durch andere Passagen ausgehöhlt. Zwar dürfen Verbindungsnachweise auch weiterhin nur zu Abrechnungszwecken kurzzeitig gespeichert werden, aber werden den Strafverfolgungsbehörden und -Organen Einblicke in die Privatsphäre des Individuums ermöglicht. Die entsprechenden Passagen beinhalten:

Gemäss §112 Absatz 1:

Kundenzugangsdaten müssen in einer separaten Datei gespeichert werden.

Gemäss §112 Absatz 2:

Auskünfte aus dieser Kundendatei einholen dürfen:

- 1.) Gerichte und Strafverfolgungsbehörden
- 2.) Polizeivollzugsbehörden zwecks Gefahrenabwehr
- 3.) Zollkriminalamt und Zollfahndung zur Vorbereitung und Durchführung von Massnahmen gemäss §39 des Aussenwirtschaftsgesetzes
- 4.) Verfassungsschutzbehörden sowie der militärische Abschirmdienst BND
- 5.) Bundesanstalt für Finanzdienstleistungsaufsicht
- 6.) Die zuständigen Stellen zur Verfolgung und Ahndung von Ordnungswidrigkeiten
- 7.) Die zuständigen Behörden zur Bekämpfung der Schwarzarbeit

§112 Absatz 4 (sinngemäss):

Die Regulierungsbehörde hat entsprechende Anfragen entgegenzunehmen und die angeforderten Zugangsdaten zu übermitteln. Prüfung auf Zulässigkeit erfolgt nur, wenn ein besonderer Anlass besteht.

Der Anfrage muss entsprechend protokolliert werden.

§113 (sinngemäss):

Die zuständigen Telekommunikationsdienstleister müssen Auskünfte an die Auskunftstellen erteilen. Das beinhaltet Zugriffsdaten zu Email-Konten oder anderer Webdienste.

Diese Paragraphen werden in der Ausführung mit nicht bedachten Problemen konfrontiert werden:

1.) Nachrichten müssen nicht in Reinform versandt werden

Emails können mittels freier Programme wie OpenPGP verschlüsselt werden. Dabei ist das Entschlüsseln einer solchen Email zurück in die Reinform keineswegs trivial. Der Email-Verkehr wird nicht verschlüsselt über den Emailserver und die jeweils benutzen Gateways und Router geschickt. Mit entsprechender Software ist es möglich, unverschlüsselte Emails in Reinschrift lesen zu können. Von da aus liegt der Schluss nahe, dass z.B. Absprachen über eine geplante Straftat oder sogar einen terroristischen Anschlag nicht in Klarschrift durch das Internet verschickt werden. Dafür spricht auch die Tatsache, dass einige Staaten wie zum Beispiel China ihren kompletten Internetverkehr über speziell staatlich kontrollierte Server abwickeln, damit die komplette Email-Korrespondenz und Netzwerkverkehr überwacht und gefiltert werden kann.

Es ist fraglich, ob diese Einschränkung des Datenschutzes zum gewünschten Erfolg führen wird.

2.) Artikel 10 des Grundgesetzes:

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, dass sie dem Betroffenen nicht mitgeteilt wird und dass an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Allerdings sagt der §112 Absatz 4 des Telekommunikationsgesetzes aus, dass Prüfung auf Zulässigkeit nur einem besonderen Anlass durchzuführen ist.

Der Emailverkehr ersetzt für viele die Korrespondenz über die klassischen Postwege. Wenn Staatsorgane aufgrund eines Verdachtes in der Lage sind, den privaten Briefverkehr einzelner Personen zu überwachen, lädt diese Möglichkeit geradezu dazu ein, grossflächig den Emailverkehr aufgrund eines "Generalverdachtes" gegen Schwarzarbeit zu überwachen, um entsprechende Beweise sammeln zu können. Wer kann garantieren, dass diese Mittel zur Strafverfolgung und -Vereitelung nicht missbraucht werden?