International Working Group
on Data Protection
in Telecommunications

Arbeitspapier
der Internationalen Arbeitsgruppe für den Datenschutz in der Telekommunikation zur Überwachung der Telekommunikation

(Übersetzung)

angenommen bei der 31. Sitzung der Arbeitsgruppe am 26./27. März 2002 in Auckland, Neuseeland

In den letzten Monaten haben viele demokratische Staaten neue Befugnisse zur Überwachung der Kommunikation geschaffen, um der Netzkriminalität zu begegnen und den Terrorismus zu bekämpfen. Die Arbeitsgruppe erkennt an, dass angemessene Gegenmaßnahmen ergriffen werden müssen. Sie betont aber auch, dass diese Maßnahmen verhältnismäßig sein müssen. In diesem Zusammenhang erinnert die Arbeitsgruppe daran, dass sie bereits mehrfach bei früheren Gelegenheiten die Bedeutung des Schutzes der Privatsphäre und der persönlichen Kommunikation gegen willkürliche Eingriffe als eines Menschenrechts betont hat (Gemeinsame Erklärung zur Kryptografie vom 12. September 1997 in Paris). Nationales und internationales Recht sollten unmissverständlich klarstellen, dass der Prozess der Kommunikation (z. B. mittels elektronischer Post) ebenfalls durch das Telekommunikationsgeheimnis geschützt ist.

Wenngleich diese Prinzipien die Staaten nicht daran hindern, Netzkriminalität und Terrorismus zu bekämpfen, muss daran erinnert werden, dass z. B. der Europäische Gerichtshof für Menschenrechte wiederholt betont hat, dass Staaten keine unbeschränkte Befugnis haben, Personen in ihrem Zuständigkeitsbereich heimlich zu überwachen. Jedes derartige Gesetz zur heimlichen Überwachung birgt die Gefahr, die Demokratie, die es verteidigen soll, zu untergraben oder gar zu zerstören. „... Staaten dürfen nicht im Namen des Kampfes gegen Spionage und Terrorismus alle Maßnahmen ergreifen, die sie für geeignet halten.“[1] Angemessene und wirksame Garantien gegen Missbrauch sind unverzichtbar. Das ist zusätzlich unterstrichen worden durch den Gemeinsamen Standpunkt der Arbeitsgruppe über die öffentliche Verantwortlichkeit in Bezug auf die Überwachung privater Kommunikation vom 15. April 1998 (Hong Kong)[2].

Vor kurzem hat auch das Europäische Parlament auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte hingewiesen, nach der jeder Eingriff in und jede Überwachung der Kommunikation notwendig und verhältnismäßig sein muss; es reicht nicht aus, dass der Eingriff nur nützlich oder wünschenswert ist.

[1] IGMR, Fall Klass und andere, Entscheidung vom 18. November 1977, Serie A Nr. 28, S. 23

[2] In diesem Gemeinsamen Standpunkt betonte die Arbeitsgruppe die Notwendigkeit von Verfahren, die der Öffentlichkeit die Gewissheit verschaffen, dass Überwachungsbefugnisse rechtmäßig, angemessen und verhältnismäßig ausgeübt werden.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

Die Arbeitsgruppe unterstützt die folgenden Vorschläge, die das Europäische Parlament in der Entschließung über die Existenz eines globalen Systems zur Überwachung privater und kommerzieller Kommunikation (ECHELON)[3] gemacht hat und fordert ihre weltweite Umsetzung:

- Staaten sollten ein gemeinsames Schutzniveau gegenüber nachrichtendienstlicher Tätigkeit anstreben und zu diesem Zweck einen Verhaltenskodex ausarbeiten, der sicherstellt, dass die Tätigkeit von Nachrichtendiensten in Übereinstimmung mit den Grundrechten und insbesondere mit dem Schutz der Privatsphäre ausgeübt wird, und sie sollten ein Verfahren der internationalen Kontrolle solcher Aktivitäten vorsehen;

- Staaten sollten ihre Bürger über die Möglichkeit informieren, dass ihre international übermittelten Nachrichten unter bestimmten Umständen abgefangen werden; diese Information sollte begleitet werden von praktischer Hilfe bei der Entwicklung und Umsetzung umfassender Schutzmaßnahmen, auch was die Sicherheit der Informationstechnik anbelangt;

- eine wirksame und effektive Politik betreffend die Sicherheit in der Informationsgesellschaft sollte entwickelt und umgesetzt werden, um auf diese Weise die Sensibilisierung aller Nutzer moderner Kommunikationssysteme für die Notwendigkeit und die Möglichkeiten des Schutzes vertraulicher Informationen zu erhöhen;

- benutzerfreundliche Kryptosoftware, deren Quelltext offen gelegt ist, sollte gefördert, entwickelt und hergestellt werden, da nur so garantiert werden kann, dass keine Hintertüren in Datenverarbeitungsprogramme eingebaut werden;

- öffentliche Verwaltungen sollten elektronische Post systematisch verschlüsseln, sodass langfristig Verschlüsselung zum Normalfall wird,

- ein Internationaler Kongress zum Schutz der Privatsphäre vor Telekommunikationsüberwachung sollte abgehalten werden, um für Nichtregierungsorganisationen eine Plattform zu schaffen, wo grenzüberschreitende und internationale Aspekte diskutiert und Tätigkeitsfelder und Vorgehen koordiniert werden können.

Die Arbeitsgruppe betont, dass diese Empfehlungen ihre Bedeutung nach den terroristischen Angriffen vom 11. September 2001 nicht eingebüßt haben.

[3] (A 5 - 0264/2001 (2001/2098) (INI))