

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder für eine freie Telekommunikation in einer freien Gesellschaft

Umfang und Intensität der Eingriffe in das von Art. 10 Grundgesetz geschützte Fernmeldegeheimnis haben in den letzten Jahren deutlich zugenommen. Ursächlich hierfür sind zum einen folgende Aspekte:

- **Erhebliche Zunahme der Telekommunikationsvorgänge**
 - Die Zahl der Telekommunikationsvorgänge hat sich vervielfacht. Darüber hinaus werden neben dem traditionellen Telefon neue Kommunikationsmöglichkeiten wie Fax und PC-Fax, das Mobiltelefon, e-mail und mail-boxen sowie das Internet genutzt.
- **Stark angestiegener Umfang und wesentlich verbesserte Aussagequalität der Daten**

- Die digitale Datenverarbeitung ermöglicht detaillierte Auswertungen großer Datenmengen.

- Die Datenverarbeitungsnetze bieten mehr und mehr aussagekräftige Bestandsdaten, wozu auch e-mail-Adresse, IP-Nummer oder domain name gehören. So können sich bei Mitgliedschaft in geschlossenen Netzen sogar Rückschlüsse auf Lebensanschauungen oder bestimmte Problemlagen ergeben, z. B. bei der Mitgliedschaft in bestimmten Interessengemeinschaften, etwa Aids-Selbsthilfegruppen.

- Die Verbindungsdaten geben in der Regel Auskunft, wer wann mit wem wie lange und wie häufig kommuniziert hat; werden fremde Geräte verwendet, geraten Unbeteiligte in Verdacht.

- Aus den Nutzungsdaten von Tele- und Mediendiensten lassen sich Rückschlüsse auf Interessengebiete und damit auf persönliche Eigenheiten und das Verhalten der Nutzenden ziehen.

- Mobiltelefone ermöglichen schon im Stand-by-Modus die Bestimmung ihres Standorts.

- **Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten**
 - Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.
- **Entwicklung des Internets zum Massenkommunikationsmittel**
 - Über das Netz werden immer mehr Alltagsgeschäfte abgewickelt: Wahrnehmung verschiedenartiger Informationsangebote, Erledigung von Bankgeschäften, Buchung von Reisen oder Bestellung von Waren und Dienstleistungen in virtuellen Kaufhäusern (e-commerce). Dadurch fallen immer mehr auswertbare Informationen über Lebensgewohnheiten und Bedürfnisse der Bürgerinnen und Bürger an.
- **Schwer durchschaubare Rechtslage**
 - Die Zersplitterung der Regelungen in Strafprozess-, Telekommunikations- und Multimediarecht machen diese wenig transparent und schwer anwendbar.

Zum anderen ist dieser größere, leichter auswert- und verarbeitbare Datenpool wachsenden Zugriffswünschen der Sicherheitsbehörden im weitesten Sinn auf nationaler und internationaler Ebene ausgesetzt:

- Die Zahlen der Telekommunikations-Überwachungsanordnungen in den letzten Jahren sind kontinuierlich angestiegen: 1995: 3667, 1996: 6428, 1997: 7776, 1998: 9802
- Immer mehr Straftatbestände wurden als Grund für eine Telekommunikationsüberwachung in § 100 a der Strafprozessordnung (StPO) einbezogen – der Katalog wurde seit Einführung 11 mal erweitert und damit bis heute nahezu verdoppelt. Neue Erweiterungen sind im Gespräch.

- Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendateien für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern verdächtige Personen einen Vertrag haben. Diese Verpflichtung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe, Behörden oder möglicherweise sogar Krankenhäuser betreffen.
- Ein europäischer Anforderungskatalog für Überwachungsmöglichkeiten unter dem Namen "ENFOPOL", befasst sich u. a. mit der Frage, welchen Anforderungen die Netzbetreiber bzw. Diensteanbieter genügen müssen, damit die auf der Grundlage nationaler Ermächtigungsgrundlagen zulässige Telekommunikationsüberwachung technisch durchführbar ist. Die G8-Staaten haben noch weitergehende Beschlüsse gefasst.

Forderungen zur Gewährleistung der freien Telekommunikation

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1996 ein Positionspapier erarbeitet. Vor diesem Hintergrund fordert die Konferenz:

- Freie Telekommunikation ist unabdingbar für eine freiheitliche demokratische Kommunikationsgesellschaft. Sie wird durch das Fernmeldegeheimnis geschützt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichts zu den verdachtslosen Abhörmaßnahmen des BND (BVerfG, Urt. v. 14.7.1999, 1 BvR 2226/94 u. a.) auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird. Die Geltung des Fernmeldegeheimnisses ist deshalb auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen.
- Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseu-donyme Nutzungsmöglichkeiten müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.
- Notwendig ist deshalb ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf eine unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt.
- Als Grundlage hierfür ist eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben vorzunehmen hinsichtlich Effektivität auf der einen und Eingriffsumfang auf der anderen Seite. Eine gesetzliche Berichtspflicht über Anlass, Verlauf, Ergebnisse und Anzahl der Betroffenen ist auch für Telekommunikationsüberwachungen einzuführen. Dass auch Unverdächtige von Abhör- und Kontrollmaßnahmen betroffen sein können, ist dabei besonders zu berücksichtigen.
- Der aus der Frühzeit der analogen Fernsprechtechnik stammende § 12 Fernmeldeanlagenengesetz, der die Herausgabe von Verbindungsdaten vergangener, nach bestrittener Rechtsprechung sogar zukünftiger Telekommunikationsvorgänge ohne Beschränkung auf schwerere Straftaten ermöglicht, muss wegen der erheblich höheren Aussagefähigkeit der digitalen Verbindungsdaten und des damit verbundenen Eingriffs in das Fernmeldegeheimnis zügig durch eine weniger weit reichende Regelung in der StPO ersetzt werden.
- Die Anforderungen aus dem bereits zitierten Urteil des Bundesverfassungsgerichts zur Telekommunikationsüberwachung sind unverzüglich umzusetzen.
- Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstellenanlagen in Hotels, Krankenhäuser oder Betrieben wäre unverhältnismäßig. Es muss deshalb verbindlich

klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungsverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o. g. Nebenstellenanlagen gilt. Darüber hinaus dürfen Anbieter von Guthabekarten zur Mobiltelefonie nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.

- Die Beachtung des Fernmeldegeheimnisses erfordert zwingend die Verschlüsselung von elektronischen Mitteilungen in offenen Netzen. Das Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik, das eine Kryptoregulierung ablehnt, ist ein wichtiger Schritt in die richtige Richtung. Gewerbliche Telekommunikationsdienstleister sollten gesetzlich verpflichtet werden, die Möglichkeit der verschlüsselten Kommunikation kostenlos zu unterstützen.
- Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen, bedürfen besonders im Interesse ihrer Klientel eines umfassenden Schutzes ihrer Telekommunikation.

Straftaten gegen den Schutz der Privatsphäre ist wirksamer entgegenzutreten. Notwendig sind z. B. die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik, eine Verbesserung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen und eine Verschärfung des strafrechtlichen Schutzes des Fernmeldegeheimnisses.