International Working Group
on Data Protection
in Telecommunications

Gemeinsamer Standpunkt zu Datenschutzaspekten des Entwurfs einer Konvention zur Datennetzkriminalität des Europarates

angenommen auf der 28. Sitzung der Arbeitsgruppe am 13./14. September 2000 in Berlin

- Übersetzung -

Vorwort

Der Europarat bereitet gegenwärtig ein „Übereinkommen über Datennetzkriminalität" vor, mit dem beabsichtigt ist, „... strafrechtliche Untersuchungen und Verfahren bezüglich der Straftaten in Verbindung mit Computersystemen und -daten wirksamer zu gestalten und um die Erfassung elektronischer Beweise bei Straftaten zu gestatten". Wichtige nichteuropäische Staaten wie die Vereinigten Staaten von Amerika, Kanada, Japan und Südafrika sind an dem Entwurfsprozess beteiligt. Der Entwurf des Übereinkommens soll bis Dezember 2000 fertig gestellt und frühestens im September 2001 zur Unterschrift aufgelegt werden. Der Entwurf selbst sieht den Beitritt weiterer Staaten auf Einladung des Ministerkomitees vor. Der Europarat hat erklärt, dass er den Konsultationsprozess mit interessierten Parteien unabhängig davon, ob es sich um öffentliche oder private Stellen handelt, vertiefen will.

Die Arbeitsgruppe erkennt an, dass eine Notwendigkeit zur internationalen Bekämpfung von Straftaten in Verbindung mit Computersystemen existiert, dass eine verbesserte internationale Kooperation in der Ära globaler Kommunikationsnetzwerke nötig ist und dass Strafverfolgungsbehörden zur Bekämpfung solcher Verbrechen angemessene Mittel benötigen. Auf der anderen Seite müssen diese Mittel mit anderen gemeinsamen Werten, z. B. dem Recht auf Datenschutz und dem Telekommunikationsgeheimnis, in Einklang gebracht werden.

Während das Europäische Übereinkommen zur Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union ausdrücklich den Schutz personenbezogener Daten regelt (Art. 23), enthält der gegenwärtige Entwurf eines Übereinkommens über Datennetzkriminalität keinen einzigen Hinweis auf Datenschutzbestimmungen. In dem Entwurf wurde auch versäumt, Verletzungen der Privatsphäre durch den einfachen Zugriff auf Computersysteme in klarer und unmissverständlicher Weise unter Strafe zu stellen.

Der Europarat verfügt über eine lange Tradition bei der Entwicklung von multilateralen Datenschutzstandards. Es scheint daher angemessen, dass in dem neuen Übereinkommen ausdrücklich auf das Übereinkommen zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108) von 1981 und die Empfehlung Nr. R (95) 4 zum Schutz personenbezogener Daten auf dem Gebiet der Telekommunikationsdienste unter besonderer Bezugnahme auf Telefondienste Bezug genommen wird. Die Arbeitsgruppe hält es für erforderlich, das Expertenkomitee des Europarates für Datenschutzfragen in den weiteren Entwurfsprozess mit einzubeziehen.

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

Neue Verfahren

Das Übereinkommen über Datennetzkriminalität zielt darauf ab, neue Verfahren einzuführen, um die Verfolgung von Verbrechen im Zusammenhang mit der Internetnutzung zu ermöglichen, einschließlich Maßnahmen, um Telekommunikationsdiensteanbieter zu zwingen, personenbezogene Daten (sowohl Inhalts- als auch Verbindungsdaten) von Kommunikationsvorgängen in Telekommunikations-Netzwerken zu speichern und diese nationalen und ausländischen Behörden, die mit strafrechtlichen Ermittlungen und Verfahren befasst sind, zugänglich zu machen.

Bereits in der Vergangenheit hat es eine Diskussion in verschiedenen Zusammenhängen über die Verpflichtung von Telekommunikations- und Internetdiensteanbietern gegeben, Daten über den gesamten Telekommunikations- und Internetverkehr für einen erweiterten Zeitraum zu speichern, damit diese Daten zur Verfügung stehen, wenn innerhalb dieses Zeitraums ein Verbrechen begangen wird. Die Arbeitsgruppe hält derartige Maßnahmen für unangemessen und damit inakzeptabel. Die Arbeitsgruppe unterstreicht, dass Verbindungsdaten im gleichen Ausmaß geschützt sind wie Inhaltsdaten (Art. 8 der Europäischen Menschenrechtskonvention). In dieser Hinsicht unterstützt die Arbeitsgruppe in vollem Umfang die Ergebnisse der Konferenz der Europäischen Datenschutzbeauftragten vom 6./7. April 2000 in Stockholm, bei der die Konferenz erklärt hat, dass eine solche Aufbewahrung von Verbindungsdaten durch Internetdiensteanbieter einen unangemessenen Eingriff in die den Einzelnen durch die Europäische Menschenrechtskonvention garantierten Grundrechte darstellen würde (http://www.datenschutz-berlin.de/doc/eu/konf/00_db_en.htm; vgl. auch Empfehlung 3/99 der Arbeitsgruppe nach Art. 29 zur Aufbewahrung von Verkehrsdaten durch Internetdiensteanbieter für Strafverfolgungszwecke; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp25de.pdf). Dies gilt auch für die Speicherung von Daten, die Aufschluss über die Internetnutzung des Einzelnen geben.

Bestehende Befugnisse zur Strafverfolgung sollten nicht in einer Art ausgeweitet werden, die in die Privatsphäre eindringen, bevor die Notwendigkeit für solche Maßnahmen überzeugend dargelegt worden ist.

Die Arbeitsgruppe hat bereits in der Vergangenheit erklärt, dass jegliches Abhören von privater Kommunikation Gegenstand von angemessenen Sicherungsmaßnahmen sein muss (vgl. Gemeinsamer Standpunkt über die öffentliche Verantwortung im Hinblick auf das Abhören privater Kommunikation; angenommen auf der 23. Sitzung in Hong Kong SAR, China, am 15. April 1998; http:/www.datenschutz-berlin.de/attachments/173/inter_de.htm). Existierende Bedingungen und Sicherungsmaßnahmen im nationalen Recht und dem Übereinkommen zur Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (Art. 23) müssen respektiert werden. Solche Bedingungen und Sicherungsmaßnahmen sollten wenigstens enthalten

- die vorherige richterliche Anordnung,
- die (nachträgliche) Benachrichtigung der Betroffenen,
- die Beschränkung der Nutzung,
- die Verpflichtung zur Protokollierung,
- die Überwachung und Kontrolle sowie
- eine öffentliche Rechenschaftspflicht.

Dementsprechend sollten solche Sicherungsmaßnahmen auch in den Entwurf des Übereinkommens über Datennetzkriminalität aufgenommen werden. Insbesondere die Zusammenarbeit von nationalen Behörden mit den Betreibern von öffentlichen und privaten Netzwerken sollte vorzugsweise auf eindeutige gesetzliche Verpflichtungen gegründet werden anstatt auf freiwillige Vereinbarungen, deren Einhaltung schwer zu kontrollieren ist.

Neue Straftatbestände

Gleichzeitig sieht die Konvention vor, verschiedene neue Straftatbestände einzuführen, die in den Strafgesetzen vieler Mitgliedstaaten des Europarates nicht enthalten sind.

Die Einführung neuer Straftatbestände im Strafrecht muss mit extremer Zurückhaltung behandelt werden, weil eine weite Formulierung solcher neuen Straftatbestände wie auch die Kriminalisierung von Versuch und Beihilfe zu solchen Straftaten zu einer erheblichen Absenkung des Datenschutzstandards für alle Nutzer von Telekommunikationsnetzen führen kann; dadurch würde eine enorme Menge personenbezogener Daten über die Nutzung von Telekommunikationsnetzen und des Internet entstehen, wodurch das Recht zur anonymen Nutzung dieser Dienste abgeschafft würde. Es ist vorhersehbar, dass die beabsichtigten Regelungen zur Personalisierung jeder einzelnen Handlung jedes Nutzers in dem globalen Netz führen könnten, was offensichtlich unangemessen wäre.

Hinsichtlich der Straftatbestände, die in den Artikeln 1 bis 13 behandelt werden, besonders der Kriminalisierung „unerlaubter Vorrichtungen“ (Art. 6), von „Datenveränderung“ und der „Störung des Systems“ (Art. 4 und 5), ist die Arbeitsgruppe der Ansicht, dass es zur Bekämpfung der Netzkriminalität geeigneter wäre, wenn die Vertragsstaaten des Übereinkommens sich verpflichten würden, Diensteanbieter dazu zu zwingen, bestimmte Sicherheitsmaßnahmen beim Anschluss ihrer Systeme an ein öffentliches Netzwerk zur Verbesserung des Sicherheitsstandards im Internet im Allgemeinen zu treffen als einfach neue Straftatbestände zu schaffen, die sich auf eine große Spannweite von Internetaktivitäten beziehen und sogar Aktivitäten unter Strafe stellen könnten, die zur Verbesserung der Sicherheit im Netz gedacht sind.