

Dr. Alexander Dix, LL.M.

Landesbeauftragter für den Datenschutz

und für das Recht auf Akteneinsicht

Brandenburg

Stellungnahme vor dem

Unterausschuss Neue Medien

des Deutschen Bundestages

Expertengespräch Cyber-Crime / TKÜV

Donnerstag, 5. Juli 2001, 15:00 – 18:00 Uhr

Ich beschränke meine Stellungnahme auf die Fragen zu b) 3, 5 und 8 und zu c) 8, 14, 15, 19 u. 20 des Fragenkatalogs.

Vorbemerkung

Die Bekämpfung der „Cyber-Kriminalität“ (nicht notwendig identisch mit „Datennetz-kriminalität“) bedarf zweifellos der verbesserten internationalen Zusammenarbeit. Dabei ist allerdings zu unterscheiden zwischen Angriffen auf die Sicherheit des Netzes oder einzelner vernetzter Rechner und der Nutzung des Netzes zur Vorbereitung von Straftaten. Hinsichtlich der zuerst genannten Risiken sollte das Hauptgewicht auf präventive Maßnahmen gelegt werden, wie es die Europäische Kommission zutreffend in ihrer Mitteilung über die Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung

der Computerkriminalität¹ getan hat. Die Kommission hat einen Diskussionsprozess in Gang gesetzt, in dem Strafverfolgungs- und Polizeibehörden mit Providern und Datenschützern nach Lösungen suchen sollen.

Soweit es um die Bekämpfung von internetgestützter Kriminalität geht, für die das Netz nicht Angriffsziel, sondern Medium ist, muss eine sorgfältige Abwägung zwischen den Interessen der Strafverfolgung und dem Recht der Nutzer auf Schutz ihrer Privatsphäre und auf unbeobachtete Nutzung der neuen Medien stattfinden. Dabei ist auch ein grundsätzliches Recht auf anonymen oder pseudonymen Zugang und Nutzung von Netzangeboten anzuerkennen². Die Interessen der Strafverfolgung rechtfertigen es in einem online-Medium ebensowenig wie in der offline-Welt, jeden Menschen und jede seiner Bewegungen bzw. Äußerungen auf Vorrat zu registrieren und ihn einem Identifikationszwang zu unterwerfen. Nur im Einzelfall kann es ausnahmsweise gerechtfertigt sein, bei einem konkreten Verdacht und unter Einhaltung rechtsstaatlicher Garantien auf vorhandene personenbezogene Daten für Strafverfolgungszwecke zuzugreifen (evtl. auch ein Pseudonym aufzudecken), die zu Zwecken der Kommunikation verarbeitet werden.

Auch die Bekämpfung der Cyberkriminalität rechtfertigt es nicht, dass die Telekommunikationsnetze entgegen ihrem ursprünglichen Zweck generell zu Überwachungsnetzen umgewidmet werden.

b) Internationale Ansätze – Cyber-Crime:

- 3. Wie bewerten Sie die in dem Konventions-Entwurf vorgesehenen Bestimmungen und Regelungen aus datenschutzrechtlicher Sicht? Inwieweit sind beispielsweise die Begriffsbestimmungen des Entwurfs kompatibel mit bestehenden internationalen Datenschutzbestimmungen und welche Voraussetzungen könnten u.U. eine Verwertung von aus dem***

¹ KOM(2000)890 endgültig

² S. Mitteilung der EU-Kommission, ebda., Ziff. 5.3

Ausland auf Grundlage der Konvention übermittelten Informationen vor nationalen Gerichten im Wege stehen?

Der Konventionsentwurf trägt auch in seiner letzten Fassung, die vom Strafrechtsausschuss des Europarates am 22 Juni 2001 gebilligt worden ist, den datenschutzrechtlichen Anforderungen nicht hinreichend Rechnung.

Der Europarat hat eine lange Tradition in dem Bemühen, den Schutz der Grund- und Menschenrechte und insbesondere den Datenschutz auf europäischer Ebene zu verankern und ihm effektive Geltung zu verschaffen. Diese Tradition hat ihren Niederschlag vor allem in der Europäischen Menschenrechtskonvention von 1950 und in der Konvention No. 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1981 gefunden, aber auch in den Empfehlungen Nr. R(87) 15 über die Nutzung personenbezogener Daten im Polizeibereich und Nr. R(95) 4 über den Schutz personenbezogener Daten im Bereich der Telekommunikationsdienste, insbesondere der Telefondienste.

Die Vorarbeiten für den Entwurf der Cybercrime-Konvention sind seit 1997 fast ausschließlich von Vertretern der nationalen Strafverfolgungs- und Polizeibehörden vorangetrieben worden. Die nationalen Datenschutzbeauftragten wie auch der beim Europarat vorhandene datenschutzrechtliche Sachverständige sind zunächst überhaupt nicht hinzugezogen worden. Das erklärt zum Teil, dass der jetzt beschlossene Entwurfstext durch eine bemerkenswerte Unausgewogenheit und Einseitigkeit zugunsten der Interessen der Strafverfolgungsbehörden gekennzeichnet ist, auch wenn gegenüber den Vorentwürfen einige, wenngleich unzureichende datenschutzrechtliche Verbesserungen vorgenommen worden sind. Diese Unausgewogenheit steht in auffallendem Gegensatz zu der erwähnten Mitteilung der EU-Kommission³.

³ S.o. Fn.1

Erst in einem relativ weit fortgeschrittenen Stadium hat die Expertengruppe des Europarats eine Entwurfsfassung veröffentlicht, so dass vorher angesichts des intransparenten Verfahrens keine Möglichkeit bestand, sich mit den Vorstellungen der Expertengruppe zur Cyberkriminalität auseinanderzusetzen.

Insbesondere die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation und die Datenschutzgruppe nach Art. 29 der Europäischen Datenschutzrichtlinie haben grundsätzliche Kritik an dem Entwurf in einer früheren Fassung (25. Version) geübt, die im Grunde nur in zwei Punkten aufgegriffen worden ist.

So hatte die Internationale Arbeitsgruppe u.a. bemängelt, dass der Konventionsentwurf mit seinen Regelungen zur Harmonisierung der materiell-rechtlichen Straftatbestände insbesondere zu Hacker-Angriffen in einer Vorversion auch solche Techniken unter Strafe gestellt hätte, die von verantwortlichen Stellen (z.B. auch großen Unternehmen in der EDV-Branche) eingesetzt werden, um die Sicherheit der eigenen Systeme gegen Angriffe aus dem Netz zu überprüfen⁴. Dem trägt die endgültige Entwurfsfassung jetzt immerhin dadurch Rechnung, dass sie solche Verfahren von der Strafandrohung ausnimmt, die nicht zum Zweck der Begehung einer Straftat, sondern zu Test- und Datensicherheitszwecken angewandt werden (Art. 6 (2) Endgültiger Entwurf).

Die Datenschutzgruppe nach Art. 29 hatte u. a. kritisiert, dass der Datenschutz und die hierzu vom Europarat initiierte Konvention No. 108 und die speziellen Empfehlungen für den Polizei- und Telekommunikationsbereich in den Vorversionen der Konvention nicht einmal in den Erwägungsgründen Erwähnung gefunden hatte⁵. Auch dieser Kritikpunkt ist in der endgültigen Entwurfsfassung berücksich-

⁴ Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation, Gemeinsamer Standpunkt zu Datenschutzaspekten des Entwurfs einer Konvention zur Datennetzkriminalität des Europarates v. 13./14.9.2000, Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht /Berliner Beauftragter für Datenschutz und Akteneinsicht (Hrsg.), Dokumente zum Datenschutz 2000, S. 69, auf Englisch abrufbar unter <http://www.datenschutz-berlin.de/doc/int/iwgdpt/cy_en.htm>

⁵ Artikel 29 – Datenschutzgruppe, Stellungnahme 4/2001 zum Entwurf einer Konvention des Europarates über Cyberkriminalität v. 22.3.2001 (WP 41), <http://europa.eu.int/comm/internal_market/de/media/dataprot/wpdocs/index.htm>

tigt worden. Damit ist der Datenschutz inzwischen immerhin über eine Erwähnung in den Fußnoten und in der Begründung hinausgekommen. Im eigentlichen Text des Konventionsentwurfs tauchen allerdings die Begriffe „Datenschutz“ oder „Privatsphäre“ nach wie vor an keiner Stelle auf. Das ist für ein internationales Abkommen, das die zwischenstaatliche Zusammenarbeit bei derart intensiven Grundrechtseingriffen regeln soll, vor dem Hintergrund unserer Verfassung nicht akzeptabel.

Der zentrale Kritikpunkt sowohl der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation als auch der Art. 29-Gruppe schon gegenüber früheren Konventionsentwürfen richtet sich gegen das völlige Fehlen von materiellen Bestimmungen zum Umgang mit personenbezogenen Daten, die im Zuge von Telekommunikationsüberwachungen oder Zugriffen auf rechnergestützte Dateien anfallen.

Die Internationale Arbeitsgruppe⁶ hat insbesondere gefordert, dass private Kommunikation nur dann überwacht werden darf, wenn bestimmte Bedingungen in den beteiligten Staaten erfüllt sind:

- 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 der die Überwachung anordnenden Stellen.

Demgegenüber begnügt sich der Konventionsentwurf damit, die prozeduralen

⁶ S.o. Fn.4

Voraussetzungen zur grenzüberschreitenden Zusammenarbeit der Behörden bei der Bekämpfung der Datennetzkriminalität festzulegen, ohne gleichzeitig die Bedingungen zu harmonisieren, unter denen die Vertragsstaaten in Grundrechte, insbesondere in das Recht auf Achtung des Privat- und Familienlebens und der Kommunikation (Art. 8 der Europäischen Menschenrechtskonvention, vgl. auch Art. 7 der Europäischen Grundrechte-Charta) eingreifen dürfen. Das ist ein gravierender Mangel, der auch durch die Sollvorschrift des Art. 15 Abs. 2 des Entwurfs nicht ausgeglichen werden kann. Danach „sollen“ die Vertragsstaaten sicherstellen, dass die vereinbarten grenzüberschreitenden Überwachungsmaßnahmen in Übereinstimmung mit innerstaatlichen Rechtsgarantien durchgeführt werden, die einen „angemessenen“ Schutz der Menschenrechte gewährleisten sollen. Die Verpflichtung zur Kooperation entfällt nicht dadurch, dass ein ersuchender Vertragsstaat dieser Sollvorschrift nicht entspricht. Art. 15 des Konventionsentwurfs verzichtet darauf, irgendwelche Sanktionen für die Nichtbefolgung vorzusehen. Damit hat die Vorschrift den Charakter eines bloßen Programmsatzes. Möglicherweise wurde diese offene Formulierung bewusst deshalb gewählt, um auch solchen Staaten den Beitritt zur Konvention zu ermöglichen, denen rechtsstaatliche Garantien und Beschränkungen für Überwachungen der Telekommunikation bisher fremd sind. Auf die dadurch entstehenden Probleme wird noch in der Antwort auf Frage 5 eingegangen.

Die Art. 29-Datenschutzgruppe⁷ hat ebenfalls nachdrücklich empfohlen, dass in den Konventionsentwurf Datenschutzbestimmungen aufgenommen werden, die umreißen, inwieweit Personen geschützt werden müssen, über die Informationen im Zusammenhang mit Überwachungsmaßnahmen verarbeitet werden sollen. Das können bekanntlich auch unverdächtige Kommunikationspartner von verdächtigen Personen sein. Der Konventionsentwurf enthält demgegenüber im auffälligen Gegensatz zum Abkommen von Schengen und zur Europol-Konvention keinerlei derartige Datenschutzregelungen.

Er unterschreitet auch das Schutzniveau, das der Rat und das Europäische Par-

lament in der Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr für den Datenexport in außereuropäische Drittstaaten etabliert haben. Diese Richtlinie wird teilweise auch im Bereich der „dritten Säule“ angewandt. Unabhängig davon wäre es nicht gerechtfertigt, den Export von personenbezogenen Daten im privaten Sektor an strengere Bedingungen zu knüpfen als im öffentlichen Sektor bzw. bei der Strafverfolgung. In den zuletzt genannten Bereichen ist der Grundrechtsbezug sogar intensiver.

Schließlich unterschreitet der Konventionsentwurf auch das Schutzniveau, das der Europarat selbst in Art. 12 der Konvention No. 108 für den grenzüberschreitenden Datenverkehr aufgestellt hat.

Es ist bezeichnend, dass in der letzten Phase der Beratungen sogar der moderate Versuch mehrerer Delegationen im Expertenausschuss für Fragen der Datennetzkriminalität gescheitert ist, die Befugnis von Vertragsstaaten zur Ablehnung von Rechtshilfeersuchen auch auf den Fall auszudehnen, dass der ersuchte Staat der Auffassung ist, dass im ersuchenden Staat kein angemessenes Datenschutzniveau gewährleistet ist. Da dieser Vorschlag von mehreren Delegationen abgelehnt wurde, gibt der Abschlussbericht des Expertenausschusses einen Kompromissvorschlag wieder, nach dem neben einer Erwähnung der Datenschutzabkommen und –empfehlungen des Europarates in den Erwägungsgründen des Konventionsentwurfs der ersuchende Staat durch eine Soll-Vorschrift („shall“) aufgefordert werden sollte, die übermittelten Informationen nur zweckgebunden in dem Strafverfahren zu verwenden, für das sie angefordert wurden. Sogar dieser Kompromissvorschlag scheiterte am Widerstand einer Delegation⁸, so dass der jetzt beschlossene Entwurfstext (Art. 28 Abs. 2) es der ersuchten Seite völlig freistellt („may“), die Datenübermittlung davon abhängig zu machen, dass der ersuchende Staat die Informationen nur zweckgebunden verwendet oder dass er sie vertraulich behandelt. Wenn der ersuchende Staat diese Bedingung ablehnt, kann der er-

⁷ S.o. Fn.2

suchte Staat entscheiden, dem Ersuchen auch ohne Bedingungen nachzukommen (Art. 28 Abs. 3).

Diese Spurenelemente der Zweckbindung und eine fakultative Verpflichtung zur vertraulichen Behandlung der übermittelten Daten sind aber nur ein kleiner Ausschnitt aus den notwendigen Datenschutzgarantien (s.o. die von der Internationalen Arbeitsgruppe geforderten weitergehenden materiell-rechtlichen Sicherungen wie z. B. Benachrichtigungs- und Löschungspflichten, die der Konventionsentwurf nicht aufweist).

Im Übrigen ermöglicht es der Konventionsentwurf an mehreren Stellen dem ersuchten Vertragsstaat, die Kooperation unter Hinweis auf die Souveränität, die Sicherheit, den ordre public oder andere wesentliche Interessen abzulehnen (Art. 27 Abs. 4, 29 Abs. 5, 30 Abs. 2). Ob der Datenschutz zum ordre public oder zu den wesentlichen Interessen im Sinne dieser Regelungen zu zählen ist, ist sehr zweifelhaft und dürfte außerdem von Land zu Land verschieden zu beurteilen sein. Auch diese Vorschriften können deshalb das Fehlen materieller und expliziter Datenschutzbestimmungen im Konventionsentwurf nicht kompensieren.

5. Welche Auswirkungen erwarten Sie durch die ausdrückliche Einladung des Europarates an Nicht-Mitglieder und/oder Nicht-Unterzeichner der Europäischen Menschenrechtskonvention, der Cyber-Crime-Konvention beizutreten und so ebenfalls in den Genuß der vereinfachten Rechtshilfe und beschleunigten Ermittlungsverfahren zu kommen?

Der Konventionsentwurf soll nach Art. 36 auch von solchen Staaten unterzeichnet werden können, die dem Europarat nicht angehören, aber an der Ausarbeitung des Konventionsentwurfs beteiligt waren. Dies sind die USA, Kanada, Japan und

⁸ Final Activity Report, 25.5.2001 (CDPC (2001) 2 rev), Notes 9, 10

Südafrika. Der Ministerausschuss kann darüber hinaus nach Art. 37 des Konventionentwurfs mit den Stimmen aller ursprünglichen Vertragsstaaten auch später weitere außereuropäische Staaten zum Beitritt auffordern.

In beiden Fällen wird die Unterzeichnung bzw. der Beitritt außereuropäischer Staaten nicht davon abhängig gemacht, dass der beitretende Staat sich verpflichtet, die Menschenrechts- und Datenschutzgarantien zu beachten, zu deren Achtung sich die Mitgliedstaaten des Europarats verpflichtet haben. Damit büßt das implizit im Konventionstext vorausgesetzte Niveau des Grundrechtsschutzes vollends seine Chancen auf Realisierung im internationalen Rechtshilfeverkehr bei der Bekämpfung der Cyberkriminalität (nicht nur Netzkriminalität) ein.

Außereuropäische Staaten sollten zumindest wie beim Schengener Abkommen verpflichtet werden, der Europarats-Konvention No. 108 zum Datenschutz beizutreten. Eine ähnliche Forderung hat auch die Parlamentarische Versammlung des Europarates erhoben. Sonst würde der Europarat seine eigenen bisher aufgestellten Standards zum grenzüberschreitenden Datenverkehr entwerten.

8. Der Entwurf sieht vor, dass die Umsetzung in nationales Recht allein nach Maßgabe der bestehenden nationalen Rechtsbestimmungen und Rechtstraditionen erfolgen soll. Ist dieser Mechanismus Ihres Erachtens hinreichend, um einer substanziellen Aushöhlung bestehender Rechtsnormen und Senkung des Grundrechtsschutzniveaus – beispielsweise in Einzelstaaten aber auch innerhalb der Europäischen Union – entgegenwirken zu können?

Der Mechanismus ist aus zwei Gründen völlig unzureichend: Zum einen enthält die Konvention keinen Mindeststandard dafür, welche materiellrechtlichen Voraussetzungen für Überwachungsmaßnahmen das nationale Recht vorsehen sollte. Zum anderen bleibt es allein den betroffenen Vertragsstaaten (er-

suchender und ersuchter Staat) überlassen, ob sie wegen Nichteinhaltung nationaler Standards die Kooperation ablehnen bzw. dennoch auf ihr bestehen.

Aber auch für die EU-Mitgliedstaaten und insbesondere für die Bundesrepublik mit einem vergleichsweise hohen Datenschutzniveau und mit besonderen Vorkehrungen zum Schutz des Fernmeldegeheimnisses würde ein Beitritt zur Konvention in der gegenwärtigen Fassung mittel- und langfristig erhebliche negative Auswirkungen haben. Sie könnten nicht auf Dauer unter Verweis auf innerstaatliche Regelungen zum Datenschutz und zum Fernmeldegeheimnis auf die Cybercrime-Konvention gestützte Rechtshilfeersuchen aus Ländern mit einem niedrigeren (inadäquaten) Schutzniveau ablehnen (wozu sie verfassungsrechtlich verpflichtet wäre), ohne jedenfalls rechtspolitisch dem Einwand des „venire contra factum proprium“ ausgesetzt zu werden. Mit anderen Worten: die Konvention wird zu einem wachsenden internationalen Druck auch auf die EU-Staaten und die Bundesrepublik beitragen, ihr innerstaatliches Rechtssystem zu Lasten des Daten- und Kommunikationsschutzes zu modifizieren. Die im Konventionsentwurf vorgesehene Harmonisierung im einseitigen Interesse der Strafverfolgungsbehörden würde zu einer kontinuierlichen Absenkung des Grundrechtsschutzes führen, die in eindeutigem Gegensatz etwa auch zur Europäischen Grundrechte-Charta (Art. 7 und 8) stünde.

Die Bundesregierung sollte aufgefordert werden, dem Konventionsentwurf im Ministerkomitee des Europarates nur dann zuzustimmen, wenn er unter Berücksichtigung der Vorgaben des Europäischen Gemeinschaftsrechts, der Europäischen Datenschutzkonvention und des nach dem Grundgesetz garantierten Fernmeldegeheimnisses modifiziert und insbesondere um materielle Vorschriften zur Sicherung dieser Vorgaben ergänzt wird.

Interessanterweise haben die USA bei der abschließenden Beratung im Strafrechtsausschuss in anderem Zusammenhang erklärt, sie könnten der Konvention aus verfassungsrechtlichen Gründen nicht beitreten, wenn sie keine Bundesstaatsklausel enthielte (was drei europäische Staaten bisher ablehnen). Dieser

letzte noch kontroverse Punkt (Art. 41) soll nun im Ministerkomitee geklärt werden. Die Bundesrepublik sollte unter Hinweis auf die verfassungsrechtliche Garantien des Datenschutzes und des Telekommunikationsgeheimnisses dem Beispiel der Vereinigten Staaten folgen und die Unterzeichnung ablehnen, solange der Konventionstext diese Garantien nicht durch die Aufnahme von Datenschutzregelungen ausdrücklich berücksichtigt.

c) Nationale Ansätze – TKÜV:

8. Sehen Sie in § 8 Nr. 3 der TKÜV-E die Verpflichtung des Verpflichteten, verschlüsselte Daten den Berechtigten unverschlüsselt zur Verfügung zu stellen?

Diese Verpflichtung besteht nur dann, wenn der Verpflichtete selbst einen Verschlüsselungsdienst netzseitig anbietet. Die Regelung hat keine Auswirkungen, wenn Endnutzer ihre Kommunikation selbst durch frei verfügbare Verschlüsselungssoftware (z.B. PGP) gegen unbefugte Kenntnisnahme Dritter schützen.

14. Inwiefern besteht die Gefahr, daß in das Fernmeldegeheimnis unbeteiligter Dritter eingegriffen wird?

Bei jeder Telekommunikationsüberwachung besteht die Wahrscheinlichkeit, dass in das Fernmeldegeheimnis unbeteiligter Dritter eingegriffen wird. Dies ist kein spezifisches Problem der TKÜV. Der Gesetzgeber ist von Verfassungs wegen verpflichtet, diesem Umstand durch Benachrichtigungs-, Lösungs- und Kennzeichnungspflichten Rechnung zu tragen. Er hat dies im materiellen Recht bereits teilweise in der Strafprozessordnung und neuerdings für einen Teilbereich (Kennzeichnung) im G 10 getan.

15. Wie bewerten Sie die Verhältnismäßigkeit des Verordnungs-Entwurfes?

Die Verhältnismäßigkeit des Verordnungs-Entwurfs ist deshalb fragwürdig, weil durch ihn eine Infrastruktur der Überwachung geschaffen würde, die auch einen unbeobachteten Zugang zum Internet und Abruf von Informationen aus dem Netz vereiteln könnte. Insbesondere die Verpflichtung der Internet-Provider zur Bereitstellung von Überwachungsschnittstellen macht es technisch möglich, künftig den gesamten Internet-Verkehr, also auch das bloße „Surfen“ zu beobachten. Die für die Sprachtelefonie bisher gegebenen Überwachungsmöglichkeiten werden durch den Verordnungs-Entwurf undifferenziert auf alle anderen Formen der elektronischen Kommunikation übertragen, ohne dass dabei berücksichtigt wird, dass bei der Nutzung des Internets ein erheblich größerer Ausschnitt der Persönlichkeit abgebildet wird als bei der Sprachtelefonie.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich deshalb in ihrer EntschlieÙung vom 11. Mai 2001 mit Entschiedenheit dagegen gewandt, dass eine technische Infrastruktur zur Überwachung des gesamten Internet-Verkehrs geschaffen wird. Sie sehen darin einen unverhältnismäßigen Eingriff in das Persönlichkeitsrecht der Nutzer und betonen, dass eine derartige Überwachung auch den Grundsätzen des Systemdatenschutzes (Datenvermeidung und Datensparsamkeit) in den Multimedia-Gesetzen von Bund und Ländern zuwiderlaufen würde.

Die Bundesregierung sollte nach meiner Auffassung den Entwurf der TKÜV solange zurückstellen, bis die Ergebnisse des vom Bundesjustizministerium in Auftrag gegebenen Gutachtens über die Effektivität der herkömmlichen Telekommunikationsüberwachung vorliegen, und dann insgesamt sowohl die gegenwärtig bestehenden materiellen Überwachungsbefugnisse als auch deren Erstreckung auf die neuen Kommunikationstechniken einer kritischen Überprüfung zu unterziehen.

Zudem muss auch der TKÜV-Entwurf vor einer endgültigen Beschlussfassung

dringend um aussagefähige Evaluationspflichten ergänzt werden.

Problematisch ist schließlich, dass § 7 des Entwurfs einen festen Datenkatalog vorgibt, den die Verpflichteten bereithalten müssen. Dadurch wird der Eindruck erweckt, die Verordnung enthalte eine entsprechende materiell-rechtliche Verpflichtung. Eine solche wäre aber durch die Verordnungsermächtigung des § 88 Abs.2 Satz 2 TKG nicht gedeckt. Welche Daten bereitzuhalten sind, kann sich nur aus dem materiellen Recht (StPO, AWG, G 10) und der darauf gestützten Anordnung ergeben. Die TKÜV kann dem Verpflichteten nur aufgeben, welche Daten er technisch bereithalten muss, wenn er dazu materiell-rechtlich verpflichtet wird.

Zudem würde § 7 Abs. 1 Satz 1 Nr. 7 TKÜV-E, der dem verpflichteten Mobilfunkbetreiber aufgibt, stets auch den Standort des Endgeräts bereitzuhalten, eine innovationshemmende Wirkung entfalten. Denn Mobilfunkbetreiber, die in Zukunft eine technische Lösung anbieten würden, bei der Nachrichten an Endnutzer ohne Kenntnis ihres Standorts übermittelt werden, dürften keine Genehmigung nach dem 4. Teil des Verordnungsentwurfs erhalten. Solche – datenschutzfreundlichen – Techniken sind in der Entwicklung

Zu begrüßen ist allerdings, dass der Verordnungsentwurf in § 7 Abs.1 Satz 1 Nr.7 keine Verpflichtung zur Bereitstellung des Endgeräte-Standorts enthält, wenn von dem Gerät keine Telekommunikation ausgeht. Demgegenüber hat der Bundesgerichtshof in einem fragwürdigen Beschluss eine solche Verpflichtung aus der Strafprozessordnung selbst dann abgeleitet, wenn mit dem Handy gerade nicht telefoniert wird (Stand-by-Modus)⁹.

19. Besteht auf Grundlage der TKÜV-E aus ihrer Sicht hinreichende Rechtsklarheit?

Das ist zu bezweifeln. Die Rechtsunsicherheit beruht allerdings weniger auf dem TKÜV-Entwurf als vielmehr auf dem zugrunde liegenden Telekommunikationsgesetz (TKG), das selbst dringend einer Novellierung bedarf. Die Begriffsbestimmungen des § 3 Nr. 16, 17 und 19 TKG haben nicht zu einer nachvollziehbaren Abgrenzung zwischen der Telekommunikation auf der Basis des physikalischen Netzes und der Dienste- bzw. der Inhaltsebene geführt.

Auch dies spricht dafür, den Erlass der TKÜV bis zur Novellierung des TKG im Zuge einer kritischen Überprüfung der Telekommunikations- und Multimediarechts zurückzustellen. Diese sollte der Gesetzgeber zugleich zum Anlass nehmen, ein Mediennutzungsgeheimnis zu schaffen, das entsprechend dem Telekommunikationsgeheimnis eine grundsätzlich unbeobachtete Kommunikation etwa bei der Nutzung von Tele- und Mediendiensten für Alltagsgeschäfte sicherstellt.

20. Wie schätzen Sie die Abgrenzungsproblematik der TKÜV-E insbesondere hinsichtlich der Teledienste und Mediendienste nach TDG und MDSStV ein?

S. o. Antwort zu Frage 19.

Dr. Dix
