

zum Entwurf zur Neuregelung der Telekommunikations-Überwachungsverordnung (TKÜV) in der Fassung vom 06.07.2004

Der zur Diskussion vorgelegte Entwurf zur Neuregelung der TKÜV führt in weiten Teilen die bereits bestehenden Verpflichtungen privater Telekommunikationsunternehmen für staatliche Zwecke bei der Telekommunikationsüberwachung fort. Es bleibt insoweit bei der grundsätzlichen Kritik an den damit verbundenen erheblichen Belastungen, die Telekommunikationsunternehmen in Deutschland auferlegt werden.

Darüber hinaus weitet der neue Entwurf die Verpflichtungen und damit die Belastungen in verschiedener Hinsicht weiter aus. Dabei lassen sich zusammenfassend drei Gruppen kritikwürdiger Neuerungen zusammenfassen:

- Der Anwendungsbereich der TKÜV wird in zweierlei Hinsicht direkt erweitert, wobei im Falle der polizeilichen Überwachung zu Präventivzwecken die eigentliche Befugnisenerweiterung aus den einzelnen Landespolizeigesetzen erfolgt und nur in der TKÜV umgesetzt wird. Unmittelbar aus der TKÜV ergibt sich dem gegenüber die künftige Einbeziehung der Netzknotenpunkte zur Zusammenschaltung mit ausländischen TK-Netzen (sog. Auslandsköpfe) in den Kreis der überwachungspflichtigen Einrichtungen.
- An zahlreichen Stellen wird eine Umformulierung bisheriger Vorschriften vorgeschlagen, die durch die Einführung neuer, oftmals offenerer Begriffe geeignet (und möglicherweise auch bestimmt) sind, in der Praxis neue Pflichten und Überwachungsmöglichkeiten zu eröffnen, ohne dass dies dem erkennbaren Willen des zur Verordnungsgebung ermächtigenden Gesetzes entspricht.
- Bei der Regelung des eigentlichen Verfahrens werden durch die nunmehr geforderte jederzeitige Rückfragemöglichkeit für die Sicherheitsbehörden die organisatorischen Anforderungen an die Unternehmen noch einmal erhöht. Zugleich wird die Chance vergeben, durch dringend erforderliche Vorgaben zur Standardisierung der Anordnungen und Zuständigkeiten für eine Vereinfachung und größere Transparenz bei der Umsetzung von Überwachungsverfügungen beizutragen.

Diese Neuerungen sind geeignet, die ohnehin schon hohe Belastung der Unternehmen durch die Pflichten bei der TK-Überwachung noch weiter zu steigern. Es bestehen hiergegen erhebliche Zweifel, ob die zusätzlichen Belastungen angesichts oft nur geringer oder zum Teil überhaupt nicht erkennbarer Sicherheitsgewinne dem Verhältnismäßigkeitsgrundsatz genügen. Insgesamt führt die im vorliegenden Entwurf enthaltene Breite und Tiefe der Bestimmungen dazu, dass sich die TKÜV in weiten Teilen außerhalb der gesetzlich vorgesehenen engen Regelungsrahmens befindet. Es sei nachdrücklich in Erinnerung gerufen, dass nach § 110 Abs. 2 TKG der Verordnungsgeber gehalten ist, für die Umsetzung von Überwachungsmaßnahmen lediglich die *grundlegenden* technischen Anforderungen festzuhalten und hinsichtlich der organisatorischen Ausgestaltung sich auf die Regelung von bloßen *Eckpunkten* zu beschränken.

BITKOM verkennt nicht, dass an einigen Stellen auch durchaus Verbesserungsvorschläge der Wirtschaft aufgegriffen wurden. Dennoch besteht weiterhin erheblicher Verbesserungsbedarf bei den Vorgaben der TKÜV, um den Unternehmen die Erfüllung der Verpflichtungen

mit möglichst geringem bürokratischem Aufwand zu ermöglichen und für ausreichende Planungs- und Rechtssicherheit sowie den Schutz der getroffenen Investitionen zu sorgen.

Im Einzelnen gilt zu den vorgeschlagenen Neuregelungen Folgendes:

§ 1: Gegenstand der Verordnung

In § 1 Nr. 1 lit. d) wird die Liste der Ermächtigungsvorschriften für die Durchführung von Maßnahmen der Telekommunikationsüberwachung auf das Landesrecht und damit auf präventivpolizeiliche Aufgaben ausgedehnt. Dies trägt einer zunehmenden Tendenz zahlreicher Landesgesetzgeber Rechnung, dieses Ermittlungsinstrument auch im Bereich der polizeilichen Gefahrenabwehr zur Verfügung zu stellen. Diese stetige Ausdehnung der Anwendungsfälle der TK-Überwachung ist nicht nur wegen der damit stetig steigenden Belastung der TK-Unternehmen, sondern vor allem auch unter den Aspekten des Datenschutzes und des Vertrauens der Kunden in eine sichere und vertrauensvolle Telekommunikation sehr kritisch zu sehen. Dessen ungeachtet ist es grundsätzlich der richtige Ansatz, die Frage der Umsetzung solcher Überwachungsbefugnisse einheitlich in der TKÜV zu regeln, um die Unternehmen nicht noch mit einer Vielzahl von Verfahrensvorschriften zu konfrontieren.

- Allerdings müssten die Unternehmen nach der jetzt vorgesehenen Regel doch zumindest beständig neben den zahlreichen Bundesregelungen zur TK-Überwachung auch den jeweils aktuellen Stand von sechzehn Landesregelungen verfolgen, um zu prüfen, ob Überwachungsbefugnisse überhaupt und, falls ja, in welchem Umfang sie bestehen. Gerade mit Blick auf die rege Regelungstätigkeit der Landesgesetzgeber sollte bei der Regulierungsbehörde eine zentrale Sammlung geltender einschlägiger Vorschriften geschaffen werden, auf die die Unternehmen zu ihrer Information zurückgreifen könnten.
- § 1 Nr. 7 TKÜV-E spricht in Anlehnung an § 110 Abs. 6 TKG von „Netzabschlusspunkten“. In der Folge greift die TKÜV diesen Begriff weder auf, noch findet er sich unter den Begriffsbestimmungen des TKG oder der TKÜV. Es ist vielmehr von „Aufzeichnungsanschlüssen“ die Rede (vgl. § 24 TKÜV-E). Diese begriffliche Inkonsistenz erschwert das Verständnis vom Inhalt der beabsichtigten Regelungen erheblich.

§ 2: Begriffsbestimmungen

- In § 2 Nr. 4 wäre eine bessere Spezifizierung der Merkmale hilfreich, aufgrund derer auf eine „tatsächliche Kontrolle über die Funktion der Telekommunikationsanlage“ geschlossen werden soll. Auf diese Weise könnte schon frühzeitig Klarheit über den Kreis der Verpflichteten geschaffen werden.
- Unter Berücksichtigung der Begriffsbestimmungen im § 3 TKG kann die Definition des Begriffs „Endgerät“ im § 2 Nr. 5 einfacher und klarer gefasst werden. Statt umständlich auf „Teilnehmer“ nach § 3 Nr. 20 TKG und „Endnutzer“ i.S.d. § 3 Nr. 8 TKG abzustellen, genügt ein Bezug auf den allgemeineren Begriff des „Nutzers“ gemäß § 3 Nr. 14 TKG. Auch in dieser kürzeren Fassung bleibt die Definition vollständig und lückenlos.
- Nicht ausreichend definiert erscheint aus Sicht des BITKOM der zentrale Begriff der zu überwachenden „Kennung“ in § 2 Nr. 16 a). Da es sich um einen technischen Begriff handelt, sollte seine präzise Beschreibung am besten auch technisch sein. Eine denkbare Formulierung wäre etwa:

„Auf einen Nutzer bezogener Parameter, der für die technische Abwicklung der sowohl für den Nutzer bestimmten als auch von ihm ausgehenden Telekommunikation benutzt wird.“

Schließlich sollte im Zusammenhang mit der Definition der Kennung eindeutig klargestellt werden, dass im Mobilfunk nur MSISDN und IMSI, nicht aber die Gerätenummer (IMEI) Kennungen sind, die einen Anschluss bezeichnen. Sollte diese Klarstellung nicht im Rahmen der Definition möglich sein (wobei nach unserer Auffassung der in der vorgeschlagenen Definition geforderte Personenbezug fehlt, da die IMEI allein einem Gerät zugewiesen ist), wäre eine entsprechende ergänzende gesetzliche Regelung vorzunehmen.

§ 3: Kreis der Verpflichteten / Streichung des bisherigen § 4

- § 3 Abs. 2 Satz 3 sieht eine klare Erweiterung des Verpflichtetenkreises vor, indem nun auch Betreiber von Netzknoten, die der Zusammenschaltung mit ausländischen Telekommunikationsnetzen dienen, erfasst werden sollen. Die äußerst knappe hierfür gegebene Begründung erscheint nicht ausreichend, um diese erneute Ausdehnung der TK-Überwachung und der damit verbundenen schwerwiegenden Belastungen der Unternehmen zu rechtfertigen.

Problematisch ist hierbei vor allem der damit entstehende Auslandsbezug der TKÜV. Es bestand bislang Konsens, dass die deutschen Vorschriften zur Überwachung und Aufzeichnung der Telekommunikation nur für das Inland gelten und dass für die Überwachung der Telekommunikation von Personen, die sich im Ausland befinden, die einschlägigen Verfahren der internationalen Rechtshilfe anzuwenden sind. Es ist aus Sicht des BITKOM kein Grund erkennbar, von diesem Prinzip abzuweichen. Vor diesem Hintergrund ist auch die geplante ersatzlose Streichung des bisherigen § 4, der die Grenzen des Anwendungsbereichs bestimmt hatte, nicht hinnehmbar. Auch die neue TKÜV sollte eindeutig definieren, in welchen Konstellationen die Telekommunikation mit einem Teilnehmer im Ausland abgehört werden darf bzw. muss, in welchen Fällen dies nicht zulässig ist und insbesondere welche technischen und organisatorischen Vorkehrungen hierfür zu treffen sind.

Die geplante Erstreckung der TKÜV auf Auslandsköpfe berücksichtigt zudem nicht die vielfältigen technischen Szenarien einer Versorgung mit TK-Dienstleistungen. So ist im Mobilfunk eine „telekommunikationstechnische Versorgung eines Nutzers in einem Staat A durch Funk- und Vermittlungstechnik denkbar, die in einem anderen Staat B betrieben wird. Es sollte daher gerade für den Mobilfunk genügen, die in einem eigenen in Deutschland betriebenen vermittlungstechnischen System ankommenden oder dort aufgebauten abgehenden Gespräche bzw. Datenverbindungen überwachen zu können.

- Die im § 3 Abs. 3 Nr. 5 statuierte Ausnahme für Anlagen, an die „nicht mehr als 1000 Teilnehmer angeschlossen sind“ ist in vielen Fällen nicht verifizierbar. Die Zahl der Anschlüsse lässt sich nicht durchgängig bestimmten Anlagen zuordnen. Die Regelung zielt darauf ab, Anlagen mit geringer Leistung vom Anwendungsbereich der TKÜV auszuklammern. Da jedoch die tatsächliche Teilnehmerzahl oft nicht ermittelbar ist, sollte auf die potentielle Leistungsfähigkeit der Anlagen abgestellt werden. Entsprechend bietet es sich an, auf ihre technische Dimensionierung zu verweisen. Es könnte daher formuliert werden:

„5. die von nicht mehr als 1000 Nutzern gleichzeitig genutzt werden kann.“

§ 5: Grundsätze

- § 5 Abs. 1 Satz 2 sieht die neue Auflage vor, die Überwachung eines Anschlusses, dem „weitere Kennungen unmittelbar zugeordnet“ sind, auch auf diese Kennungen zu erweitern. Hierdurch wird nicht nur der Umfang der TK-Überwachung erneut ausgeweitet, es

werden auch den betroffenen Unternehmen Entscheidungen und Ermittlungsarbeiten auferlegt, die eigentlich in den Aufgabenbereich der Ermittlungsbehörden fallen. In der Praxis lässt sich schon gar nicht immer zweifelsfrei feststellen, wann der von der Norm beschriebene Fall vorliegt. Dies gilt etwa bei E-Mail-Adressen mit Alias-Namen oder Produkten im Mobilfunk wie Twin- bzw. Kombi-Karten. Um die absehbaren Schwierigkeiten von vornherein zu vermeiden, ist zwingend daran festzuhalten, dass die der Überwachungsmaßnahme zugrunde liegende Anordnung alle zu überwachenden Kennungen abschließend nennt.

- Der neue Satz 3 im § 5 Abs. 4 sollte gestrichen werden. Zum einen ist die darin enthaltene Auflage unerfüllbar, da „unerwartete Einflüsse“ auf die Verschleierung schon ihrer Natur nach nicht vorhersehbar und damit auch nicht durch irgendwelche Vorkehrungen zu unterbinden sind. Zum anderen stellt aber selbst die hierzu gegebene Begründung unter Punkt 2.5. der Einleitung fest, dass hinsichtlich der Verschleierung keine rechtssystematischen Lücken bestünden. Tatsächlich genügen die – auch allein erfüllbaren – Vorgaben der Sätze 1 und 2 zur Regelung völlig aus.

§ 6: Grundlegende Anforderungen an die technischen Einrichtungen

- § 6 Abs. 3 droht durch die Neufassung eine wesentlich größere Tragweite zu erhalten. Bislang muss der Verpflichtete seine Überwachungseinrichtung so gestalten, dass die Überwachung der auf einer Kennung basierenden Telekommunikation ermöglicht wird, indem Bezug genommen wurde auf Kennungen, die „für die technische Abwicklung der Telekommunikation“ benutzt werden. Entsprechend der gesetzlichen Vorgaben wurde mit der Kennung die zu überwachende Telekommunikation bestimmt. Die Fassung des Entwurfs geht jedoch darüber hinaus und spricht auch von Kennungen, die „bei“ (d.h. gelegentlich) der zu überwachenden Telekommunikation benutzt werden, ohne dass die Telekommunikation zwangsläufig auf der Kennung beruht. Es besteht die Befürchtung, dass sich aus dieser Umformulierung eine deutliche Verschärfung der an die Überwachungseinrichtung zu stellenden Anforderungen ergibt. Diese Verschärfung ist unverhältnismäßig, weil für die Gewährleistung der Überwachungsmaßnahme nicht erforderlich. Soweit der Personenbezug der Kennung fehlt, ist die Anforderung zudem nicht durch § 100 b Abs. 1 StPO gedeckt. Von einer Abänderung der Formulierung des § 6 Abs. 3 sollte daher dringend abgesehen werden.
- Im Übrigen ist es für die Verpflichteten für die Gestaltung ihrer Überwachungseinrichtungen von essentieller Bedeutung, auf eine abschließende Liste der relevanten und zu beachtenden Kennungen zurückgreifen zu können. Um hier ein Mindestmaß an Rechtssicherheit zu erzielen, sollte diese Liste technikbezogen in der TR TKÜ verbindlich festgelegt werden.

§ 7: Bereitzustellende Daten

- Die Präzisierung des Begriffs „Anschluss“ hin zum „Telekommunikationsanschluss“ im § 7 Abs. 1 Nr. 4 ist nur scheinbar. Nach § 2 Nr. 9 ist der „Telekommunikationsanschluss“ lediglich eine technische Funktion der TK-Anlage und damit je TK-Anlage nur einmal vorhanden. Unter diesen Umständen kann es keine zeitweise oder feste Zuordnung der Kennung geben. Davon abgesehen liegt die Information über die fest zugeordnete Rufnummer dem Verpflichteten in diesen Fällen in der Regel nicht vor.
- Die in § 7 Abs. 1 Nr. 6 angesprochenen Angaben über die Störungsursachen liegen dem Verpflichteten in den Fällen der „für sie bestimmten“ Telekommunikation nicht vor. Daher bedarf es in Nr. 6 derselben Einschränkung wie sie in § 7 Abs. 1 Nr. 5 vorgenommen

wurde. Der Verpflichtete kann die Daten mithin nur bereitstellen, „soweit diese Angaben in dem Netzknoten vorhanden sind, in dem die Überwachungsmaßnahme umgesetzt wird“.

- Einer Korrektur bedarf auch die nächste Regelung zur Übermittlung von Angaben zum Standort eines Mobilfunkgerätes. Nach § 7 Abs. 1 Nr. 7 sind Angaben mit der Genauigkeit zu übermitteln, „die in dem das Mobilfunkgerät versorgenden Netz *an diesem Standort zur Verfügung* steht“. Diese Formulierung ist eine unvollkommene Umschreibung des entsprechenden Netzknotens, an dem die Überwachungsmaßnahme vorgenommen wird. Wir bitten daher, die technische Einrichtung im § 7 Abs. 1 Nr. 7 explizit zu benennen und die Regelung dahingehend abzuwandeln:

„[...] Angaben zum Standort des Mobilfunkgerätes, soweit diese Angaben in dem Netzknoten vorhanden sind, in dem die Überwachungsmaßnahme umgesetzt wird;“

Anderenfalls könnte die jetzige Formulierung dahingehend missverstanden werden, dass die Unternehmen womöglich verpflichtet wären, verschiedene in ihrem Netz vorhandene Informationen zusammenzutragen, um eine möglichst genaue Standortangabe zu ermöglichen. Dies kann wegen des enormen damit verbundenen Aufwands jedoch schon aus Verhältnismäßigkeitserwägungen nicht von den Unternehmen verlangt werden. Darüber hinaus erscheint eine solche Informationszusammenführung im Einzelfall auch technisch nicht realisierbar.

§ 8: Übergabepunkt

- Die vorgesehene Ergänzung im § 8 Abs. 2 S. 1 Nr. 3 3. Halbsatz ist nicht sachgerecht. Es nicht nachvollziehbar, warum eine Kopie der Telekommunikation im Internet auf IP-Basis bereitgestellt werden muss und nicht in dem Format bereitgestellt werden darf, in dem sie den Verpflichteten vorliegt. Diese erschwerende Differenzierung ist nicht hinnehmbar, da andere Möglichkeiten (bspw. ATM) von vorneherein ausgeschlossen werden. Technische Innovation kann dann nur um den Preis einer Rückwandlung auf IP erfolgen, die aber kostenmäßig zu Lasten des Verpflichteten geht.
- Ein fallweises Dispensrecht der Regulierungsbehörde gemäß § 8 Abs. 2 Satz 2, das befristete Ausnahmen vom IP-gestalteten Übergabepunkt gestattet, schafft hier keine ausreichende Abhilfe. Die Entscheidungsbefugnis der Regulierungsbehörde ist völlig kontrollos und ist nicht geeignet, den Betroffenen ein Mindestmaß an Rechtssicherheit zu geben. Insbesondere bedarf es, damit der Dispens gegenüber späteren Veränderungen rechtlicher Vorgaben nicht wirkungslos bleibt, einer Ergänzung, dass die Adressaten einer ausgesprochenen Duldung, gegenüber nachfolgenden Änderungen in der TKÜV bzw. der dazugehörigen Technischen Richtlinie Bestandschutz genießen. Weiterhin fällt dieser technische Detailpunkt rein systematisch in den Regelungsrahmen der Technischen Richtlinie und nicht in den der Verordnung.
- Die geplante Neufassung in § 8 Abs. 3 ist in ihrer beabsichtigten Wirkung nicht eindeutig; dies gilt insbesondere für das Tatbestandsmerkmal „verändern lässt“. Hier ist darauf hinzuweisen, dass der Verpflichtete grundsätzlich nicht für die Leistungsmerkmale der in seinem Telekommunikationsnetz genutzten Endgeräte verantwortlich. Hierhin fallen beispielsweise Mobiltelefone mit der üblichen Funktionalität zur Verschlüsselung auf der Luftschnittstelle, explizite Kryptomobiletelefone oder Kryptosoftware für mobile Endgeräte. Daher müsste deutlicher eingegrenzt werden, unter welchen Voraussetzungen der Verpflichtete welche Anforderungen zur Bereitstellung der „ursprünglichen Telekommunikation“ zu erfüllen hat.

- Daneben bedarf auch die Regulierung zum Einsatz von Komprimierungsverfahren in § 8 Abs. 3 Satz 2 einer Einschränkung. Dies sollte schon immer dann bei der Bereitstellung der Überwachungskopie zulässig sein, wenn der berechtigten Stelle in ihrem Backend eine Dekomprimierung möglich ist.

§ 11: Technische Richtlinie

- Das Anhörungsverfahren bei Arbeiten an der Technischen Richtlinie sollte neben Herstellern und Unternehmensverbänden auch die unmittelbar von den Regeln betroffenen Betreiber von Telekommunikationsnetzen direkt beteiligen. Dies gewährleistet die Einbringung des spezifischen Sachverstands und die Berücksichtigung spezieller Bedürfnisse auf Seiten der verpflichteten Betreiber. Zudem gebietet auch das Gleichbehandlungsgebot eine Gleichstellung mit den Anlagenherstellern.
- Im Rahmen des § 9 Abs. 1 ist darauf zu achten, dass zu detaillierte technische Vorgaben an die Kopieübermittlung, insbesondere an die Signaturregelungen nicht zu einer Bevorzugung des Produkts eines einzelnen Herstellers führen. Zur Vermeidung eines Herstellermonopols müssen sich etwaige Signaturregelungen in der Technischen Richtlinie auf Vorgaben zu Schlüsselstärken und anerkannte Schlüsselverfahren beschränken. Etwas anderes könnte nur dann gelten, wenn die entsprechenden Geräte vom Bund kostenfrei zur Verfügung gestellt werden und eine angemessene Aufwandsentschädigung für Schulung der Mitarbeiter und den Betrieb gewährt wird.
- § 110 Abs. 5 Satz 2 TKG respektiert den Umstand, dass Unternehmen, die richtlinienkonform gestaltete Einrichtungen bereits betreiben, bei späteren Änderungen oder Erweiterungen bestehender Vorgaben der Technischen Richtlinie zumindest für den Zeitraum von drei Jahren einen unbedingten Bestandsschutz genießen müssen. Daher ist auch in der TKÜV für Anlagen, für welche ein Nachweis nach § 19 TKÜV-E vorliegt, ungeachtet späterer Änderungen oder Erweiterungen bestehender Vorgaben der Technischen Richtlinie ein entsprechender Bestandsschutz vorzusehen. In Anlehnung an § 110 Abs. 5 Satz 1 muss darüber hinaus § 11 TKÜV den Verpflichteten auch für den Fall einen realistischen Umsetzungszeitraum einräumen, wenn in die Technische Richtlinie erstmalig neue Vorgaben aufgenommen werden. In dieser Konstellation sollte die Anpassung an neue Verpflichtungen beim nächsten Technikhub, frühestens jedoch innerhalb von 24 Monaten erfolgen.

§ 12: Entgegennahme der Anordnung

Im Rahmen der Verfahrensregeln in § 12 wurde die Chance versäumt, im Rahmen der Neuregelung für die Unternehmen einfachere und zugleich sichere Verfahrensvorgaben zu machen. Stattdessen werden den Unternehmen noch weitere Belastungen einseitig auferlegt, während die Anforderungen an die anordnenden Stellen – etwa hinsichtlich der Form der Anordnungen und ihrer Übermittlung – nicht verbessert werden.

- So enthält § 12 Abs. 2 des Entwurfs eine neue einseitige Belastung der verpflichteten Betreiber. Durch das Standardisieren der Übermittlung der Anordnungen per Telefax vorab und die zwingend vorgeschriebenen Rückrufe wird den Verpflichteten erheblicher weiterer Aufwand mit der Kontrolle der späteren ordnungsgemäßen Zustellung der Anordnung aufgebürdet. Die Verpflichteten haben keinen Einfluss auf das ordnungsgemäße Absenden der Anordnungen, sind aber für den ordnungsgemäßen Eingang verantwortlich und müssen bei dessen Ausblieben weitere Maßnahmen treffen. Unberücksichtigt bleibt, dass den berechtigten Stellen gerade im Zusammenhang mit staatsanwaltlichen Eilanordnungen häufig selbst lediglich eine Kopie der Anordnung vorliegt;

die Existenz einer ordnungsgemäßen Anordnung ist also schon bei den berechtigten Stellen zum Zeitpunkt der Anforderung der Schaltung nicht immer gewährleistet.

Die angestrebte höhere Missbrauchsprävention wäre besser zu erreichen, wenn endlich bei den Ländern zentrale Stellen für die Durchführung von TK-Überwachungen geschaffen würden, über die einheitlich alle Anordnungen verarbeitet werden. Damit würde eine überschaubare Zahl von Ansprechpartnern für die Unternehmen geschaffen, die gewährleisten würden, dass Missbräuche mit großer Sicherheit ausgeschlossen werden könnten. Zugleich würden durch die festen Wege und die größere Routine solcher Stellen die Bearbeitungskosten sowohl auf Seiten der Justizbehörden als auch der Unternehmen gesenkt.

Hinsichtlich der Anordnung einer zwingenden Rückfrage nach Faxerhalt ist schließlich anzumerken, dass die Wirksamkeit einer solchen Regelung überhaupt zweifelhaft ist. Denn die Rufnummern, an die im Überwachungsfall überhaupt die Telekommunikation ausgeleitet wird, sind alle in einer Closed-User-Group. Ein Missbrauch ist daher ohnehin nur dann möglich, wenn jemand auf Seiten der anerkannten Bedarfsträger aktiv würde. Dieses interne Missbrauchsrisiko kann aber durch einen Rückruf auch nicht beseitigt werden.

- Schon heute ist die Übermittlung der Überwachungsbeschlüsse per Fax gängige Praxis der Bedarfsträger. Hieraus ergeben sich unnötige Belastungen für die Unternehmen. Es sollte daher festgeschrieben werden, dass nur in Ausnahmefällen und bei Gefahr im Verzug der Übertragungsweg per Fax gewählt werden kann und sonst im Regelfall die rechtzeitige Versendung der Originalbeschlüsse erfolgen muss. So würde auch der Aufwand für den Verpflichteten minimiert werden können, durch Rückruf die Korrektheit der Faxbeschlüsse bestätigt zu bekommen.
- Soweit ein Faxversand erfolgt, wäre die Festlegung eines einheitlichen, für die berechtigten Stellen verbindlichen Faxformates mit Mindestanforderungen an die Lesbarkeit und korrekte äußere Form der Anordnungen in einer nachgeordneten Regelung überaus hilfreich. Dies wäre eine Vorstufe zu der künftig geplanten Übermittlung der Anordnung auf standardisiertem gesichertem elektronischem Weg. Insoweit ist übrigens zu begrüßen, dass bei Nutzung dieses Verfahrens auf einen Rückabruf und die Vorlage des Originals oder einer beglaubigten Abschrift der Anordnung verzichtet werden soll.
- Hinsichtlich der in § 12 Abs. 2 vorgesehenen Vereinbarung von Dienststellen zur Authentizitätsprüfung von per Fax übermittelten Anordnungen ist darauf hinzuweisen, dass solche Vereinbarungen bislang nicht bestehen. Dies würde bei Beibehaltung des strengen Rückfrageerfordernisses in der TKÜV-Neufassung in der Praxis dazu führen, dass nach deren Inkrafttreten keine Überwachungsmaßnahme mehr aufgrund eines per Telefax zugeleiteten Anordnungsschreibens eingeleitet werden dürfte, weil sich die Verpflichteten an keine Referenzstelle wenden könnten.
- § 12 Abs. 3 statuiert eine zusätzliche Pflicht zur jederzeitigen, jedenfalls aber unverzüglichen Auskunftserteilung auf Rückfragen zu laufenden Überwachungsmaßnahmen. Diese Verpflichtung der Unternehmen ist völlig unverhältnismäßig. Eine Klärung von Rückfragen kann zeit- und kostenaufwendig sein. Es ist nicht haltbar, diese weit reichende Pflicht im Rahmen einer Verordnung zur TK-Überwachung zu statuieren, zumal hierfür auch keine Entschädigung vorgesehen ist. Es ist daher dringend erforderlich, die Verpflichtung inhaltlich einzuschränken und die zeitliche Vorgabe zu streichen. Rückfragen sollten nur hinsichtlich Fragen zur Funktion einer realisierten oder zu realisierenden Überwachungsmaßnahme (d.h. insbesondere zu Störungen, die den Zweck der Maßnahme gefährden könnten) zulässig sein. Angesichts der möglichen Komplexität und

des benötigten Expertenwissens für eine Antwort sind auch fixe Zeitvorgaben (wie jetzt mit der 6-Stunden-Regel vorgesehen) völlig praxisfern und deshalb nicht akzeptabel.

§ 13: Entstörung und betriebsbedingte Unterbrechung

Die in § 13 Satz 5 vorgesehene Regelung bedarf aus Sicht des Mobilfunks gleich in zweierlei Hinsicht der Korrektur: Zum einen ist die Privilegierung des Satz 5 nicht nur auf Störungen der Überwachungseinrichtungen, sondern auch auf Unterbrechungen einer Maßnahme zu erstrecken, so dass eine Mitteilung immer nur auf Anfrage zu erfolgen hätte. Grund ist, dass im Mobilfunk aus technischen Gründen grundsätzlich unklar bleibt, auf welche konkrete Überwachungsmaßnahme sich eine betriebsbedingte Unterbrechung auswirken wird. Zum anderen sollte die Erleichterung nicht nur Störungen mit regional begrenzter Wirkung, sondern Störungen insgesamt betreffen. So ist etwa in Mobilfunknetzen der temporäre Ausfall des zentralen S-Record-Managers zwar ein überregionaler Störfall i.S.d. § 13. Es wäre jedoch offensichtlich unverhältnismäßig, diese Störungsart in allen Überwachungsfällen sämtlichen betroffenen berechtigten Stellen mitteilen zu müssen, weil diese Störung für den Erfolg der Überwachungsmaßnahme letztlich unschädlich ist, da nach dem Wiederherstellen der ordnungsgemäßen Funktion des Managers die Daten vollständig zugeführt werden können.

§ 14: Schutzanforderungen

Die neu vorgesehene Formulierung, dass „eine Übermittlung [der Überwachungskopie] an Nichtberechtigte technisch ausgeschlossen werden kann“, setzt zu hohe Anforderungen und ist daher unverhältnismäßig. Grundsätzlich kann und sollte für alle Schutzanforderungen ein einheitlicher Maßstab gelten. Jeweils ist ein Schutz durch angemessene Verfahren bzw. angemessene technische Maßnahmen sicherzustellen. Darüber hinausgehende Forderungen sind dagegen unverhältnismäßig.

§ 16: Protokollierung

- Die jetzt vorgesehene Fassung der Protokollpflicht in § 16 führt zu Kollisionen mit Vorgaben des Betriebsverfassungsgesetzes. Eine verhaltensbezogene Kontrolle sollte vermieden werden. Daher muss im Abs. 1 Satz 3 Nr. 5 genügen, wenn ein Merkmal zur *Erkennbarkeit* (statt *Erkennung*) der die Eingabe vornehmenden Person protokolliert wird.
- Die Vorgabe im § 16 Abs. 2 Nr. 3 ist unklar und widersprüchlich. Zum einen ist eine absolut nicht löschbare Datei technisch kaum vorstellbar. Stünde sie aber zur Verfügung, könnte ihre Überschreibung, die in Nr. 3 angesprochen wird, auch nicht vorgenommen werden.
- Des weiteren ist § 16 Abs. 2 Nr. 4 zu kategorisch gefasst: Die Auflage, dass ein nachweisfreier Zugriff auf Datenverarbeitungsanlagen oder auf Datenbestände nicht möglich sein darf, ist ebenso wie die überzogene Formulierung im § 14 mit vertretbaren Mitteln nicht erfüllbar und daher unverhältnismäßig; zum Phänomen nicht löschtbarer Dateien und ihrer Überschreibung vgl. Anmerkung zu § 16 Abs. 2 Nr. 3.

§ 17: Prüfung und Löschung der Protokolldaten, Vernichtung von Unterlagen

- Die in § 17 Abs. 1 S. 1 enthaltene Forderung, mindestens 20% der Protokolldaten zu überprüfen, stellt eine hohe Belastung der betroffenen Unternehmen ohne erkennbaren Nutzen dar. Die Verpflichtung ist daher unverhältnismäßig und wegen der immensen Be-

lastung unhaltbar. Bei der Bewertung der Notwendigkeit einer solchen Pflicht ist zu berücksichtigen, dass jeder Missbrauch der technischen Einrichtungen zur Realisierung von Überwachungsmaßnahmen strafbar ist und zudem unmittelbare arbeitsrechtliche Konsequenzen hätte. Auch würde eine ungerechtfertigte Beeinflussung einer angeordneten Maßnahme von der berechtigten Stelle sofort bemerkt, da sowohl über das Einrichten als auch das Abschalten einer Maßnahme diese zeitnah durch entsprechende S-Records informiert werden muss. Es muss daher in die Verantwortung der Unternehmen gestellt bleiben, wie sie das ordnungsgemäße Anwenden der entsprechenden Technik und die anordnungsgerechte Durchführung der Maßnahmen sicherstellen. Eine Prüfungspflicht kann daher jedenfalls nur in Fällen bestehen, in denen es einen konkreten Anlass für eine Nachprüfung gibt. Neben dieser mehrfachen innerbetrieblichen Sicherung ist eine zusätzliche stichprobenartige Kontrolle durch die Regulierungsbehörde nach § 17 Abs. 4 völlig ausreichend. Hinzuweisen ist in diesem Zusammenhang auch darauf, dass selbst der Bundesbeauftragte für den Datenschutz bei der Überprüfung des § 90 TKG alter Fassung keine relevante Stichprobenprüfung macht (vgl. BfD-Jahresbericht 2002). Es ist insofern nicht einsichtig, wieso dies hier nun den privaten Unternehmen aufgebürdet werden soll.

- Die Befugnis der Regulierungsbehörde, gemäß § 17 Abs. 4 Einsicht in die Protokolle zu nehmen, steht in einem Spannungsverhältnis zur Verschwiegenheitspflicht gemäß § 15.

§ 19: Nachweis

- Die Vorschrift muss beachten, dass die üblichen Realisierungszeiträume für die Umsetzung der technischen Vorgaben rund 36 Monate betragen. Dies hat auch das TKG selbst in der Änderung des § 110 Abs. 5 TKG berücksichtigt. Daher kann Grundlage eines Nachweisverfahrens nicht die jeweilige aktuelle Fassung der TKÜV und der Technischen Richtlinie sein, sondern nur eine entsprechend zurückliegende Version sein. Eine dahingehende Regelung im Abs. 1, 2 und 6 ist wirtschaftlich zwingend notwendig und mit den Vorgaben des § 110 Abs. 5 TKG vereinbar, der abweichende Regelungen in der TKÜV und der Technischen Richtlinie ausdrücklich zulässt.
- In § 19 Abs. 4 wäre es wünschenswert, wenn genauer bestimmt würde, was eine „gesetzte angemessene Frist“ ist. Anderenfalls drohen hier erhebliche Verzögerungen des Nachweisverfahrens, die zu Rechtsunsicherheiten für die betroffenen Unternehmen führen.
- Im Rahmen der Mitwirkungsverpflichtung nach § 19 Abs. 5 Nr. 3 muss klar gestellt werden, dass die Verpflichteten der Regulierungsbehörde in keinem Fall Backends der berechtigten Stellen zu stellen haben.
- Entweder in einem gesonderten Absatz von § 19 oder ggf. auch in der Übergangsregelung in § 30) sollte noch einmal klargestellt werden, dass das Nachweisverfahren nicht für diejenigen Verpflichteten gilt, die zum Zeitpunkt des Inkrafttretens der TKÜV 2004 über eine Genehmigung nach § 88 Abs. 2 Satz 1 TKG 1996 i.V.m. § 18 TKÜV 2002 verfügen bzw. dass das Nachweisverfahren dann nur eingreift, wenn die TKÜV 2004 bzw. die zukünftige TR TKÜV neue Anforderungen enthalten oder wenn der Verpflichtete Änderungen seiner Überwachungsanlagen vornimmt oder neue Dienste einführt. Dies lässt sich zwar schon aus dem Wortlaut von § 110 Abs. 1 des neuen TKG schließen, weil die Anlage schon in Betrieb ist; es ist aber wünschenswert, diesen Punkt noch einmal ausdrücklich klarzustellen. Keinesfalls wäre es hinnehmbar, wenn schließlich doch jeder Anlagenbetreiber jetzt das Nachweisverfahren durchlaufen müsste.

§ 19 Abs. 6, § 21, § 22 Abs. 1: Duldungen durch die Regulierungsbehörde

Es ist erforderlich, dass in der TKÜV in den §§ 19 Abs. 6, 21 und 22 Abs. 1 klargestellt wird, dass bei von der Regulierungsbehörde erteilten Duldungen ein Bestandsschutz für die Unternehmen gegenüber nachfolgenden Änderungen der TKÜV und der Technischen Richtlinie besteht.

§ 23: Funktionsprüfungen der Überwachungseinrichtungen oder der Aufzeichnungs- und Auswertungseinrichtungen der berechtigten Stellen

- Die Neufassung des § 23 Abs. 1 erhöht bürokratische Vorgaben für die Unternehmen, ohne dass ein spezieller Nutzen erkennbar wird. So müssten künftig Netzbetreiber sämtliche Vorbeugemaßnahmen zur Vermeidung von Störungen (z.B. alle Prüfungen der Interceptionfunktion bei Arbeiten an der MSC) anmelden. Dieser unverhältnismäßig hohe Verwaltungsaufwand ist insbesondere im Hinblick auf die bereits vorgesehene Absicherung durch §§ 16 und 17 TKÜV-E nicht gerechtfertigt. Stattdessen sollte es nach § 23 für den Netzbetreiber zulässig sein, aufgrund einer unbefristeten Bestätigung durch die Regulierungsbehörde Testanschlüsse zu verwenden, die von Dritten nicht genutzt werden dürfen.
- Überdies sollte die Vorschrift stärker berücksichtigen, dass neue Überwachungstechnik negative Auswirkungen auf die Telekommunikationsnetze haben kann und vor ihrem Einsatz auf ihre Netzverträglichkeit geprüft werden muss. Aus diesem Grund muss § 23 Abs. 2 das Recht der Netzbetreiber vorsehen, die Überwachungstechnik der berechtigten Stellen vorab zu testen.

§ 31: Inkrafttreten, Außerkrafttreten

Die Übergangsregelung im § 30 Abs. 1 Satz 1 enthält eine Umsetzungsfrist lediglich bezogen auf Anforderungen aus der früheren Version der TKÜV in der Fassung vom 22. Januar 2002. Daneben bedarf es aber einer entsprechend prolongierten Umsetzungsfrist auch für die neuen Vorgaben, die sich aus der jetzt zu erlassenden Neufassung der TKÜV ergeben. Soweit hier technische bzw. organisatorische Änderungen bei den betroffenen Unternehmen erforderlich sind, ist ein Bestandsschutz für genehmigte Anlagen von mindestens 36 bzw. eine Umsetzungsfrist bis zum nächsten Technikhub, frühestens jedoch innerhalb von 24 Monaten ab Inkrafttreten der Neufassung realistisch.

Berlin, den 30. August 2004

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., BITKOM, vertritt 1.300 Unternehmen mit etwa 120 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Produzenten von Endgeräten und Infrastruktursystemen sowie Anbieter von Software, Dienstleistungen, neuen Medien und Content. Der BITKOM setzt sich insbesondere für bessere ordnungsrechtliche Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.