

zum Gesetzentwurf zur Änderung des Bayerischen Polizeiaufgabengesetzes (BayPAG-E) vom 6. Juli 2004

Der Bayerische Ministerrat hat in seiner Sitzung vom 6. Juli 2004 einem Entwurf zur Änderung des Bayerischen Polizeiaufgabengesetzes zugestimmt, indem weitreichende Regelungen u.a. im Bereich der Telekommunikationsüberwachung zum Zwecke der präventiven Gefahrenabwehr sowie weitere Zugriffsrechte auf Kommunikationsdaten enthalten sind.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., BITKOM, sieht die vorgeschlagenen Änderungen mit erheblicher Skepsis. Die vorgesehene deutliche Ausweitung der Telekommunikationsüberwachung, bislang ein Mittel der repressiven Strafverfolgung, durch die Anwendung als Mittel der präventiven Gefahrenabwehr führt zu einer weiteren Aushöhlung des grundrechtlich geschützten Fernmeldegeheimnisses. Dieses Grundrecht auf ungestörte und unüberwachte Kommunikation ist ein zentrales Element für die freie Persönlichkeitsentfaltung der Menschen; seine Gewährleistung ist zentrales Element, um das Vertrauen der Nutzer in die Verlässlichkeit elektronischer Kommunikationsmittel zu wahren. Dieses Vertrauen ist gerade dann unerlässlich, wenn der Bürger ein öffentliches Telekommunikationsnetz nutzt. Aus diesem Grund haben auch die Anbieter elektronischer Kommunikationsdienste ein großes Interesse an der Aufrechterhaltung eines hohen Schutzniveaus in diesem Bereich.

Betroffen sind von den geplanten neuen Auflagen aber nicht nur die Freiheitsgrundrechte der Nutzer, sondern auch die Wirtschaftsgrundrechte der verpflichteten Telekommunikationsunternehmen. Ihnen werden durch die geplanten Mitwirkungspflichten erhebliche wirtschaftliche Belastungen zugemutet, die allein im staatlichen Interesse stehen. Die Verhältnismäßigkeitsprüfung bei der Einführung neuer Pflichten muss daher neben dem Fernmeldegeheimnis der Nutzer stets auch die erheblichen Belastungen der verpflichteten Unternehmen berücksichtigen. Vor diesem Hintergrund steht die Verfassungsgemäßheit der jetzt angedachten Verpflichtungen zumindest teilweise in Frage.

Dies gilt insbesondere mit Blick darauf, dass das Gesetz keine Entschädigungsregeln für die Inanspruchnahme der privaten Unternehmen für rein staatliche Zwecke vorsieht. Diese müssen nicht nur erhebliche Investitionskosten für die Ermöglichung der TK-Überwachung aufbringen, sondern haben auch hohe Lasten durch die Ausführung der einzelnen Anordnungen und die Bearbeitung von Datenanfragen zu tragen. Es ist für die Verhältnismäßigkeit der neuen Pflichten daher von entscheidender Bedeutung, dass parallel zu den Eingriffsbefugnissen für die Sicherheitsbehörden auch Entschädigungsregeln geschaffen werden, die die Kosten der Unternehmen aufwandsgerecht erstatten. Vorzugsweise sollte dies im Polizeiaufgabengesetz selbst erfolgen bzw. es sollten entsprechende Verordnungsermächtigungen geschaffen werden. Alternativ ist auch eine teilweise Delegation der Regelungsbefugnis auf den Bund denkbar, der durch das neue Telekommunikationsgesetz bereits verpflichtet wurde, eine Verordnung mit Regeln zur aufwandsgerechten Erstattung im Rahmen der Pflichten zur TK-Überwachung zu schaffen.

Im Einzelnen gilt zu den geplanten Regelungen das Folgende:

**Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.**
Postadresse: Postfach 640144, 10047 Berlin
Besucher: Albrechtstr. 10, 10117 Berlin
Tel.: 030/27576-0, Fax: -400
E-Mail: bitkom@bitkom.org
Internet: www.bitkom.org

Präsident:
Willi Berchtold

Geschäftsführung:
Dr. Bernhard Rohleder (Vors.)
Dr. Peter Broß

Ansprechpartner:
RA Wolf Osthaus
Bereichsleiter
Telekommunikations- und Medienpolitik
Postfach 640144, 10047 Berlin
Telefon 030/27576-221, Fax -222
E-Mail: w.osthaus@bitkom.org

Zu Art. 30 Abs. 5

Die vorgelegte Ausweitung des Straftatenkatalogs, der einen Eingriff in die grundgesetzlich geschützte informationelle Selbstbestimmung eines Nutzers von TK-Einrichtungen gestatten soll, lässt jedes Augenmaß vermissen und geht über den verfassungsrechtlich zulässigen Rahmen weit hinaus. Bei der notwendigen Abwägung zwischen der schwere des Eingriffs in Grundrechtspositionen Einzelner einerseits und dem legitimen staatlichen Interesse an wirksamer Kriminalitätsbekämpfung andererseits zeigt § 100 a StPO, dass eine Überwachung der Telekommunikation nur bei Vorliegen weniger, besonders schwerwiegender Straftatbestände noch verhältnismäßig erscheint. Demgegenüber enthält das BayPAG-E eine dreifache Ausweitung.

- Zum einen sieht Art. 30 Abs. 5, insbesondere in Satz 2, eine beträchtliche Erweiterung des Straftatenkatalogs vor.
- Zum anderen soll gemäß Art. 34 a Abs. 1 BayPAG-E präventiv schon die Annahme, jemand sei *geneigt* eine Katalogstraftat zu begehen, jemand kommuniziere mit *geneigten* Straftätern oder überlasse ihnen eine Kommunikationseinrichtung einen Grundrechtseingriff rechtfertigen.
- Überdies soll nach Art. 34 a Abs. 1 Satz 2 des Entwurfs eine technische Überwachung bereits dann durchgeführt werden dürfen, „wenn die Erfüllung einer polizeilichen Aufgabe auf andere Weise *gefährdet* oder erheblich erschwert wäre.“ Damit wird die Schwere des Eingriffs durch technische Überwachung (der Entwurf spricht hier verharmlosend von „Datenerhebung“) bagatellisiert. Der Charakter dieses technischen Mittels als ultima ratio des zur Verfügung stehenden Maßnahmenspektrums wird in unzulässiger Weise abgeschafft und die Schwelle des § 100 a StPO, der die technische Überwachung nur gestattet, „wenn die Erforschung des Sachverhalts auf andere Weise *aussichtslos* oder erheblich erschwert wäre“, spürbar herabgesetzt.

Diese kumulierte Absenkung der Eingriffsschwelle missachtet den Verfassungsrang des zu wahrenen Rechtsguts und ordnet die informationelle Selbstbestimmung Einzelner scheinbaren Bedürfnissen nach präventiver Verbrechensbekämpfung gänzlich unter.

Des weiteren führte die doppelte Ausweitung polizeilicher Eingriffsbefugnisse zu einem weiteren Anstieg der überaus zeit- und kostenintensiven Überwachungsmaßnahmen, Auskunftserteilungen und Zielwalsuchen. Die gemäß Art. 34 b BayPAG-E zur Mitwirkung verpflichteten Telekommunikationsunternehmen wären einer weiteren Zunahme ihrer Belastung durch die entschädigungslose Indienstnahme für staatliche Zwecke ausgesetzt. Dies liefe auf die Verschärfung eines bereits heute verfassungswidrigen Zustands hinaus. Bezeichnenderweise übergeht der Entwurf diesen Punkt völlig. Die Überlegungen zu möglichen Kosten des BayPAG-E bleiben eindimensional und betrachten lediglich mögliche Auswirkungen auf die öffentlichen Haushalte.

In dieser Form ist die Regelung des § Art. 30 Abs. 5 BayPAG-E unverhältnismäßig.

Zu Art. 34a Abs. 1

Der vorgelegte Gesetzesentwurf zur Änderung des bayerischen Polizeiaufgabengesetzes leidet, soweit er Regelungen zur präventiven TK-Überwachung enthält, am grundlegenden Mangel der Gesetzgebungskompetenz des Landes. Dies ergibt sich aus der Anwendung der vom BVerfG formulierten Maßstäben zur Ermittlung der konkurrierenden Gesetzgebungsbefugnis des Bundes für das Strafrecht nach Art. 74 Nr. 1 GG. In seinem Beschluss zur nachträglichen Sicherheitsverwahrung führt das Gericht aus:

„Die Gesamtheit der Normen, die der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung dienen, bilden keinen selbständigen Sachbereich im Sinne der grundgesetzlichen Verteilung der Gesetzgebungszuständigkeit zwischen Bund und Ländern. Normen, die der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung in einem bestimmten Sachbereich dienen, sind für die Abgrenzung der Gesetzgebungskompetenz vielmehr dem Sachbereich zuzurechnen, zu dem sie in einem notwendigen Zusammenhang stehen. Erscheint eine Regelung als Annex zu einem Sachgebiet, auf dem der Bund tätig ist, umfasst die Zuständigkeit zur Gesetzgebung auch präventive Regelungen in diesem Sachbereich.“ - BVerfG, 2 BvR 834/02 vom 10.2.2004, Absatz Nr. 96.

Übertragen auf die Materie präventiver Telekommunikationsüberwachung ergibt sich hiernach, dass eine Gesetzgebungskompetenz des Landes Bayern nicht gegeben ist. Die Telekommunikationsüberwachung ist vom Bund seit langem in den Bestimmungen der §§ 110 a, b StPO sowie im § 110 TKG und der dazugehörigen TKÜV umfassend geregelt. Wie sich etwa aus dem geplanten Art. 34 a Abs. 1 Satz 1 Nr. 1 und 2 a BayPAG-E ergibt, zielt die landesrechtliche Regelung auf die Gefahrenabwehr bzw. auf Personen, die eine schwerwiegende Straftat i.S.d. Art. 30 Abs. 5 BayPAG-E mutmaßlich begehen wollen. Auch der einleitende Problemaufriss zum vorliegenden Gesetzesentwurf spricht ausdrücklich davon, das im Rahmen der Strafverfolgung eingesetzte Mittel der technischen Überwachung der Telekommunikation in den Bereich der präventiven Kriminalitätsbekämpfung vorzuverlagern. Die beabsichtigten Regelungen stehen daher mit einem Sachbereich in einem notwendigen Zusammenhang, auf dem der Bund bereits tätig ist. Nach den vom BVerfG erarbeiteten Maßstäben ist die präventive Telekommunikationsüberwachung als Annex zu bereits bestehenden bundesrechtlichen Normierungen zu begreifen und eine landesrechtliche Gesetzgebungskompetenz daher zu verneinen.

Darüber hinaus erscheint die Einführung einer präventiven Telekommunikationsüberwachung nicht erforderlich. Zwar wird seitens der Polizeibehörden regelmäßig vorgetragen, das den Strafverfolgungsbehörden zur Verfügung stehende Instrumentarium dürfe der Polizei für die Aufgabe der Gefahrenabwehr nicht vorenthalten werden. Vor dem Hintergrund bestehender Regelungen ist diese Forderung jedoch nicht nachvollziehbar.

Schon der weit gefasste § 100 a StPO enthält zahlreiche Tatbestandsmerkmale, die unmittelbar oder auch als bloße Beweisanzeichen den Verdacht einer Katalogstraftat oder strafbaren Vorbereitungstat begründen und das Eingreifen von Strafverfolgungsbehörden rechtfertigen können. Eine noch weiter gehende Vorverlagerung dürfte daran scheitern, dass dann kaum noch eine konkrete Gefahr bejaht werden kann, die Eingriffsvoraussetzung wäre.

Art. 34 a Abs. 1 Satz 1 Nr. 2 enthält somit eine bedenkliche Aufweichung des klassischen Gefahrenbegriffs, indem nicht reale Geschehensabläufe, sondern bloße Vermutungen zum Anknüpfungspunkt für das präventive polizeiliche Handeln gewählt werden. Entscheidend ist danach nämlich die Annahme, ob eine Person eine Straftat begehen will. Dies zeigt aber, dass das primäre Ziel der Ausweitung des polizeilichen Instrumentariums zur Gefahrenabwehr nicht die Abwehr der Gefahr oder ein Gefahrenforschungseingriff, sondern die allgemeine Ermittlung ist, ob überhaupt eine Gefahrenlage gegeben ist. Damit wird im Ergebnis nicht mehr Gefahrenabwehr, sondern Risikosteuerung betrieben!

Zu Art. 34a Abs. 2

Die Sätze 2-4 regeln den Umgang mit Daten Dritter, die gelegentlich der Überwachungsmaßnahme erhoben wurden. Statt aber ihre unbedingte Löschung anzuordnen, gestatten Satz 3 und Satz 4 ihre weitere Verwendung. Damit werden Daten von Personen, die in

der der Überwachung zugrunde liegenden Anordnung nicht benannt sind, wie rechtmäßig gewonnene Informationen behandelt. Der Überwachung ohne richterliche Anordnung werden damit Tür und Tor geöffnet.

Zu Art. 34a Abs. 2 und Abs. 3 Satz 1 Nr. 2

Die Entwurfsverfasser möchten den Einsatz sog. IMSI-Catcher erlauben, um „den Standort eines [...] mitgeführten Mobilfunkgerätes zu ermitteln“. Auf Seite 27 unten der Begründung zum Gesetzesentwurf geben sie ihre Annahme zum Ausdruck, der IMSI-Catcher sei ein „Ortungsggerät“. Dies suggeriert, der IMSI-Catcher zeige dem Anwender schnell und zuverlässig den Aufenthaltsort des Nutzers eines Mobilfunkgerätes an. Es verhält sich jedoch anders. Die technischen Ortungsmöglichkeiten, die ein IMSI-Catcher bieten kann, sind weit weniger nützlich, als es die Verfasser irrtümlich annehmen, und beinhalten darüber hinaus ein beträchtliches Schadenspotential:

Durch den Einsatz der angesprochenen Technik kann lediglich verifiziert werden, ob sich das Mobilfunkendgerät der gesuchten Person im Sendebereich des IMSI-Catchers befindet oder nicht, vorausgesetzt, Rufnummer oder Endgeräteerkennung sowie benutztes Mobilfunknetz sind bekannt. Die Größe des Sendebereiches hängt von der eingesetzten Sendeleistung des IMSI-Catchers ab. Bei hoher Leistung ergibt sich ein großer Sendebereich, die Chance, dass sich das gesuchte Mobilfunkendgerät innerhalb des Sendebereiches aufhält, steigt, aber die Aussagekraft ist offensichtlich gering, wenn der Sendebereich viele Quadratkilometer abdeckt. Zudem steigt die Anzahl der regulären Kunden im Sendebereich bei hoher Leistung erst recht, und die Telekommunikation aller dieser Kunden wird während des gesamten Einsatzzeitraumes des IMSI-Catchers gestört oder unterbunden. Bei geringer Leistung ist der Sendebereich entsprechend kleiner, die Störungen werden kleiner, aber die Chance auf positive Verifikation sinkt. Sollte die Polizei ohnehin wissen, dass die gesuchte Person nur wenige zehn oder hundert Meter vom eigenen Standort entfernt ist, so braucht sie keinen IMSI-Catcher mehr, sondern sie kann die gesuchte Person auch direkt aufgreifen. Liegen für das Verbleiben der gesuchten Person aber keine Anhaltspunkte vor, könnte ihr Aufenthaltsort mittels eines IMSI-Catchers nur ermittelt werden, indem das betreffende Mobilfunknetz höchst aufwendig flächendeckend systematisch – und unter Inkaufnahme entsprechend vieler Störungen der Telekommunikation - abgesucht wird. Und selbst dann erhielte man ein valides Ergebnis nur, wenn die gesuchte Person in ihrer Funkzelle verbleibt, d.h. ihren Standort während der Suchdauer nicht verändert – eine im *Mobilfunk* nicht nahe liegende Annahme. Mit einem von den Verfassern so genannten Ortungsggerät hat dies jedoch nur wenig zu tun. Zudem wirft jeglicher Einsatz eines IMSI-Catchers beträchtliche Haftungsfragen auf, wenn beispielsweise reguläre Kunden auf Grund eines IMSI-Catcher-Einsatzes einen Anruf nicht annehmen oder absetzen konnten. Zu Verminderung der Schäden müsste der Einsatz eines IMSI-Catchers stark limitiert werden und mit den Betroffenen Netzbetreibern abgesprochen werden.

Grundsätzlich gilt, dass technische Maßnahmen, die Auswirkungen auf die Netzintegrität haben können, nur nach vorheriger Beteiligung des betroffenen Netzbetreibers ergriffen werden dürfen. Hierzu ist in § 34 Abs. 2 hinter „Voraussetzungen des Abs. 1“ der Zusatz „nach Absprache mit den betroffenen Netzbetreibern“ einzufügen.

Zu Art. 34a Abs. 4

Die Bestimmung führt zwei neue Maßnahmen ein, die schwerwiegende Auswirkungen auf die Erbringung von Telekommunikationsdienstleistungen haben. Die Befugnis, Kommuni-

kationsverbindungen durch den Einsatz technischer Mittel gezielt zu unterbrechen oder zu verhindern ist ein Novum. Die Regelung erscheint in ihrer Kürze nicht durchdacht. Jedenfalls ist sie unbestimmt.

Die Verfasser des Entwurfs lassen nicht erkennen, dass sie in ihre Überlegungen auch den Umstand einbezogen haben, dass eine Störung oder gar Unterbrechung der Telekommunikation ihrerseits nicht vorhersehbare und unkalkulierbare Gefahren für Leben oder Gesundheit einer Person hervorrufen kann. Es bleibt offen, wie eine Unterbrechung der Kommunikation, etwa im Fall einer Geiselnahme, zu rechtfertigen ist, wenn sie ggf. gleichzeitig Unbeteiligten die Möglichkeit nimmt, einen lebensrettenden Notruf abzuschicken. Das Gesetz schafft hier ohne Not lediglich die Möglichkeit einer nicht auflösbaren Kollisionslage.

Gemäß der dazugehörigen Begründung auf Seite 27 scheinen die Verfasser einseitig davon auszugehen, dass eine ferngesteuerte Zündung von Sprengstoffen mit einem Mobiltelefon nur durch dessen *Anwählen* ausgelöst werden kann, so dass eine Unterbrechung der Funkversorgung Abhilfe schaffen könnte. Unberücksichtigt bleibt indessen, dass ein geeigneter Mechanismus ebenso auch umgekehrt funktionieren kann und ein Sprengsatz ferngezündet werden kann, wenn eine bestehende Funkversorgung plötzlich beendet wird. In diesem Fall wäre eine Verhinderung von Kommunikationsverbindungen unheilvoll. Welche Variante die Attentäter gewählt haben, können Polizeikräfte in der Regel nicht vorab wissen. Der Nutzen einer Telekommunikationsunterbrechung bleibt in diesen Fällen spekulativ.

Überdies enthält die Bestimmung keinerlei einschränkende Eckpunkte zur zulässigen räumlichen Tragweite einer Störung oder Unterbrechung oder zur Wahl der hier zulässigen technischen Mittel. Dies wird völlig in das Ermessen des Adressaten gestellt.

Schließlich berücksichtigt Art. 34 a Abs. 4 BayPAG-E nicht die zivilrechtlichen Implikationen, die eine bewusste Störung oder Unterbrechung der Telekommunikation mit sich bringt (etwa Haftung für durch verursachte Schäden bei Nutzern und Diensteanbietern).

Insgesamt stellt die Möglichkeit Kommunikation zu unterbinden einen schweren Eingriff in die Erwerbstätigkeit der Telekommunikationsanbieter und in deren Vertragsbeziehung mit den Kunden dar. Die gegebenenfalls großflächige, grundsätzlich zeitlich unbefristete Möglichkeit zur Unterdrückung könnte zu Umsatzeinbußen, Kundenunzufriedenheit und einem erhöhten Beschwerdeaufkommen führen und stellt damit einen Eingriff in Art. 12 und 14 GG dar. Diesen Auswirkungen stehen keine entsprechenden, den konkreten Gegebenheiten angepassten Entschädigungsregeln gegenüber. Aus diesem Grund ist in den Wortlaut eine zeitliche und räumliche Begrenzung der Maßnahme sowie eine Entschädigungsregel aufzunehmen, die Erstattung für den für die Unterbrechung erforderlichen Aufwand und für durch die Unterbrechung verursachte Schäden einschließlich möglicher Verdienstaussfälle infolge einer Netzbeeinträchtigung gewährt.

Zu Art. 34b Abs. 2 Satz 1 Nr. 3

Nach Art. 34b Abs. 2 Satz 1 Nr. 3 sollen Mobilfunkunternehmen verpflichtet werden, den Polizeibehörden Auskunft über Geräte- und Kartenummer (IMEI und IMSI) zu erteilen. Diese Verpflichtung begegnet bedenken, da diese Daten nicht durchgehend in den Netzen erhoben und verarbeitet werden und insoweit gar nicht immer vorliegen. Dieser Tatsache ist dadurch Rechnung zu tragen, dass der Wortlaut dahingehend ergänzt wird, dass nur Auskunft erteilt werden muss, soweit die geforderten Daten im Rahmen der Realisierung der Telekommunikation im jeweiligen Telekommunikationsnetz erhoben und verarbeitet werden.

Darüber hinaus ist darauf hinzuweisen, dass eine solche Auskunftspflicht keinen Mehrwert für die Ermittlungstätigkeiten der Polizei darstellen, da IMEI und IMSI Merkmale sind, die nicht hinreichend gegen Fälschung und sonstige Manipulation gesichert sind. Gerade die IMEI ist auch als Anknüpfungspunkt für Ermittlungen nicht geeignet, da sich die Zielperson auch durch eine Weitergabe bzw. Austausch des Endgerätes einer Überwachung entziehen kann. Gerade im Bereich der professionellen Kriminalität ist dies auch hinlänglich bekannt, so dass Erfolge nur bei dummen Tätern oder solchen mit geringer kriminellen Energie oder Erfahrung zu erwarten sind.

Zu Art. 34b Abs. 2 Satz 2

Art. 34 b Abs. 2 Satz 2 eröffnet der Polizei die Möglichkeit, Anfragen nach eingehenden Anrufen auf eine bestimmte Nummer zu stellen, somit eine Inverssuche zu starten. Eine solche Inverssuche bedeutet, dass im Rahmen einer Zielwahlsuche alle Telekommunikationsanbieter alle Verkehrsdaten aller Kunden durchsuchen müssen, um eine Beauskunftung vornehmen zu können. Dies ist technisch nur durch Bindung erheblicher Ressourcen des Netzes und der Rechensysteme möglich und stellt einen unverhältnismäßigen Eingriff in den Betrieb der Telekommunikationsdienstleister dar. Die mit solchen Anfragen einhergehenden Belastungen werden noch dadurch verstärkt, wenn einzelne Gespräche oder Zeiträume abgefragt werden sollen. Eine besondere Problematik entsteht dadurch, dass nach Art. 34 b Satz 2 i.V.m. Art. 34c Abs. 2 Satz 2 PAG diese Maßnahme sogar durch den „normalen“ Polizeibeamten angeordnet werden kann, wenn diese Befugnis auf ihn übertragen wurde und wenn es um die Ermittlung eines Aufenthaltsortes des Verdächtigen geht. Dadurch sind Anfragen in erheblicher Anzahl zu erwarten, welche nicht mit den derzeit vorhandenen Ressourcen bearbeitet werden könnten. Die Verpflichtung zur Auskunftserteilung über eingehende Anrufe ist daher zwingend zu streichen.

Dies folgt schließlich auch daraus, dass die geplante Befugnis für den in der Begründung angeführten Zweck im Ergebnis auch gar nicht erfolgreich eingesetzt werden könnte. Die Begründung stellt hierbei nämlich insbesondere auf das Auffinden von Vermissten und von Suizidkandidaten ab. Für diesen Bedarf ist aber die in Satz 2 normierte Verpflichtung, Daten über Telekommunikationsverbindungen zur Verfügung zu stellen, die zu den gesuchten Personen hergestellt worden sind, typischerweise ungeeignet. Denn die sehr aufwändige Zielwahlsuche kann in der Regel frühestens zwei Tage nach dem fraglichen Ereignis gestartet werden. Das ist für den seitens der Polizeibehörden am häufigsten genannten Fall abgängiger Suizidkandidaten ein viel zu langer Zeitraum, um den angestrebten Erfolg der Lebensrettung in akuter Gefahrensituation überhaupt erreichen zu können. Schon deshalb ist die formulierte Verpflichtung nicht zweckmäßig.

Überdies hat das BVerfG klare Vorgaben bezüglich der Abfrage von Verbindungsdaten gemacht. Vor dem Grundrecht des Fernmeldegeheimnisses erachtet es eine Abfrage von Verbindungsdaten nur dann für zulässig, wenn sie eine Straftat von erheblicher Bedeutung betrifft (BVerfG, NJW 2003, 1787 ff.). Noch strenger ist das BVerfG soweit es um Zielwahlsuchläufe geht: hier gibt es zu erkennen, dass die Zielwahlsuche einer gesonderten Kontrolle durch das Parlament oder den Datenschutzbeauftragten zugeführt werden sollten.

Der Suizid bzw. der Versuch des Suizids ist unstreitig selbst keine strafbare Handlung. Es spricht auch Vieles dafür, dass es sich beim Suizid um die Betätigung des freien Willens eines Individuums handelt, der von der grundrechtlich geschützten Handlungsfreiheit umfasst wird. Daher ist es keineswegs rechtlich gesichert, dass ein angekündigter Suizid ein polizeiliches Einschreiten rechtfertigt.

Wertet man den angekündigten Suizid des ungeachtet als eine grundrechtliche Kollisionslage, kann diese jedenfalls nicht dazu führen, dass zu deren Abwendung auch in Grundrechte unbeteiligter Dritter eingegriffen werden kann. Dass es sich bei der belastenden Anordnung einer Verbindungsdatenauskunft um einen Eingriff in die Grundrechte des Verpflichteten Unternehmens nach Art. 12 und 14 GG handelt, bedarf keiner weiteren Erläuterung.

Erst recht gelten diese Überlegungen für den bloßen Vermisstenfall. Eine akute Gefährdungslage ist hier jedenfalls per se nicht gegeben. Im Gegenteil gehen viele Vermisstenmeldungen an dem Umstand vorbei, dass die Gesuchten gar nicht gefunden werden wollen und keiner „Rettung“ bedürfen. Vor diesem Hintergrund wäre eine grundrechtsbeeinträchtigende Verpflichtung der TK-Unternehmen evident verfassungswidrig.

Zu Art. 34b Abs. 2 Satz 3

Art. 34b Abs. 2 Satz 3 überlässt es den Polizeibehörden, die zeitlichen und technischen Rahmenbedingungen der Übermittlung der Daten festzulegen. Dies kann nicht akzeptiert werden, da die technischen und zeitlichen Anforderungen bereits auf Grundlage des TKG durch die TKÜV und die dazu ergangene Technische Richtlinie abschließend geregelt sind. Art. 34b Abs. 1 stellt dementsprechend auch klar, dass die Mitwirkungspflichten sich nach dem TKG und den dazu ergangenen Verordnungen bemessen. Satz 3 ist entsprechend zu streichen.

Zu Art. 34b Abs. 3

Die in Art. 34b Abs. 3 vorgesehene Definition der herauszugebenden Daten im PAG muss entfallen, da es den Unternehmen nicht zumutbar ist, neben dem Katalog des TKG und der TKÜV weitere Anforderungen zu beachten. Die vorgesehenen Definitionen sind bereits durch das TKG erfolgt und damit auch inhaltlich begrenzt worden. Hierauf wurde in Abs. 1 der Norm auch ausdrücklich Bezug genommen.

Speziell zu dem Merkmal „Kartennummern“ ist anzumerken, dass diese in keinem Fall in Zusammenhang mit einer Telekommunikation technisch erhoben oder erfasst werden. Gleiches gilt für den in Abs. 3 Nr. 1 verwandten und in diesem Kontext unüblichen Begriff der „Berechtigungskennung“. Gerade diese Unklarheiten sprechen dafür, die Definitionen nur an zentralem Ort im Spezialgesetz, also im TKG, vorzunehmen, und hierauf in den Landesgesetzen nur Bezug zu nehmen.

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.