

Stellungnahme

zum Entwurf eines Vierten Gesetzes zur Änderung des Brandenburgischen Polizeigesetzes

14. August 2006

Seite 1

Der BITKOM vertritt mehr als 1.000 Unternehmen, davon 800 Direktmitglieder mit 120 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Geräte-Hersteller, Anbieter von Software, IT- und Telekommunikationsdiensten sowie Content.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Zusammenfassung

Das Brandenburgische Innenministerium hat den Entwurf eines Vierten Gesetzes zur Änderung des Brandenburgischen Polizeigesetzes vorgelegt, der weit reichende Regelungen u.a. im Bereich der präventiven Telekommunikationsüberwachung sowie weitere Zugriffsrechte auf Kommunikationsdaten enthält.

Albrechtstraße 10
10117 Berlin
+49. 30. 27576-0
Fax +49. 30. 27576-400
bitkom@bitkom.org
www.bitkom.org

Nachdem das Bundesverfassungsgericht Regelungen zur präventiven Telekommunikationsüberwachung in Niedersachsen für verfassungswidrig und nichtig erklärt hat (1 BvR 668/04 v. 27.07.2005), begegnet der Entwurf verfassungsrechtlichen Bedenken. Eine Ausweitung der Telekommunikationsüberwachung, bislang ein Mittel der repressiven Strafverfolgung, betrifft die BITKOM-Branche dabei doppelt:

Ansprechpartner
Dr. Volker Kitz LL.M. (NYU)
Rechtsanwalt
Bereichsleiter
Telekommunikations- und
Medienpolitik
+49. 30. 27576-221
Fax +49. 30. 27576-222
v.kitz@bitkom.org

Zum einen bedeutet sie eine weitere Aushöhlung des grundrechtlich geschützten Fernmeldegeheimnisses. Seine Gewährleistung ist aber ein zentrales Element, um das Vertrauen der Nutzer in die Verlässlichkeit elektronischer Kommunikationsmittel zu wahren. Deshalb besteht nicht nur aus bürgerrechtlicher, sondern auch aus wirtschaftlicher Sicht ein großes Interesse an der Aufrechterhaltung eines hohen Schutzniveaus in diesem Bereich.

Präsident
Willi Berchtold

Zum anderen müssen die Unternehmen auch die erheblichen Kosten für die geplanten Mitwirkungspflichten tragen, denn bis heute fehlt eine adäquate Entschädigungsregelung für die Inanspruchnahme der privaten Unternehmen für rein staatliche Zwecke. Diese Kosten umfassen erhebliche Investitionskosten für die Ermöglichung der TK-Überwachung ebenso wie hohe Lasten für die Ausführung der einzelnen Anordnungen und die Bearbeitung von Datenanfragen.

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Die Verhältnismäßigkeitsprüfung bei der Einführung neuer Pflichten muss daher neben dem Fernmeldegeheimnis der Nutzer stets auch die Wirtschaftsgrundrechte der verpflichteten Unternehmen berücksichtigen, was die Verfassungskonformität der geplanten Verpflichtungen doppelt in Frage stellt. Dabei ist es für die Verhältnismäßigkeit der neuen Pflichten von entscheidender Bedeutung, ob parallel zu den Eingriffsbefugnissen für die Sicherheitsbehörden auch Entschädigungsregeln geschaffen werden, welche die Kosten der Unternehmen aufwandsgerecht erstatten.

Stellungnahme

Brandenburgisches Polizeigesetz

Seite 2

Zu den geplanten Regelungen im Einzelnen:

§ 33b Abs. 1 BbgPolG-E

Nach Abs. 1 Satz 1 kann die Polizei „personenbezogene Daten durch den verdeckten Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation erheben“.

Diese Formulierung ist zumindest missverständlich, da sie offen lässt, ob die Polizei die Maßnahme selbst durchführt oder sich dabei eines Netzbetreibers bedient. Erst aus der Begründung geht hervor, dass Regelungsgegenstand des Abs. 1 „lediglich“ die Telekommunikationsüberwachung im Sinne des TKG und der StPO ist, d.h. die Überwachung infolge einer Anordnung gegenüber dem Netzbetreiber. Bereits der Normtext sollte klarstellen, dass es nicht um die Überwachung durch den verdeckten Einsatz von Techniken wie den „IMSI-Catcher mit zusätzlicher Abhörfunktionalität“ geht. Denn gerade im Zusammenhang mit der Nutzung des IMSI-Catchers wurde in Deutschland immer wieder betont, dass hierdurch lediglich IMSI und IMEI erfasst, keinesfalls aber die (bei einzelnen Geräten technisch bestehende) Möglichkeit zur Telekommunikationsüberwachung und -aufzeichnung genutzt würde. Eine weniger missverständlich Fassung könnte lauten: „Die Polizei kann durch die Überwachung und Aufzeichnung der Telekommunikation personenbezogene Daten erheben, wenn ...“.

Das Bundesverfassungsgericht betont in der zitierten Entscheidung, dass dem Straftatenkatalog ein „auf die Besonderheiten der Telekommunikationsüberwachung im Vorfeld zugeschnittenes gesetzgeberisches Konzept zu entnehmen“ sein muss, „das sich auf den Schutz besonders hochrangiger Rechtsgüter bezieht und beschränkt“ (Rz. 152). § 100 a StPO bietet ein Beispiel für ein Ergebnis der bei der Telekommunikationsüberwachung vorzunehmenden Interessenabwägung, an dem sich auch der Landesgesetzgeber orientieren sollte. Eine Ausweitung auf alle Verbrechen (i.V.m. § 10 Abs. 3 Satz 1 BbgPolG), also laut Entwurfsbegründung auf alle Straftaten die bereits den Bereich der „mittleren Kriminalität überschreiten“, dürfte den Schutz nur „besonders hochrangiger“ Rechtsgüter weit überschreiten.

Auch die Anknüpfung an „konkrete Informationen über Planungs- und Vorbereitungshandlungen“ genügt nicht den Anforderungen des Bundesverfassungsgerichts. Zwar empfiehlt das Bundesverfassungsgericht eine Einengung des Tatbestandes auf konkrete Vorbereitungshandlungen (Rz. 124). Jedoch nimmt es dabei ausdrücklich und mehrfach (Rz. 124 und 150) Bezug auf die Regelung in § 23a ZFdG, und zwar nicht auf Abs. 1, sondern ausschließlich auf Abs. 2 und 3. In § 23a Abs. 2 und 3 ZFdG aber finden sich die Vorbereitungshandlungen nicht nur als Schlagwort, sondern als ganz konkrete Umschreibungen (z.B. „das Führen von Verhandlungen über die Lieferung von Gütern oder das Erbringen von Dienstleistungen“). Evident geht das Bundesverfassungsgericht also nicht davon aus, dass eine bloße Bezugnahme auf „konkrete Informationen über Planungs- und Vorbereitungshandlungen“ den Bestimmtheits- und Verhältnismäßigkeitsanforderungen entsprechen kann. Vielmehr lässt dies die vom Gericht (Rz. 121) monierte „hohe Ambivalenz“ eines „unterschiedlich deutbaren Ge-

Stellungnahme

Brandenburgisches Polizeigesetz

Seite 3

schehens“ unberührt. Macht sich der Gesetzgeber hier nicht die Mühe, dem klaren Ratschlag des Gerichts zu folgen und für jede Katalogstraftat nach dem Vorbild des § 23a Abs. 2 und 3 ZFdG die Vorbereitungshandlungen klar zu umschreiben, so läuft er Gefahr, gewarnt und sehenden Auges eine eigene verfassungsrechtliche Niederlage zu erleiden.

§ 33b Abs. 2 BbgPolIG-E

Die in Abs. 2 Nr. 3 vorgeschlagene Befugnis, Kommunikationsverbindungen zu unterbrechen oder zu verhindern, ist ein Novum, das nicht ausreichend durchdacht scheint, jedenfalls aber zu unbestimmt ist.

Grundsätzlich begrüßenswert ist, dass der Brandenburgische Gesetzgeber von dem im Rahmen der Polizeigesetze der Länder weithin diskutierten Ansatz, den Netzbetreiber zur regionalen Abschaltung seines Netzes auf Anordnung der Polizei zu zwingen, Abstand genommen hat. Wie die Begründung zu Recht ausführt, entbehrt eine solche Verpflichtung jeglicher Notwendigkeit, da die Polizei über ausreichende eigene technische Möglichkeiten verfügt.

Allerdings bringt auch der vom Brandenburgischen Gesetzgeber gewählte Ansatz Probleme mit sich: Eine Störung oder gar Unterbrechung der Telekommunikation kann ihrerseits unvorhersehbare und unkalkulierbare Gefahren für Leben oder Gesundheit einer Person hervorrufen. Es bleibt offen, wie eine Unterbrechung der Kommunikation, etwa im Fall einer Geiselnahme, zu rechtfertigen ist, wenn sie gleichzeitig Unbeteiligten die Möglichkeit nimmt, einen lebensrettenden Notruf abzuschicken. Das Gesetz schafft hier ohne Not lediglich die Möglichkeit einer nicht auflösbaren Kollisionslage.

Die in der Begründung erwähnte ferngesteuerte Zündung von Sprengstoffen mit einem Mobiltelefon kann nicht nur durch dessen Anwählen ausgelöst werden, sondern genauso auch umgekehrt, indem eine bestehende Funkversorgung plötzlich beendet wird. Welche Variante die Attentäter gewählt haben, kann die Polizei nicht vorab wissen. Die Begründung zum Entwurf suggeriert außerdem zu Unrecht, dass eine Verhinderung oder Unterbrechung von Telekommunikationsverbindungen beim Anschlag von Madrid hilfreich gewesen wäre. Es ist inzwischen allgemein bekannt, dass in Madrid ausschließlich die Weckfunktion eines Mobiltelefons zur Aktivierung der Bombe genutzt wurde. Eine „Unterbrechung oder Verhinderung von Kommunikationsverbindungen“ hätte diesen Anschlag nicht verhindern können.

Überdies enthält die Bestimmung keine Einschränkung zur zulässigen räumlichen Tragweite einer Störung oder Unterbrechung der Telekommunikation oder zur Wahl der zulässigen technischen Mittel, ebenso wenig über eine zulässige Höchstdauer (s. Abs. 5). Auch technisch ist eine räumlich beschränkte Unterbindung des Mobilfunkverkehrs schwer zu bewerkstelligen, wie die Entwurfsbegründung selbst einräumt. So würde der Einsatz so genannter „Jammer“ zu erheblichen Störungen im Sinne des § 55 Abs. 1 TKG führen. Den Ausführungen der Begründung, wonach sich der Einsatz von Störsendern auf bestimmte Gebäude beschränken lasse, widersprechen wir. Eine

Stellungnahme

Brandenburgisches Polizeigesetz

Seite 4

solche Beschränkung ist in der Regel technisch ausgeschlossen. Auch ein IMSI-Catcher stört alle in seinem Wirkungsbereich befindlichen mobilen Endgeräte, sofern die spezifischen Gerätekennungen des Adressaten der Maßnahme noch nicht bekannt sind. Die in der Begründung enthaltene Aussage, die Wirkungen des IMSI-Catchers ließen sich technisch ausschließlich auf das vom Adressaten der Maßnahme benutzte Endgerät beschränken, muss insoweit relativiert werden.

Des Weiteren lässt die Formulierung die intendierte Beschränkung des Anwendungsbereichs auf den Mobilfunk nicht erkennen. So lässt sich die Norm in der bestehenden Fassung auch so auslegen, dass auch Festnetzverkehre durch technische Mittel unterbrochen oder verhindert werden dürften. Da der Gesetzgeber dies erkennbar nicht beabsichtigt, empfehlen wir eine entsprechende Klarstellung im Normtext.

Schließlich berücksichtigt der Vorschlag nicht die zivilrechtlichen Implikationen, die eine bewusste Störung oder Unterbrechung der Telekommunikation mit sich bringt, etwa Haftung für hierdurch verursachte Schäden bei Nutzern und Diensteanbietern. Hier fehlen Regelungen darüber, wie mit Schäden betroffener Dritter umzugehen ist, ebenso wie zu einer Information der Endkunden über die „Netzstörungen“.

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 kann zu Umsatzeinbußen, Kundenzufriedenheit und einem erhöhten Beschwerdeaufkommen führen. Diesen Auswirkungen stehen keine entsprechenden, den konkreten Gegebenheiten angepassten Entschädigungsregeln gegenüber.

Aus diesem Grund sind in den Wortlaut zumindest eine räumliche Begrenzung der Maßnahme sowie eine Entschädigungsregelung aufzunehmen. Letztere muss einen Aufwandsersatz ebenso wie Ersatz von durch die Unterbrechung verursachten Schäden einschließlich möglicher Verdienstauffälle infolge einer Netzbeeinträchtigung gewähren.

§ 33b Abs. 5 BbgPolG-E

Satz 4 Nr. 1:

Laut Entwurf muss eine Anordnung Namen und Anschrift des Adressaten lediglich „soweit bekannt“ beinhalten. Dies weicht gegenüber der StPO die Anforderungen an die Anordnung von Maßnahmen weiter auf und verursacht den Netzbetreibern zusätzlichen Konsolidierungsaufwand. Zudem dürfte sich eine solche Aufweichung noch weiter negativ auf die in der Praxis ohnehin schon oft unzureichende Beschlussqualität auswirken.

Stellungnahme

Brandenburgisches Polizeigesetz

Seite 5

Satz 5 Nr. 1:

Sowohl in den Fällen des Abs. 2 Nr. 2 (Unterbrechen/Verhindern von Telekommunikationsverbindungen) als auch im Falle des Abs. 2 Nr. 1 (Standortermittlung) geht es um den Einsatz eines IMSI-Catchers mit den bekannten Nebenwirkungen auf Netzintegrität und -verfügbarkeit. Es ist daher im Hinblick auf die damit einhergehenden Beeinträchtigungen für Dritte und für die Netzbetreiber nicht ersichtlich, warum bei Nr. 1 der mögliche Anordnungszeitraum deutlich länger ist als bei Nr. 2. Eine enge Befristung von drei Tagen ist vielmehr in beiden Fällen geboten.

Satz 5 Nr. 2:

Hier fehlt eine effektive zeitliche Einschränkung der Befugnis der Polizei, Telekommunikationsverbindungen unterbrechen zu dürfen. Nach dem Entwurf ist die Maßnahme auf drei Tage zu beschränken. Sie ist jeweils um drei Tage verlängerbar, wenn die Voraussetzungen weiterhin erfüllt sind. Eine schon anfänglich vergleichsweise lange Dauer von drei Tagen, gepaart mit einer offenbar unbeschränkten Verlängerungsmöglichkeit, steht wegen des besonderen Störpotenzials dieser Maßnahme nicht im Einklang mit den in der Begründung für diese Maßnahme angeführten Notwendigkeits- und Angemessenheitserwägungen. Hier ist zumindest eine absolute Obergrenze erforderlich.

§ 33b Abs. 6 BbgPolIG-E:

Satz 2:

Nach der vorgeschlagenen Fassung kann die Polizei die Netzbetreiber verpflichten, „unverzüglich Auskunft über [...] künftige Verkehrsdaten [...] zu erteilen“. Gemeint ist sicherlich die unverzügliche Umsetzung einer Maßnahme zur Beauskunftung, die in die Zukunft weist. Wir empfehlen eine Klarstellung.

Inhaltlich ermächtigt Satz 2 „die Polizei“, vom Diensteanbieter Auskunft zu verlangen. Damit enthält der Entwurf erstmalig die ausdrückliche Ermächtigung eines "einfachen" Polizisten, Auskunft über Daten zu verlangen, welche das Fernmeldegeheimnis schützt. Hierfür sieht der Entwurf – im Gegensatz zu bisherigen Einschränkungen des Richtervorbehaltes bei Eingriffen in das Fernmeldegeheimnis – nicht einmal Gefahr im Verzug vor. Auch schreibt der Entwurf kein Verfahren für das Auskunftersuchen vor. Aus unserer Sicht ist die Regelung daher verfassungsrechtlich problematisch.

Auch will Satz 2 Anbieter dazu verpflichten, der Polizei Auskunft über Geräte- und Kartennummer (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. Hier ist zumindest eine Einschränkung dahingehend nötig, dass Auskunft nur erteilt werden muss, soweit die geforderten Daten im Rahmen der Realisierung der Telekommunikation im jeweiligen Telekommunikationsnetz erhoben und verarbeitet werden. Hier erscheint eine Anlehnung an § 7 Abs. 1 TKÜV erforderlich.

Stellungnahme

Brandenburgisches Polizeigesetz

Seite 6

Satz 3:

Die in Satz 3 schließlich vorgesehene Entschädigung nach § 23 JVEG gewährleistet keine angemessene Entschädigung. Eine Entschädigung nach Zeugenentschädigungsrecht ist nicht sachgerecht. Die Anbieter werden gerade nicht als gewöhnliche Zeugen nach den allgemeinen Zeugenregelungen (§§ 48 ff. StPO) in Anspruch genommen. Vielmehr unterliegen sie zahlreichen Sonderverpflichtungen, die über Jedermannspflichten weit hinausgehen. Der vorliegende Entwurf ist nur ein Beispiel für eine solche Sonderverpflichtung. Auch nach Häufigkeit und im Umfang werden Telekommunikationsanbieter weitaus intensiver in Anspruch genommen als normale Bürger in ihrer Zeugenpflicht. Die Entschädigungssätze nach JVEG sind dabei nicht ansatzweise kostendeckend. Wo die Pflichten weit über die Jedermannspflichten hinausgehen, ist aber ein Verweis auf die „Jedermann-Entschädigungssätze“ verfehlt. Vielmehr bedarf es hier aus verfassungsrechtlichen Gründen auch eines besonderen Entschädigungsregimes.

Anwendbarkeit der Telekommunikations-Überwachungsverordnung

Das Landesgesetz sollte ausdrücklich klarstellen, dass für Anforderungen und Durchführung der Überwachungsmaßnahmen die Telekommunikations-Überwachungsverordnung (TKÜV) des Bundes gilt. Diese erklärt sich zwar selbst in § 1 Nr. 1d) auf Überwachungsmaßnahmen nach Landesrecht für anwendbar. Jedoch erfordert die Rechtssicherheit, dass auch das Landesrecht ausdrücklich auf die TKÜV verweist, und zwar im Gesetzestext selbst und nicht nur in der Gesetzesbegründung.

In der Praxis sehen sich die verpflichteten Unternehmen leider all zu oft mit „atypischen“ Anfragen konfrontiert. Dies hat seine Ursache darin, dass bei Gefahr im Verzug der Kreis der Anordnungsberechtigten sehr weit (und daher durch die Verpflichteten oft nicht mehr kontrollierbar) gefasst ist und hier mitunter Personen tätig werden, die bisher wenig oder keine Erfahrung bei der Anordnung von Telekommunikationsüberwachungen haben. Die dann von den Unternehmen nicht selten zu leistende beträchtliche rechtliche und technische Aufklärungsarbeit bedeutet eine zur eigentlichen Überwachungsmaßnahme zusätzliche, jedoch unnötige Belastung. Hier ist es wichtig, dass der Anordnende selbst sofort aus dem jeweiligen Landesgesetz erkennen kann, welche Anforderungen für die Anordnung und Durchführung der von ihm erstrebten Maßnahmen gelten.