

## **Eckpunkte zur Anpassung der Regelungen des § 90 TKG**

### **Einleitung**

Nach mehrfacher Kabinettbefassung in den Jahren 1992 / 1993 hat die Bundesregierung beschlossen, im Interesse der Strafverfolgung gesetzliche Regelungen einzuführen, die auch in einem privatisierten und liberalisierten Telekommunikationsmarkt und den absehbaren Vermarktungsmethoden der Telekommunikationsdienstleistungen eine Zuordnung von Rufnummern zu den Kunden der Telekommunikationsunternehmen ermöglicht.

Dazu wurde im Telekommunikationsgesetz von 1996 die Vorschrift des § 90 eingeführt, die das Auskunftersuchen für die Sicherheitsbehörden regelt und die die Telekommunikationsunternehmen verpflichtet, Kundendateien zu führen, in die die Rufnummern sowie Name und Anschrift der Inhaber der Rufnummern aufzunehmen sind, auch soweit sie nicht in öffentliche Verzeichnisse eingetragen sind. In diese Datei sollen auch entsprechende Kundendaten von Inhabern von Prepaid-Karten aufgenommen werden. Das Bundesministerium für Post und Telekommunikation in seiner Funktion als Regulierungsbehörde für Telekommunikation und Post hat 1997 nach Abstimmung innerhalb der Bundesregierung zur Interpretation der Vorschrift eine Leitlinie erlassen, wonach die Identität des Kunden mittels geeigneter amtlicher Dokumente nachgewiesen werden soll.

Das Verwaltungsgericht Köln kam mit Urteilen vom 22.09.2000 zu dem Schluss, dass die Regelungen des § 90 TKG nicht ausreichen, um Daten von Inhabern von Prepaid-Karten zu erheben. Gegen diese Entscheidung hat die Reg TP Rechtsmittel eingelegt. Bis zu einer entgültigen Entscheidung bleibt es bei dem bisherigen Verfahren.

## **Begründung der Notwendigkeit einer Datenerfassung auch für Prepaid-Karten,**

### **Verifizierung dieser Daten**

Die Verwendung anonym oder pseudonym erworbener Prepaid-Karten erschwert die Ermittlungstätigkeit der Sicherheitsbehörden. Die Erfahrungen der Behörden zeigen, dass die gesetzliche Regelungslücke unter Straftätern bekannt ist und in nahezu allen Deliktsbereichen mit steigender Tendenz genutzt wird, um Beweisführungen der Ermittler unmöglich zu machen.

Derzeit werden Prepaid-Karten von Straftätern häufig unter Angabe falscher bzw. fiktiver Personalien oder unter dem Namen der Vertriebspartner (Händler) erworben und registriert, oder es werden nicht existente Anschriften angegeben. Die Telekommunikationsbetreiber geben sich vielfach mit nicht überprüften Selbstauskünften der Käufer zufrieden oder verlangen innerhalb einer Frist von bis zu drei Monaten eine Identitätsangabe. Der tatsächliche Anschlussinhaber kann aufgrund dieser Vertriebspraxis nicht ermittelt werden, denn die Karteninhaber bleiben anonym und Kontakte zwischen Beschuldigten und /oder Zeugen werden auf diese Weise verschleiert.

Ein Einstieg in ein strafrechtliches Ermittlungsverfahren ist dadurch oftmals unmöglich, oder bereits eingeleitete Ermittlungsverfahren müssen eingestellt werden. Außerdem kommt es wegen der zum Teil falschen Angabe von Personalien unbeteiligter Dritter immer wieder zu zeitaufwendigen und kostenintensiven Ermittlungsmaßnahmen gegen Unschuldige. Durch andere Maßnahmen (z.B. Observation oder Videoüberwachung der Verdächtigen) sind diese Lücken in der Telekommunikationsüberwachung nur bedingt zu schließen. Regelmäßig kommt es auch zu Schwierigkeiten bei der Telekommunikationsüberwachung (z.B. nach § 100a StPO), denn dort sind Anschlussinhaberverfeststellungen von entscheidender Bedeutung.

Die Datenerhebung bei Prepaid-Karten ist allerdings nicht nur zur Vorbereitung und Durchführung von Telekommunikationsüberwachungsmaßnahmen erforderlich, sondern stellt ein unverzichtbares Instrument auch zur Durchführung polizeilicher Standardmaßnahmen im Rahmen von Ermittlungsverfahren dar. Dieses gilt etwa insofern, als die Feststellung des Anschlussinhabers auch für Auskünfte über Verbindungsdaten nach § 100g und § 100h StPO unerlässlich ist. Bei offenen Ermittlungsmaßnahmen wie Wohnungsdurchsuchungen, Sicherstellungen oder in Beschlagnahmefällen fallen häufig Mobiltelefonnummern in schriftlicher Form an (Notizbücher, Timer, auf Telefonrechnungen, elektronisch gespeichert in anderen Mobiltelefonen), die u.a. zur Feststellung von (Kommunikations-)Verbindungen, zur Ermittlung weiterer Tatbeteiligter etc. überprüft werden müssen. Davon hängen im Einzelfall umfangreiche weitere Maßnahmen ab, wie z.B. die nationale und internationale Ausschreibung

ermittelter Tatverdächtiger zur Festnahme oder die Durchführung von Maßnahmen der Öffentlichkeitsfahndung. Im Rahmen des internationalen polizeilichen Nachrichtenaustausches bzw. des justiziellen Rechtshilfeverkehrs sind Anfragen ausländischer Behörden mit der Bitte um Anschluss-Inhaberfeststellung zur Wahrnehmung der dortigen Aufgaben gängige Praxis.

Nicht nur für Ermittlungen im klassischen Sinne (Sammeln von gerichtsverwertbaren Beweisen zu Taten und Tätern), sondern auch für die Zielfahndung (Aufspüren von erkannten Straftätern, die sich der Festnahme/Haft entzogen haben) ist die Erfassung der Kundendaten geboten. Im Rahmen jeder Zielfahndung wird das persönliche Umfeld des gesuchten Straftäters aufgeklärt, um möglicherweise bestehende Kontakte zum Gesuchten feststellen und nachvollziehen zu können. Hierbei sind in erster Linie die Kommunikationsmöglichkeiten dieses Umfeldes von Interesse.

Sicherheitsbehörden sind oftmals damit konfrontiert, dass Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, die Karte wechseln oder mehrere Prepaid-Karten parallel nutzen und diese teilweise von Telefonat zu Telefonat wechseln.

Steht der Käufer einer Prepaid-Karte fest, so lässt sich bei Weitergabe oder Schenkung der Karte an Dritte durch ergänzende Ermittlungen feststellen, welche Person aus dem Umfeld des Käufers die Karte nutzt. Insbesondere mit Blick auf die Qualität des internationalen Terrorismus ergeben sich - vor allem bei Ermittlungen in Strukturverfahren - hier Möglichkeiten, weitere wichtige Ermittlungsansätze zu erhalten.

Die nahezu ausschließliche Verwendung von Prepaid-Karten spielt vor allem in den Bereichen der Organisierten Kriminalität, des Drogenhandels und der Staatsschutzkriminalität eine erhebliche Rolle. Bei überwachten Gesprächen, die einen sofortigen Handlungsbedarf nach sich ziehen (z.B. Rauschgiftbestellungen/-transporte), ist es dringend erforderlich, in möglichst kurzer Zeit den Anschlussinhaber zu erfahren.

Die Verwendung von Prepaid-Karten nimmt auch in allen Beobachtungsbereichen der Nachrichtendienste kontinuierlich zu. Dies gilt vor allem im Bereich islamistischer terroristischer Gruppierungen. Aufgrund der steigenden Tendenz der Verwendung dieser Karten in einschlägigen Kreisen wird es ohne die Erfassung von Kundengrunddaten zu nicht hinnehmbaren Ermittlungslücken in einem Bereich führen, der als einer der gefährlichsten für die innere Sicherheit der Bundesrepublik Deutschland eingeschätzt wird.

Schließlich ergeben sich erhebliche Sicherheitsdefizite durch die Nicht-Erfassung der Kundendaten im Bereich der polizeilichen Gefahrenabwehr. In Vermisstensachen, bei polizeilichen Maßnahmen nach Suizid-Ankündigungen, Bombendrohungen oder Entführungs-

und Erpressungsfällen ist die schnelle Verfügbarkeit verlässlicher Anschlussinhaberdaten dringend erforderlich.

Aufgrund der geschilderten Probleme kommt es oft dazu, dass Ermittlungsverfahren allein wegen fehlender Kundendaten eingestellt werden müssen und Straftaten nicht aufgeklärt oder verhindert werden können. Im Interesse einer nachhaltigen Kriminalitätsbekämpfung, einer effektiven Gefahrenabwehr und zur Wahrung übergeordneter Sicherheitsinteressen der Bundesrepublik Deutschland besteht daher dringender Rechtsänderungsbedarf.

Auch im Zusammenhang mit Prepaid-Karten sollten daher die Kundengrunddaten erfasst, verifiziert und den Sicherheitsbehörden grundsätzlich im automatisierten Verfahren zugänglich gemacht werden. Die gesetzliche Regelung muss die oben erwähnten Vertriebswege berücksichtigen, so dass bei der Kartenweitergabe ein möglichst lückenloser Nachweis über die Identität des Karteninhabers geführt werden kann. Für Verstöße sollten geeignete Sanktionsmöglichkeiten vorgesehen werden.

Bei dem Schließen der bestehenden Regelungslücke ist den vom Bundesverfassungsgericht festgelegten datenschutzrechtlichen Anforderungen (vgl. BVerfGE 65, 1, 44 ff.) Rechnung zu tragen.

### **Forschungsvorhaben des BMJ zum Thema „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach §§ 100a, 100b StPO“**

Das Forschungsvorhaben zum Thema "Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach §§ 100a, 100b StPO" befasst sich nicht mit Fragen der Erfassung von Kundendaten bei Prepaid-Karten im Rahmen des § 90 TKG.

### **Vergleichbare Regelungen in den angrenzenden Staaten der EU**

Die Ständige Vertretung der Bundesrepublik Deutschland bei der Europäischen Union hat eine Umfrage bei den Vertretungen mehrerer EU-Staaten dazu durchgeführt, ob für Prepaid-Karten im Mobilfunk von den Anbietern Kundendaten erhoben werden.

Gegenwärtig sind lediglich in Frankreich die Anbieter von Prepaid-Karten verpflichtet, Kundendaten zu erheben. Es kommt vor, dass trotz Vorgaben von Regierungsseite völlig

unzutreffende Angaben gemacht werden. In den anderen EU-Staaten, aus denen Informationen vorliegen, gibt es keine gesetzlichen Regelungen, die bei dem Verkauf von Prepaid-Karten zu beachten sind. In einigen dieser EU-Staaten erheben die Provider Daten auf freiwilliger Basis und bieten den Kunden dafür Vergünstigungen an.

### **Würdigung im Hinblick auf Regelungen im Bereich des Datenschutzes (national und EU)**

Datenschutzrechtliche Anforderungen bestehen sowohl auf der Ebene des Gemeinschaftsrechts wie auch in der nationalen Gesetzgebung.

Die Daten, um deren Erhebung, Verarbeitung und etwaige Übermittlung an Sicherheitsbehörden es im Rahmen des § 90 TKG geht, sind sogenannte **Bestandsdaten**, die regelmäßig für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erhoben werden.

Die Bestandsdaten sind abzugrenzen von den **Verbindungsdaten**. Diese umfassen alle Daten, die bei der Bereitstellung und Erbringung von Telekommunikationsdiensten erhoben werden. Informationen über diese Daten können mittels § 90 TKG **nicht** gefordert werden.

Bei der Beurteilung der datenschutzrechtlichen Grenzen im Umgang mit Bestandsdaten sind zunächst die europäischen Vorgaben zu beachten.

Die sektorspezifische **Datenschutzrichtlinie 97/66/EG** (ABl. EG Nr. L 24 vom 30.1.1998, S. 1) für den Bereich der Telekommunikation enthält indes, ebenso wie der von der Kommission vorgelegte Entwurf einer neuen Datenschutzrichtlinie für die elektronische Kommunikation [KOM (2000) 385 vom 12.07.2000], **keine Regelungen** über die Verarbeitung der Bestandsdaten.

Rechtliche Anforderungen an die Verarbeitung von Bestandsdaten enthält die allgemeine **Datenschutzrichtlinie 95/46/EG** (ABl. EG Nr. L 281 vom 23.11.1995, S. 31). Gemäß **Artikel 7 Buchst. c)** der Richtlinie ist die Verarbeitung personenbezogener Daten zulässig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der für die Verarbeitung Verantwortliche unterliegt.

Eine Verpflichtung zur Erhebung der Vertragsdaten und zur Übermittlung dieser Angaben im Ermittlungsfall an die Strafverfolgungsbehörden steht auch im Einklang mit Artikel 7 Buchst. c) der RL 95/46/EG.

Im nationalen Datenschutzrecht sind Bestandsdaten im Bereich der Telekommunikation von der TDSV erfasst. § 3 Abs. 1 TDSV erlaubt die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch Telekommunikationsdiensteanbieter nur, soweit die Verordnung oder eine andere Rechtsvorschrift dies gestattet oder der Beteiligte eingewilligt hat.

Als Erlaubnisnorm kommt jede gesetzliche oder auf ein Gesetz gestützte Verordnungsregelung in Betracht. § 90 TKG wäre daher eine grundsätzlich geeignete Vorschrift zur Regelung der Erhebung, Verarbeitung und Übermittlung von Kundendaten bei Prepaid-Karten.

### **Abgleichung der relevanten Regelungen der §§ 89 und 90 TKG**

Rechtssystematisch stünde dem Bestreben, § 90 TKG als eigenständige Vorschrift über die Erhebung, Verarbeitung und Übermittlung von Bestandsdaten auszugestalten, nichts im Wege. Während § 89 TKG die allgemeinen Anforderungen an den Datenschutz in der Telekommunikation regelt, könnte § 90 TKG einen bestimmten Aspekt gesetzlich normieren.

Dabei gilt es jedoch, auch in § 90 TKG die datenschutzrechtlichen Grundsätze zu beachten. Dies gilt insbesondere hinsichtlich der Festlegung von Speicherfristen, der Beachtung des Grundsatzes der Verhältnismäßigkeit und der Beschränkung der Datenverarbeitung auf das Erforderliche.

### **Interessenlage der Mobilfunkbetreiber zur Datenerhebung**

Die Einführung des automatisierten Verfahrens nach § 90 TKG wird von der Wirtschaft wegen der Erleichterung gesetzlicher Verpflichtungen prinzipiell positiv beurteilt.

Die Erhebung von Kundendaten bei Prepaid-Karten liegt im Sinne einer Kundenbindung nach Darlegung eines Mobilfunkbetreibers auch im Eigeninteresse der Wirtschaft und wird insofern unterstützt. Die vom damaligen BMPT herausgegebene Leitlinie, die die Prüfung der Identität an Hand eines amtlichen Ausweises fordert, ist der Wirtschaft jedoch zu restriktiv. Sie verursache einen hohen Aufwand und täusche angesichts bestehender anderer Lücken eine vollständige Datenerfassung nur vor. Etwa 50 % der Karten werde innerhalb eines Jahres verschenkt, größtenteils innerhalb der Familie. Ein schriftlicher Übernahmeantrag werde vom Kunden nicht akzeptiert und auch von der Wirtschaft als zu aufwendig angesehen. Zudem gebe es im internationalen Bereich Prepaid-Roaming-Verfahren, die national nicht zu erfassen seien.

Von Seiten der Wirtschaft wird als aussichtsreicher eingestuft, die im Eigeninteresse liegende Kenntnis über die Kundendaten und damit auch die Information im Sinne des § 90 dadurch zu gewinnen, dass bei Erwerb oder Weitergabe der Prepaid-Karten an andere Nutzer ein finanzieller Anreiz im Sinne von Vergünstigungen angeboten wird oder, dass die Angabe der Kundendaten als Voraussetzung zur Nutzung bestimmter Dienste oder für eine einfachere Zulassung hierzu verwendet würde.

### **Verwendung von Jokerzeichen und phonetischen Abfragen**

#### **- Notwendigkeit aus Sicht der Strafverfolgungs-/Sicherheitsbehörden**

Nach § 90 Abs. 4 hat die Regulierungsbehörde für Telekommunikation und Post die Daten, die in den Kundendateien der Telekommunikationsbetreiber gespeichert sind, auf Ersuchen der Strafverfolgungs-/Sicherheitsbehörden im automatisierten Verfahren abzurufen und an die ersuchende Stelle zu übermitteln. Eine nähere Ausgestaltung des automatisierten Verfahrens sieht § 90 Abs. 4 TKG nicht vor. Insbesondere ist gesetzlich nicht ausdrücklich geregelt, ob auf den Datenbestand auch dann zugegriffen werden kann, wenn Identitätszweifel bestehen.

Bei unvollständig vorhandenen Teilnehmerdaten, die zu Identitätszweifeln führen, besteht die technische Möglichkeit, Jokerzeichen bei der Datenabfrage zu verwenden. Als Jokerzeichen bezeichnet man einen Platzhalter ("?", "\*", "#") für unbekannte Buchstaben

oder Ziffern innerhalb eines Teilnehmerdatums. Ein Jokerzeichen kann die Ziffern 0 bis 9 oder Buchstaben ersetzen.

Bei phonetisch aufgenommenen, darum ungesicherten oder unvollständigen Teilnehmerdaten, die zu Identitätszweifeln führen, ist vorstellbar, phonetische Abfragen zuzulassen. Phonetische Abfragen berücksichtigen eine für alle Abfragen im Voraus festgelegte begrenzte Bandbreite ähnlich lautender Bezeichnungen (daher auch die Bezeichnung "Ähnlichenservice" für dieses Verfahren). Bei einer phonetische Abfrage wird z. B. die ungesicherte Angabe "Meier" um bestimmte ähnliche Angaben, wie "Maier", "Mayer" etc. erweitert.

Bei Sprachen, die eine andere Schrift benutzen, gibt es z. T. keine Zeichen für (gesprochene) Vokale, so z. B. im Arabischen. Daher hängt die Transkription in lateinische Schrift jeweils davon ab, in welcher Weise die umsetzende Person dies handhabt. Ein gutes Beispiel hierfür ist die Terrororganisation Al-Quaida, von der es je nach Nationalität oder Vorlieben des Transkribierenden zahlreiche Varianten gibt, z. B. El (oder Al) Quaida, El Qaida, Al Quaeda (so die International Herald Tribune), Kaeda, Kaida etc..

Transkriptionsprobleme gibt es auch in Sprachen aus dem osteuropäischen und dem asiatischen Raum (russisch, chinesisches), die dem Umsetzenden verschiedene Schreibweisen eröffnen.

Das Verfahren ist technisch definiert (z. B. "Kölner Phonetik" in INPOL / NADIS) und stellt somit eine begrenzte Erweiterung dar.

In der täglichen Ermittlungsarbeit besteht erheblicher Bedarf zur Ermöglichung einer Datenrecherche mit unvollständigen Angaben und eines Ähnlichenservices. In nahezu allen Bereichen der Arbeit der Polizei- und anderen Sicherheitsbehörden (INPOL-, ZEVIS-, NADIS-, Melderegisterabfragen usw.) ist die Recherchemöglichkeit mittels Jokerzeichen und phonetischer Abfragen ein effizientes und wichtiges Ermittlungsinstrument. Die derzeit fehlende gesetzliche Möglichkeit der Abfrage mittels Jokerzeichen bei unvollständigen Angaben über Suchkriterien oder phonetischen Abfragen stellt sich für die Sicherheitsbehörden dabei als äußerst problematisch dar. Die Datenrecherche wird auch vor dem Hintergrund zunehmender, täterseitiger Mobilität wichtiger als bisher werden, zum Beispiel um die Rufnummer einer Zielperson zwecks Standortlokalisierung zu kennen. Die Möglichkeit der Abfrage unvollständiger Daten ist teilweise bereits technisch implementiert, allerdings noch nicht freigegeben.

Momentan ist die Abfrage beispielsweise bei fehlenden Ziffern einer Rufnummer sehr arbeitsaufwendig, da alle in Frage kommenden Möglichkeiten einzeln abgefragt werden müssen. Es sind stets zehn Abfragen erforderlich, um eine unbekannte Ziffer zu ersetzen. Eine solche Verfahrensweise führt zwangsläufig zu vermeidbarem Mehraufwand (Mehrfachanfragen oder Abfragen nach § 89 Absatz 6 TKG) sowohl bei den Bedarfsträgern als auch bei den Telekommunikationsdiensteanbietern und bei der RegTP sowie zu Verzögerungen der Ermittlungen.

Sowohl die Suche mit unvollständigen Identifizierungsdaten als auch der Ähnlichenservice müssen allerdings datenschutzrechtlichen Anforderungen genügen, weil sie regelmäßig dazu führen, dass Datensätze mehrerer Personen übermittelt werden, obwohl nur eine Person gesucht wird. Es steht von vornherein fest, dass der gesuchten Person allenfalls ein Datensatz zugeordnet werden kann. Nur dieser Datensatz ist für die behördliche Aufgabenerfüllung wirklich erforderlich, alle anderen nicht. Wegen dieser „Streuwirkung“ bedarf die Suche mit Jokerzeichen und über phonetische Abfragen einer ausdrücklichen gesetzlichen Grundlage (siehe z. B. § 10 Abs. 3 AZRG) und einer präzisen Regelung ihrer Voraussetzungen und Modalitäten. Dabei ist insbesondere zu gewährleisten, dass Mindestanforderungen an den Umfang der bei der Abfrage einzugebenden Daten festgelegt werden, damit die gesuchte Person wenigstens einigermaßen konkret bezeichnet und die Zahl der auszugebenden Datensätze begrenzt wird, und nicht benötigte Daten umgehend gelöscht werden.

- **Interessenlage der Mobilfunkbetreiber zum Jokerzeichen**

Für die Einführung von Jokerzeichen wird keine Notwendigkeit gesehen. Eine derartige Möglichkeit hält man auch für datenschutzrechtlich höchst bedenklich.

**Stellungnahme des BfD**

- **Erfassung der Kundendaten bei Prepaid-Karten**

Entscheidend für die datenschutzpolitische Bewertung dieser Frage ist vor allem die von

verschiedenen Stellen wiederholt erhobene Forderung, zur Förderung der Akzeptanz neuer Anwendungen der Informationstechnik auch anonyme Nutzungsmöglichkeiten vorzusehen. Die 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte deshalb bereits am 23./24.10.1997 einen entsprechenden Beschluss gefasst. In diesem Zusammenhang ist auch der Schlussbericht der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Verwaltung“ des Deutschen Bundestages zu erwähnen, in dem Maßnahmen gefordert werden, die eine datensparsame Gestaltung der in Telekommunikationsnetzen verwendeten Geräte, Programme und Übertragungswege vorsehen. Um die Gebote der Datensparsamkeit und der Datenvermeidung zu erfüllen, sollte danach die anonyme und pseudonyme Nutzung der neuen Dienste gefördert werden (BT-Drs. 13/11004).

Auch der datenschutzrechtliche Grundsatz des Verbots einer Vorratsdatenspeicherung muss Beachtung finden. Auf ihn wurde im übrigen auch von der Bundesregierung verwiesen, als ein Verlangen des Bundesrates nach der Vorgabe von Mindestspeicherfristen von Kundendaten gefordert wurde. Damals wurde darauf hingewiesen, dass die Verarbeitung von Telekommunikationsdaten regelmäßig auf den betrieblich erforderlichen Zweck der Abwicklung der jeweiligen vertraglich vereinbarten Telekommunikationsdienstleistung beschränkt werden müsste (BT-Drs. 13/4438, S. 39). Dies muss auch für die Kundendaten bei Prepaid-Karten gelten, deren Erfassung für die Telekommunikationsdienstleistung nicht notwendig ist und als unzulässige Vorratsspeicherung von Daten angesehen werden muss.

Aus Sicht des Datenschutzes bieten die Prepaid-Verfahren die besten Voraussetzungen für die Realisierung eines sicheren elektronischen Zahlungsverfahrens, das die gleiche Anonymität des Bezahlers erlaubt wie das Bezahlen mit Bargeld.

Für die Teledienste gibt es bereits eine entsprechende datenschutzgerechte Regelung. Nach § 4 Abs. 6 Teledienstedatenschutzgesetz sind die Telediensteanbieter verpflichtet, die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen. Auf europäischer Ebene hat sich dieser Gedanke auch für den Bereich der Telekommunikation durchgesetzt. So sieht die EG-TK-Datenschutzrichtlinie vom 15. Dezember 1997 in Erwägungsgrund 18 die Einführung eines anonymen Zugangs zu öffentlichen Telekommunikationsdiensten vor. Diesen Gedanken hat die Bundesregierung bei der Novellierung der Telekommunikations-Datenschutzverordnung (TDSV)

aufgegriffen. Nach § 3 Abs. 4 TDSV sind die Telekommunikationsunternehmen verpflichtet, sich bei der Durchführung der TK-Verträge an den Zielen der Datenvermeidung und Datensparsamkeit auszurichten.

- **Regelung der Jokerabfrage**

Die Jokerabfrage ist grundsätzlich datenschutzrechtlich bedenklich, weil immer auch Daten Unbeteiligter mitbetroffen sind. Die Rechtsgrundlage für diese Abfragemöglichkeit - die von Seiten des BfD immer als notwendige Voraussetzung für die Einführung der Jokerabfrage gefordert wurde - muss deshalb auf das unbedingt Wesentliche beschränkt werden.

Ausgeschlossen werden sollten Abfragen, mit denen bei geschickter Verwendung der Jokerzeichen eine größere Anzahl von Personendaten mitgeteilt würden z.B. die nahezu komplette Belegschaft einer Firma oder aller Personen, die zur Zeit der Abfrage in einem Krankenhaus ein Telefon nutzen. Wichtig wäre z.B. eine Beschränkung des Einsatzes eines Jokerzeichens nur für eine Stelle im Rahmen der Abfrage.

**Lösungsvorschlag**

Die Ressortarbeitsgruppe hat einen Textentwurf mit Begründung zur Änderung der §§ 89, 90 und 96 TKG erarbeitet.