- Fassung vom 27.06.2003 -

Der staatliche Zugriff auf Telekommunikations-Bestandsdaten aus verfassungsrechtlicher Sicht

Aus Anlass der Umsetzung europäischer Richtlinien ist derzeit eine weitreichenden Überarbeitung des Telekommunikationsgesetzes (TKG) im Gange. Nach Beratungen mit der Wirtschaft und den Sicherheitsbehörden hat das Bundesministerium für Wirtschaft und Arbeit einen konkreten Referentenentwurf vorgelegt (TKG-RefE)[1]. Bei den Regelungen über den staatlichen Zugriff auf Telekommunikations-Bestandsdaten sieht dieser Entwurf gegenüber der bisherigen Rechtslage einige Entlastungen vor, behält die bisher schon weit gehenden Zugriffsrechte aber im Übrigen bei und enthält auch einige wesentliche Verschärfungen. Im Folgenden sollen die verfassungsrechtlichen Grenzen des staatlichen Zugriffs auf Bestandsdaten unter Berücksichtigung der bisherigen Rechtslage und der geplanten Änderungen untersucht werden.

Als Telekommunikations-Bestandsdaten bezeichnet man Daten, die ein Anbieter von Telekommunikationsdiensten von seinen Kunden erhebt, um mit ihnen ein Vertragsverhältnis über die Erbringung von Telekommunikationsdiensten zu begründen, es auszugestalten oder zu ändern (vgl. §§ 88 Abs. 6 TKG, 2 Nr. 3 TDSV, § 3 Nr. 3 TKG-RefE). Es handelt sich also um diejenigen Kundendaten, die der Anbieter für die Durchführung des Vertrags dauerhaft in seinem Datenbestand halten muss, etwa Name und Anschrift des Kunden, dessen Kontoverbindung, aber auch dienstbezogene Merkmale wie eine dem Nutzer zugewiesene Rufnummer oder Emailadresse sowie Kenn- oder Passwörter des Nutzers (z.B. PINs und PUKs im Mobiltelefonbereich). Keine Bestandsdaten sind demgegenüber der Inhalt und die veränderlichen Umstände einzelner Kommunikationsvorgänge (z.B. Rufnummer des Gesprächspartners, Zeit eines Anrufs).

Verfassungsrechtliche Einordnung

Bestandsdaten sind personenbezogene Daten, die als solche jedenfalls durch das Recht auf informationelle Selbstbestimmung geschützt sind[2]. Dies entspricht dem Schutzzweck dieses Rechts, Grundrechtsträger vor der Gefahr zu schützen, dass der Staat über sie unbegrenzt Kenntnisse sammelt und infolgedessen nachteilige Maßnahmen ihnen gegenüber ergreifen kann. Nicht nur die staatliche Kenntnis von Kommunikationsinhalten oder Verbindungsdaten begründet diese Gefahr. Auch die Kenntnis der Tatsache, dass ein Bürger überhaupt ein vertragliches Verhältnis mit einem bestimmten Diensteanbieter begründet hat und wie dieses ausgestaltet ist, kann zu unerwünschten Kommunikationsanpassungen seitens des Einzelnen führen. Wer beispielsweise an der Teilnahme an einem Internet-Chat für Muslime in Deutschland interessiert ist, wird es in Erinnerung an Maßnahmen der „Anti-Terror-Rasterfahndung“ mit anschließender Befragung der „Ausgefilterten“ möglicherweise vorziehen, auf die Ausübung seiner Grundrechte (hier unter anderem der Religionsfreiheit) zu verzichten. Dasselbe kann etwa für die Anmeldung zur Teilnahme an einem Meinungsforum gelten, in dem Protestaktivitäten gegen die Atomkraft diskutiert werden (Meinungsfreiheit, Versammlungsfreiheit). Auch die Mitgliedschaft in sonstigen geschlossenen Netzen, bereitgestellt etwa von einer Aids-Selbsthilfegruppe, kann Rückschlüsse auf bestimmte Problemlagen erlauben[3]. Dasselbe gilt bereits für Standard-Telekommunikationsdienste[4]. Wer beispielsweise einen Internetzugang zum Pauschaltarif nutzt, wird von den Behörden als intensiver Internetnutzer angesehen werden. Wer bei der deutschen Telefongesellschaft „Alo Vatan“ angemeldet ist, wird im Zweifel einen Bezug zu der Türkei aufweisen. Wer einen bestimmten Optionstarif im Mobilfunknetz nutzt, bei dem man fünf Festnetzanschlüsse vom

[1] Abrufbar unter www.tkrecht.de/index.php4?direktmodus=novelle-genese.

[2] OVG Münster, MMR 2002, 563 (564).

[3] DSB-Konferenz vom 14./15.03.2000, www.bfd.bund.de/information/info5/anl/an06.html.

[4] Vgl. ULD-SH, Sichere Informationsgesellschaft, www.datenschutzzentrum.de/material/themen/cybercri/-cyberkon.htm, Punkt 7c.

Alle Rechte vorbehalten – Keine Vervielfältigung oder Verbreitung ohne ausdrückliche Einwilligung des Autors

Handy aus besonders preisgünstig erreichen kann (wird etwa von der Firma Eplus angeboten), gibt schon mit diesen Bestandsdaten preis, mit wem er oft telefoniert. Die genannten Beispiele zeigen, dass Bestandsdaten nicht nur besonders sensibel sein können, sondern auch weit gehende Rückschlüsse auf Inhalt und Umstände einzelner Kommunikationsvorgänge erlauben können.

Fraglich ist, ob Telekommunikations-Bestandsdaten auch durch das Fernmeldegeheimnis (Art. 10 GG) geschützt sind[5]. Einer Einbeziehung von Bestandsdaten in den Schutzbereich des Art. 10 GG steht der Wortlaut „Fernmeldegeheimnis“ zunächst nicht entgegen. Er erlaubt die Auslegung, dass das „Geheimnis“ auch das Vertragsverhältnis umfassen soll, welches den einzelnen Fernmeldevorgängen zugrunde liegt.

Für eine Einbeziehung von Bestandsdaten in den Schutzbereich des Art. 10 GG spricht, dass die Information, welcher Anbieter für die Telekommunikation genutzt wird und wie das Vertragsverhältnis zu diesem Anbieter ausgestaltet ist, die im Rahmen dieses Vertragsverhältnisses abgewickelten Kommunikationsvorgänge inhaltlich näher beschreibt und damit einen näheren Umstand der einzelnen Kommunikationsvorgänge darstellt[6]. Dass das Fernmeldegeheimnis für die näheren Umstände einzelner Kommunikationsvorgänge gilt, ist anerkannt. Bestandsdaten unterscheiden sich von Verbindungsdaten nur dadurch, dass sie die Umstände von Kommunikationsvorgängen stets in gleicher Weise wiedergeben, während sich Verbindungsdaten typischerweise von Verbindung zu Verbindung ändern. Dass darin kein relevanter Unterschied liegt, zeigt aber das Beispiel der Internetnutzung. Während manche Internet-Access-Provider dem Nutzer eine IP-Adresse fest zuweisen (dann Bestandsdatum), teilen andere Dienste dem Nutzer für jede Verbindung eine andere IP-Adresse zu (dann Verbindungsdatum). Solche Zufälligkeiten können für die Bestimmung des Schutzbereichs des Fernmeldegeheimnisses richtigerweise keine Rolle spielen.

Darüber hinaus lässt sich aus der Information, dass eine Person Kunde eines Kommunikationsmittlers ist, regelmäßig schließen, dass der jeweilige Dienst auch in Anspruch genommen wird. Bereits die Tatsache, dass sich jemand des Mediums der Telekommunikation bedient, fällt als „Ob“ der Telekommunikation nach der Definition des Bundesverfassungsgerichts in den Schutzbereich des Art. 10 GG, wenn das Gericht feststellt, zu den Kommunikationsumständen gehöre „insbesondere, ob, wann und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat“[7]. Diese Definition ist bereits ihrem Wortlaut nach nicht auf einzelne Telekommunikationsvorgänge beschränkt.

Hinzu kommt, dass die Kenntnis von Bestandsdaten oftmals Vorbedingung für den staatlichen Zugriff auf einzelne Kommunikationsvorgänge ist. Anbieter von Telekommunikationsdiensten müssen beispielsweise immer auf Bestandsdaten zurück greifen, um dem Staat Auskunft darüber erteilen zu können, welche Personen an einem Kommunikationsvorgang beteiligt waren. In den Aufzeichnungen der Anbieter über einzelne Kommunikationsvorgänge ist nämlich regelmäßig nur ein technisches Merkmal zur Identifizierung der Kunden gespeichert (beispielsweise deren Rufnummer), nicht aber auch deren Name und Anschrift. Auch dieser Zusammenhang spricht dafür, Bestandsdaten in den Schutz des Fernmeldegeheimnisses einzubeziehen.

Schließlich ist der Schutzzweck des Fernmeldegeheimnisses zu beachten, nämlich die an der Telekommunikation Beteiligten so zu stellen, wie sie bei unmittelbarer Kommunikation miteinander stünden[8]. Im Falle der unmittelbaren Kommunikation gäbe es keine

---

[5] Dafür, soweit Bestandsdaten eine staatliche Überwachung ermöglichen AK-GG-Bizer, Art. 10 Rn. 71; dagegen OVG Münster, MMR 2002, 563 (564); Schaar, Sicherheit und Freiheitsrechte, www.peter-schaar.de/schutzkonzepte.pdf, 21; Kooperationskreis „IuK-Datenschutz“, in: Garstka, Jahresbericht 1998, www.datenschutz-berlin.de/jahresbe/98/teil5.htm, unter 5.3 sowie die h.M.

[6] A.A. ohne Begründung Wuermeling/Felixberger, CR 97, 230 (234).

[7] BVerfGE 100, 313 (358).

[8] BVerfGE 85, 386 (396); BVerfGE 100, 313 (363); Gusy, JuS 86, 89 (90 f.); vgl. auch Dreier-Hermes, Art. 10 Rn. 47.

Alle Rechte vorbehalten – Keine Vervielfältigung oder Verbreitung ohne ausdrückliche Einwilligung des Autors

Vertragsverhältnisse zu einem Kommunikationsmittler, in deren Rahmen personenbezogene Daten über die an der Kommunikation Beteiligten gespeichert würden. Insoweit realisiert sich das spezifische Risiko für die Vertraulichkeit der Telekommunikation, das mit der Inanspruchnahme von Telekommunikationsdiensten verbunden ist, in der Speicherung von Bestandsdaten bei Kommunikationsmittlern. Bestandsdaten über das Vertragsverhältnis mit Kommunikationsmittlern sind daher nicht nur durch das Recht auf informationelle Selbstbestimmung sondern auch durch das Fernmeldegeheimnis geschützt.

Der staatliche Zugriff auf Bestandsdaten

Konsequenz daraus ist zunächst, dass in den Normen, die den staatlichen Zugriff auf Bestandsdaten regeln (§§ 89 Abs. 6, 90 TKG und §§ 107-108 TKG-RefE), Art. 10 GG zu zitieren ist. Darüber hinaus sollte die grundsätzliche Gleichstellung der Bestandsdaten mit Verbindungsdaten Anlass geben, die Verhältnismäßigkeit des bisher ohne Eingriffsschwelle zulässigen Zugriffs auf Bestandsdaten zu überprüfen. Die genannten Vorschriften verpflichten Telekommunikationsanbieter bisher zur Auskunfterteilung über Bestandsdaten zur Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung und zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes. Daneben dürfen folgende Stellen kostenfrei im Wege eines weltweit einzigartigen[9] automatischen Online-Abrufverfahrens auf Bestandsdaten zugreifen: Gerichte, Staatsanwaltschaften, andere Justizbehörden, sonstige Strafverfolgungsbehörden, Polizeien des Bundes und der Länder für Zwecke der Gefahrenabwehr, Zollfahndungsämter für Zwecke von Strafverfahren, das Zollkriminalamt zur Vorbereitung und Durchführung von Abhörmaßnahmen, die Verfassungsschutzbehörden des Bundes und der Länder, der Militärischen Abschirmdienst sowie der Bundesnachrichtendienst zur Wahrnehmung sämtlicher ihrer Aufgaben. § 108 TKG-RefE will dieser Liste Einrichtungen, die Notrufe bearbeiten, die Bundesanstalt für Finanzdienstleistungsaufsicht und die für die Verfolgung und Ahndung von Schwarzarbeit zuständigen Behörden hinzufügen.

Die praktische Relevanz des staatlichen Zugriffs auf Bestandsdaten wird nicht nur an der Aufzählung der berechtigten Stellen sondern zahlenmäßig auch daran deutlich, dass im Jahr 2002 etwa 2 Mio. Zugriffe im Wege des automatischen Abrufverfahrens erfolgten[10]. Seit dem Jahr 2000 hat sich die Anzahl der Zugriffe jedes Jahr um 50% Jahr erhöht[11]. Da jede Abfrage eine Vielzahl von Datensätzen umfassen kann, ist die Wahrscheinlichkeit, dass an einem beliebigen Tag auf die Bestandsdaten eines beliebigen Bürgers zugegriffen wird, hoch. Diese Wahrscheinlichkeit wird weiter erhöht durch § 108 Abs. 1 S. 4 TKG-RefE, der die Verwendung von Jokerzeichen bei Online-Abfragen erlauben soll. Die Sicherheitsbehörden dürften danach also beispielsweise den Namen, die Adresse und das Geburtsdatum aller Anschlussinhaber, die in einer bestimmten Straße wohnen, abrufen.

Der staatliche Zugriff auf Telekommunikations-Bestandsdaten kann allenfalls insoweit relativ unproblematisch sein, wie er erforderlich ist, um zur Durchführung von Maßnahmen der Telekommunikationsüberwachung nach den §§ 100a, 100g StPO, nach dem G10 oder dem AWG das Unternehmen ausfindig zu machen, über welches die Zielperson ihre Telekommunikation abwickelt[12]. Wenn der staatliche Zugriff auf Kommunikationsinhalte und Verbindungsdaten zulässig ist, dann ist es auch der vorbereitende Zugriff auf Bestandsdaten.

Die §§ 89 Abs. 6, 90 TKG bzw. §§ 107-108 TKG-RefE beschränken den Zugriff jedoch keineswegs auf Fälle der Telekommunikationsüberwachung. Sie erlauben die Anforderung von

---

[9] Berliner Kommentar-Groß, Art. 10 Rn. 36.

[10] BfD, 19. Tätigkeitsbericht (2001-2002), 79, www.bfd.bund.de/information/19tb0102.pdf.

[11] BfD, 19. Tätigkeitsbericht (2001-2002), 79, www.bfd.bund.de/information/19tb0102.pdf.

[12] Ähnlich BfD, Info 5, www.bfd.bund.de/information/info5/kap04/04_06_01.html: „Daten, die keinen spezifischen Telekommunikationsbezug haben, dürfen nach Auffassung des Bundesbeauftragten für den Datenschutz nicht abgefragt werden“; Kooperationskreis „IuK-Datenschutz“, in: Garstka, Jahresbericht 1998, unter 5.2.

Alle Rechte vorbehalten – Keine Vervielfältigung oder Verbreitung ohne ausdrückliche Einwilligung des Autors

Bestandsdaten vielmehr sogar zur Verfolgung von Ordnungswidrigkeiten, zu deren Ahndung eine Telekommunikationsüberwachung in keinem Fall zulässig ist. Die Bestandsdaten von Telekommunikationsunternehmen dürfen demnach von den oben aufgeführten Behörden ohne jeden Telekommunikationsbezug als eine Art bundesweites Adressregister missbraucht werden, was für die berechtigten Behörden einen Zugriff auf Einwohnermeldedaten entbehrlich macht. Insoweit existiert nicht einmal eine Subsidiaritätsklausel. Mit dem Argument, durch die Auskunftspflicht solle nur der bis 1996 durch die Bundespost im Wege der Amtshilfe gewährte Zugriff auf Bestandsdaten fortgeschrieben werden[13], übersah der Gesetzgeber des TKG, dass Art. 10 GG und das Recht auf informationelle Selbstbestimmung schon immer amtshilfefest waren[14], so dass die damalige Amtshilfe durch die Bundespost mangels gesetzlicher Grundlage verfassungswidrig war.

Die obige Darstellung zeigt, dass Bestandsdaten nicht generell mehr oder weniger schutzwürdig als Kommunikationsinhalte oder sonstige Kommunikationsumstände sind, dass die Unterscheidung von Bestandsdaten also nur technischer Art sein kann. Entsprechend ihrer hohen Schutzwürdigkeit stellt beispielsweise das englische Recht Bestandsdaten den Telekommunikations-Verkehrsdaten gleich und unterwirft sämtliche dieser „Kommunikationsdaten“ („communications data“) den gleichen Schutzmechanismen[15]. Dasselbe gilt für Österreich und Finnland[16]. Gemäß den Art. 2 Abs. 1, Art. 1 Abs. 2 GG und Art. 10 GG ist auch in Deutschland eine Gleichstellung geboten, so dass zumindest die §§ 100g, 100h StPO als Vergleichsmaßstab heranzuziehen sind. Der lange Katalog berechtigter Stellen in den §§ 89 Abs. 6, 90 TKG bzw. §§ 107-108 TKG-RefE sowie die gänzlich fehlende Eingriffsschwelle wird der besonderen Sensibilität von Bestandsdaten nicht gerecht und ist daher mit den genannten Grundrechten in Verbindung mit dem Verhältnismäßigkeitsprinzip unvereinbar. Der Zugriff auf Bestandsdaten darf nur zur Abwehr dringender Gefahren für wichtige Rechtsgüter sowie zur Verfolgung schwerer Straftaten zugelassen werden.

Im Hinblick auf Art. 3 Abs. 1 GG stellt sich außerdem die Frage, ob es zu rechtfertigen ist, dass eine Auskunftspflicht über Bestandsdaten alleine für Telekommunikationsunternehmen, nicht aber beispielsweise für Banken oder Stromversorgungsunternehmen vorgesehen werden soll. Weder sind Telekommunikations-Bestandsdaten weniger sensibel als sonstige Bestandsdaten, noch sind sie für die staatliche Aufgabenwahrnehmung nützlicher. Letzteres gilt jedenfalls außerhalb der Bereichs der Vorbereitung von Maßnahmen der Telekommunikationsüberwachung. Während im Bereich der Telekommunikationsüberwachung mit besonderen Gefahren des freien Informationsaustauschs mittels Telekommunikation argumentiert werden könnte, ist diese Argumentation ausgeschlossen, wo jeder Zusammenhang mit Telekommunikation fehlt und Bestandsdaten als allgemeines Adressregister missbraucht werden. Jedenfalls außerhalb des Bereichs der Telekommunikationsüberwachung existieren daher keine Gründe von solcher Art und solchem Gewicht, dass sie eine Diskriminierung der Telekommunikationsbenutzung gegenüber sonstigen Vertragsverhältnissen rechtfertigen könnten, so dass eine auf Telekommunikationsunternehmen beschränkte Auskunftspflicht über Bestandsdaten mit Art. 3 Abs. 1 GG unvereinbar ist.

In den §§ 89 Abs. 6, 90 TKG bzw. §§ 107-108 TKG-RefE fehlt im Übrigen die verfassungsrechtlich gebotene Anordnung, dass die Verwendung erlangter Daten nur zur Verfolgung derjenigen Zwecke zulässig ist, zu deren Erreichung die Daten nach dem Gesetz erhoben werden durften (Zweckbindungsgebot)[17]. Eine darüber hinaus gehende Verwendung

---

[13] Bundesregierung, BT-Drs. 13/3609, 55.

[14] Enderle, MMR 2002, 565 (565); vgl. BVerfGE 65, 1 (46).

[15] Queen Mary (University of London), Studie über Netzkriminalität, http://europa.eu.int/ISPO/eif/-InternetPoliciesSite/Crime/Study2000/Report.html, wo ein vergleichbares Schutzniveau für Bestandsdaten, Verkehrsdaten und Inhalten gefordert wird.

[16] EU-Questionnaire, www.statewatch.org/news/2002/nov/euintercept-2002-11-20.html.

[17] BVerfGE 65, 1 (46).

Alle Rechte vorbehalten – Keine Vervielfältigung oder Verbreitung ohne ausdrückliche Einwilligung des Autors

ist nur aufgrund einer normenklaren gesetzlichen Ermächtigung zulässig[18]. Außerdem fehlt es an der verfassungsrechtlich gebotenen Anordnung der Protokollierung jeder Erhebung, Verwendung, Übermittlung und Vernichtung von Telekommunikations-Bestandsdaten[19].

Verfassungsrechtlich geboten ist es auch, eine Benachrichtigung der Betroffenen von Eingriffen sicherzustellen[20]. Von dem Grundsatz der Benachrichtigungspflicht abweichende Regelungen sind zwar im Rahmen der Verhältnismäßigkeit zulässig[21]. Unverhältnismäßig ist ein Ausschluss der Benachrichtigung aber jedenfalls dann, wenn die Benachrichtigung den Zweck der Maßnahme nicht mehr gefährden kann[22]. Dass eine unüberschaubare Vielzahl von Personen betroffen ist und eine Benachrichtigung daher unpraktikabel wäre, kann den Ausschluss einer Benachrichtigung allenfalls dann rechtfertigen, wenn die Daten sofort nach ihrer Erhebung als irrelevant vernichtet werden, ohne verwendet worden zu sein[23]. Ansonsten müssen Wege gefunden werden, um Massenbenachrichtigungen praktikabel und kostengünstig zu machen. Beispielsweise ist an eine Benachrichtigung auf der Telefonrechnung des Betroffenen oder per Email an eine von diesem angegebene Emailadresse zu denken.

Darüber hinaus sehen die §§ 89 Abs. 6, 90 TKG bzw. §§ 107-108 TKG-RefE keinerlei Evaluierungsregelungen vor. Während Erkenntnisse über die Effektivität der Befugnisse möglicherweise noch im Wege repräsentativer Teiluntersuchungen gewonnen werden können, lässt sich die Belastungswirkung der Befugnisse nur einschätzen, wenn eine Statistik über die Anzahl von Anfragen sowie über die Anzahl der jeweils betroffenen Bestandsdatensätze geführt wird. Da die Kenntnis dieser Daten für die Beurteilung der Verhältnismäßigkeit der §§ 89 Abs. 6, 90 TKG bzw. §§ 107-108 TKG-RefE erforderlich ist, ist die Erstellung einer solchen Statistik verfassungsmäßig geboten.

Vorratsspeicherung von Bestandsdaten

§ 106 TKG-RefE soll nunmehr eindeutig die Frage regeln, ob sich Telekommunikationsnutzer gegenüber dem Telekommunikationsunternehmen auch dann identifizieren müssen, wenn dies für die Erbringung des Telekommunikationsdienstes nicht erforderlich ist (z.B. bei vorausbezahlten Mobiltelefonkarten). Die gesetzliche Klarstellung gegenüber § 90 TKG ist zu begrüßen und verfassungsrechtlich geboten. Seiner inhaltlichen Ausgestaltung nach ist § 106 TKG-RefE jedoch höchst problematisch, weil er eine allgemeine Identifizierungspflicht mit anschließender Vorratsspeicherung vorsieht. Anbieter von Telekommunikationsdiensten für die Öffentlichkeit, die Rufnummern vergeben, sollen § 106 TKG-RefE zufolge nämlich vor Freischaltung des Dienstes die Rufnummer, den Namen, die Anschrift und das Geburtsdatum des Rufnummerninhabers erheben und speichern. Diese Daten sollen bis ein Jahr nach Vertragsende für staatliche Abrufe bereit gehalten werden. § 90 Abs. 3 TKG-RefE verpflichtet auch andere Anbieter von Telekommunikationsdiensten, etwa erfasste Bestandsdaten bis ein Jahr nach Vertragsende aufzubewahren.

Abgesehen von Sondergebieten wie dem Bereich finanzieller Transaktionen (Geldwäschegesetz) ist eine staatlich angeordnete Identifizierungspflicht im deutschen Recht bisher einmalig. In Verbindung mit den oben beschriebenen, breiten staatlichen Zugriffsrechten auf die erfassten Kundendaten stellt § 106 TKG-RefE einen einzigartigen Präzedenzfall vorsorglicher staatlicher Überwachung der Bürger dar. Verfassungsrechtlich ist die in § 106 TKG-RefE vorgesehene Datenerfassung und -speicherung durch Telekommunikationsunternehmen als staatlicher Grundrechtseingriff anzusehen, weil sie

[18] Dazu BVerfGE 65, 1 (62 f.).
[19] Vgl. BVerfGE 100, 313 (395 f.).
[20] BVerfGE 30, 1 (31); BVerfGE 100, 313 (361).
[21] BVerfGE 100, 313 (361).
[22] BVerfGE 100, 313 (361).
[23] BVerfGE 100, 313 (397 ff.).

Alle Rechte vorbehalten – Keine Vervielfältigung oder Verbreitung ohne ausdrückliche Einwilligung des Autors

hoheitlich angeordnet ist und den Unternehmen dabei kein Handlungsspielraum zur Verfügung steht[24]. § 106 TKG-RefE muss sich daher an dem Verhältnismäßigkeitsprinzip messen lassen.

Bisher liegen keinerlei empirische Erkenntnisse bezüglich der Frage vor, in welchem Maße eine Identifizierungspflicht zur Erreichung der damit verfolgten Ziele geeignet ist[25]. Zwar ist bekannt, dass Straftäter heutzutage verbreitet anonym gekaufte, vorausbezahlte Mobiltelefonkarten einsetzen, um einer Überwachung ihrer Telekommunikation zu entgehen[26]. Gerade bei ernsthaften und daher wirklich gefährlichen Kriminellen erscheint es aber naiv, anzunehmen, dass diese durch eine Identifizierungspflicht dazu bewegt werden könnten, bei dem Kauf von Karten für ihr „Arbeitshandy" brav ihre persönlichen Daten anzugeben.

Guthabenkarten lassen sich vielmehr ohne Weiteres privat handeln und weitergeben[27]. Anbieter von Mobiltelefonie schätzen, dass schon heute etwa 50% aller Prepaid-Karten innerhalb eines Jahres weitergegeben werden[28]. § 106 TKG-RefE sieht eine Identifizierungspflicht nur für Telekommunikationsanbieter und ihre Vertriebspartner vor, nicht aber für private Gelegenheitsverkäufer von Guthabenkarten. Dies trägt der Tatsache Rechnung, dass eine Identifizierungspflicht bei oder gar ein Verbot von Privatverkäufen nicht durchsetzbar wäre. Die Folge davon ist aber, dass Kriminelle auch nach Einführung des § 106 TKG-RefE Guthabenkarten ohne Weiteres privat erwerben könnten, ohne sich identifizieren zu müssen. Die Identifizierungspflicht liefe damit leer.

In Frankreich, wo eine Identifizierungspflicht für den Kauf von Guthabenkarten bereits besteht, hat man die Erfahrung gemacht, dass erfasste Daten nicht selten unzutreffend sind[29]. In der Tat haben Kriminelle ohne Weiteres die Möglichkeit, sich Händler auszusuchen, die es mit der Identifizierung nicht allzu genau nehmen. Es gibt keine praktikable Möglichkeit, dies zu verhindern. Das Gleiche gilt für die fortbestehende Möglichkeit der Nutzung anonym im Ausland gekaufter Guthabenkarten in Deutschland („Roaming"). Jedenfalls in Anbetracht der gegenwärtigen Erkenntnisse lässt sich daher nicht vertretbarerweise behaupten, dass eine Identifizierungspflicht einen nennenswerten Beitrag zur Bekämpfung ernsthafter Kriminalität leisten könnte. Ein Nutzen der Maßnahme ist allenfalls in Bezug auf Unbedarfte zu erwarten, also im Bereich von Kleinkriminalität und Ordnungswidrigkeiten.

Demgegenüber belastet eine Identifizierungspflicht unbescholtene Bürger in ganz erheblichem Maße, weil diesen eine anonyme Telekommunikationsnutzung in weiten Bereichen unmöglich gemacht würde. Bisher konnten Personen wie Journalisten, die staatliche Missstände recherchierten, Organisatoren staatskritischer Demonstrationen oder Vertreter von Wirtschaftsunternehmen, die Wirtschaftsspionage befürchteten, durch die Benutzung vorausbezahlter Mobiltelefonkarten anonym telefonieren. Ein Identifizierungszwang könnte dagegen zur Folge haben, dass auf den Austausch sensibler Informationen mittels Telekommunikation zunehmend verzichtet würde. Damit drohen Beeinträchtigungen der gesamtgesellschaftlichen Kommunikation und, wo es sich um politische Kommunikation handelt, auch eine Beeinträchtigung der Funktionsfähigkeit unseres demokratischen Systems. Auf dem Gebiet der Verschlüsselung hat die Politik erkannt, dass die Gewährleistung der Vertraulichkeit der Telekommunikation wichtiger ist als die marginalen Sicherheitsgewinne, die eine Kryptoregulierung bestenfalls bewirken könnte. Nicht anders verhält es sich in Bezug auf die Möglichkeiten anonymer Telekommunikation.

---

[24] Vgl. BVerfG, 1 BvR 330/96 vom 12.3.2003, Absatz-Nr. 50, www.bverfg.de/entscheidungen/-rs20030312_1bvr033096.html.

[25] Entschließung zwischen der 63. und 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24.05.2002, www.datenschutz-berlin.de/doc/de/konf/sonst/02indenttele.htm.

[26] Heise Newsticker, IMSI-Catcher zur Mobilfunküberwachung bald legal, www.heise.de/newsticker/data/-hod-30.11.01-000/.

[27] Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 24.05.2002 (Fn. 25).

[28] BMWi-Ressortarbeitsgruppe, Eckpunkte zur Anpassung der Regelungen des § 90 TKG, 28.03.2002, 7, www.almeprom.de/fiff/material/Eckpunkte_90_TKG_Prepaid.pdf.

[29] BMWi-Ressortarbeitsgruppe, Eckpunkte (Fn. 28), 4 f.

Alle Rechte vorbehalten – Keine Vervielfältigung oder Verbreitung ohne ausdrückliche Einwilligung des Autors

Angesichts dessen liegt es auf der Hand, dass der mögliche Nutzen einer Identifizierungspflicht von Telekommunikationsnutzern außer Verhältnis zu den damit verbundenen Nachteilen steht. Eine Vorratsspeicherung von Telekommunikations-Bestandsdaten wäre also unverhältnismäßig[30]; eine derart weitgehende Registrierung der Bürger aus dem Bestreben nach möglichst großer Effektivität der Polizeigewalt und Erleichterung der polizeilichen Überwachung der Bevölkerung widerspräche den Prinzipien des freiheitlichen Rechtsstaates[31]. § 106 TKG-RefE ist daher mit den Art. 2 Abs. 1, Art. 1 Abs. 2 GG und mit Art. 10 GG unvereinbar. Die außerdem drohenden Belastungen für die Wirtschaft – beispielsweise müssten ganze Vertriebskanäle wie der Kartenvertrieb mittels Automaten eingestellt werden – seien nur kurz erwähnt. Es ist nicht einmal klar, ob § 106 TKG-RefE noch den Betrieb öffentlicher Telefonzellen, die über eine Rufnummer erreichbar sind, zuließe.

Die konkrete Ausformung der Identifizierungspflicht in § 106 TKG-RefE verstärkt die allgemeine Unangemessenheit einer solchen Regelung. § 106 TKG-RefE schreibt nämlich nicht vor, dass die Angaben von Kunden bezüglich ihrer persönlichen Daten überprüft werden müssen. Eine Nachprüfung der Angaben anhand eines Ausweisdokuments, wie es eine Entscheidung des OVG Münster[32] und ein Kabinettsbeschluss aus dem Jahr 2002[33] noch vorsahen, schreibt § 106 TKG-RefE nicht mehr vor. Vielmehr soll es nach § 90 Abs. 4 TKG-RefE den Anbietern überlassen bleiben, ob sie sich einen Ausweis vorzeigen lassen oder nicht. Müssen die von Kunden angegebenen persönlichen Daten demnach in keiner Weise überprüft werden, dann ist die „Identifizierungspflicht" des § 106 TKG-RefE ohnehin Makulatur. Daneben ermöglicht es § 106 Abs. 3 TKG-RefE, Altverträge auf unbegrenzte Zeit identifizierungsfrei fortzuführen. Auf diese Weise wird eine weitere Umgehungsmöglichkeit eröffnet.

Unter dem Aspekt des Art. 3 Abs. 1 GG ist schließlich zu beachten, dass sich mangels empirischer Anhaltspunkte derzeit nicht vertretbarerweise behaupten lässt, dass die Benutzung von Telekommunikationsnetzen gefahrenträchtiger als sonstige Alltagshandlungen sei, oder dass Telekommunikations-Bestandsdaten für die Gefahrenabwehr oder Strafverfolgung nützlicher seien als Daten über beliebige andere Vertragsverhältnisse. Dass sich eine Vorratsspeicherung von Bestandsdaten nur auf dem Gebiet der Telekommunikation finanziell günstig realisieren lassen mag, kann die gravierende Ungleichbehandlung der Telekommunikationsbenutzung gegenüber der Inanspruchnahme sonstiger Leistungen nicht rechtfertigen, so dass § 106 TKG-RefE auch mit Art. 3 Abs. 1 GG unvereinbar ist.

Zugriff durch Beschlagnahme und Rasterfahndung

§ 85 Abs. 3 S. 3 TKG sieht bisher vor, dass Anbieter von Telekommunikationsdiensten Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur aufgrund solchen gesetzlichen Vorschriften weitergeben dürfen, die sich ausdrücklich auf Telekommunikationsvorgänge beziehen. Diese Regelung gewährleistet, dass das Fernmeldegeheimnis durch allgemeine Auskunftsrechte und -pflichten nicht durchbrochen werden kann. Damit wird der hohen Bedeutung der Telekommunikation für die freie Kommunikation in unserer Gesellschaft Rechnung getragen.

§ 85 Abs. 3 S. 3 Hs. 2 TKG-RefE soll nun eine Ausnahme von diesem einfachgesetzlichen Zitiergebot für die strafprozessuale Beschlagnahme von Gegenständen (§§ 94-98 StPO) und für die strafprozessuale Rasterfahndung (§§ 98a, 98b StPO) schaffen. Aufgrund der §§ 94, 98a StPO sollen also Eingriffe in das Fernmeldegeheimnis zulässig sein (z.B. durch Beschlagnahme einer Festplatte mit Telekommunikations-Bestandsdaten), obwohl diese Normen keinerlei Bezug zu Telekommunikationsvorgängen aufweisen. Bereits aus diesem mangelnden Bezug

[30] Ebenso Schaar, Forderungen an Politik und Gesetzgebung, www.peter-schaar.de/FES-statement.pdf; GDD, Stellungnahme zum Entwurf für Änderungen der §§ 89, 90 und 96 TKG, www.gdd.de/pdf/ak-stellTKG.pdf.

[31] Vgl. BVerwGE 26, 169 (170).

[32] OVG Münster, MMR 2002, 563 (563).

[33] Kabinettbeschluss des Bundesregierung vom 17.04.2002, www.dud.de/dud/documents/tkg-aend-e-020417.pdf.

Alle Rechte vorbehalten – Keine Vervielfältigung oder Verbreitung ohne ausdrückliche Einwilligung des Autors

ergibt sich, dass der Gesetzgeber bei Beschluss dieser Regelungen die Möglichkeit von Eingriffen in das Fernmeldegeheimnis nicht berücksichtigt hat. Dementsprechend sehen die §§ 94, 98a StPO auch nicht die bei Eingriffen in das Fernmeldegeheimnis von Verfassungs wegen gebotenen verfahrensrechtlichen Grundrechtssicherungen[34] (z.B. Benachrichtigungspflicht, Protokollierungspflicht) vor.

Normalerweise gewährleistet das Zitiergebot des Art. 19 Abs. 1 S. 2 GG, dass Grundrechtsbeschränkungen nur insoweit gelten, wie sich der Gesetzgeber ihrer Tragweite bewusst war. Das Zitiergebot gilt aber nicht für vorkonstitutionelles Recht[35] wie es die Regelungen über die Beschlagnahme darstellen. Aus diesem Grund steht Art. 19 Abs. 1 S. 2 GG nur einer Rasterfahndung (§ 98a StPO) unter Zuhilfenahme von Telekommunikationsdaten entgegen. Diesen Mangel kann der Gesetzgeber nur durch ein Zitat des Art. 10 GG in § 98a StPO beheben.

Fraglich ist, ob eine Ausweitung der §§ 94, 98a StPO auf Tatsachen, die dem Fernmeldegeheimnis unterliegen, mit den Grundrechten vereinbar ist. Wegen des hohen verfassungsrechtlichen Stellenwerts einer unbefangenen Telekommunikation sind strafprozessuale Eingriffe in das Fernmeldegeheimnis nur zur Verfolgung von Straftaten erheblicher Bedeutung verhältnismäßig[36]. Während die §§ 100a, 100g StPO dies berücksichtigen und auch § 98a StPO dieser Anforderung gerecht würde, kann eine Beschlagnahme prinzipiell wegen jeder Bagatellstraftat angeordnet werden. Auch in Bezug auf die übrigen Eingriffsvoraussetzungen, die verfahrensrechtlichen Sicherungen und die Möglichkeiten der Verwendung erlangter Kenntnisse bleiben die §§ 94, 98a StPO teilweise erheblich hinter den §§ 100a, 100g StPO zurück. Eine Ausdehnung der §§ 94, 98a StPO auf Tatsachen, die dem Fernmeldegeheimnis unterliegen, ist daher mit Art. 10 GG in Verbindung mit dem Verhältnismäßigkeitsprinzip unvereinbar. Auch im Hinblick auf Art. 3 Abs. 1 GG ist kein sachlicher Grund ersichtlich, der eine Umgehung der Voraussetzungen der §§ 100a, 100g StPO in Fällen der Beschlagnahme und der Rasterfahndung rechtfertigen könnte. Ein Zugriff auf Telekommunikationsdaten im Wege der §§ 94, 98a StPO erscheint vielmehr nur bei Vorliegen der Voraussetzungen der §§ 100a, 100g StPO gerechtfertigt.

Hintergrund

Auch wenn die Befürwortung eines breiten staatlichen Zugriffs auf Telekommunikations-Bestandsdaten in guter Absicht erfolgen mag, darf nicht außer Acht gelassen werden, dass die damit verbundenen, für sich genommen vielleicht harmlos erscheinenden Grundrechtseingriffe nur einen kleinen Bestandteil der gesamten staatlichen Überwachungsbefugnisse darstellen, deren Umfang in den letzten Jahren stetig gestiegen ist. Diese Entwicklung steht im Widerspruch zu dem historisch gewachsenen Grundgedanken unseres Rechtsstaats, demzufolge die Gewährleistung von Sicherheit um jeden Preis nicht in unserem Interesse liegt. Das Bestreben nach immer mehr Sicherheit vor den verschiedensten Risiken des täglichen Lebens führt vielmehr letztendlich zu unbegrenzten Befugnissen der Staatsmacht. Dies aber würde das Ende der Freiheit und Sicherheit bedeuten, mit deren Schutz die Eingriffsbefugnisse begründet wurden. Das Leben in Polizeistaaten ist noch nie sicherer gewesen als das Leben in demokratischen Rechtsstaaten. Benjamin Franklin warnte daher zurecht davor, dass Bürger, die immer mehr Sicherheit auf Kosten der Freiheit gewinnen wollten, am Ende beides verlieren würden.

Patrick Breyer

Dieser Beitrag wurde veröffentlicht in RDV (Recht der Datenverarbeitung) 2003, S. 218-222.

[34] BVerfGE 100, 313 (359 ff.).

[35] BVerfGE 2, 121 (122 f.); BVerfGE 5, 13 (16).

[36] BVerfG, 1 BvR 330/96 vom 12.3.2003, Absatz-Nr. 75, www.bverfg.de/entscheidungen/-rs20030312_1bvr033096.html.

Alle Rechte vorbehalten – Keine Vervielfältigung oder Verbreitung ohne ausdrückliche Einwilligung des Autors