Univ.-Prof. Dr. Dieter Kugelmann

Leiter des Fachgebietes Öffentliches Recht mit Schwerpunkt Polizeirecht einschließlich des internationalen Rechts und des Europarechts

Deutsche Hochschule der Polizei
Zum Roten Berge 18 - 24
D-48165 Münster

Tel.: 02501/806-437
Sekretariat: 02501/806-279
E-mail: Dieter.Kugelmann@dhpol.de

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)680 E neu

Stellungnahme

zur Anhörung vor dem Innenausschuss des Deutschen Bundestages

zu dem

Entwurf eines Gesetzes zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft

BT Drs. 17/12034

1. Das Ziel

Mit dem Gesetzentwurf kommt der Gesetzgeber einer Vorgabe des Bundesverfassungsgerichts nach, das in seinem Beschluss vom 24. Januar 2012 (1 BvR 1299/05) einige Regelungen des TKG verfassungskonform ausgelegt und andere für verfassungswidrig erklärt hat. Die weitere Anwendbarkeit hat es für eine Übergangszeit bis längstens zum 30. Juni 2013 zugestanden. Die Neuregelungen des Gesetzentwurfes sollen diese Regelungen konkretisieren und normenklar erneuern.

Als unmittelbare Reaktion auf das Urteil des Bundesverfassungsgerichts vollzieht der Gesetzentwurf überwiegend die verfassungsgerichtlichen Vorgaben nach. Neue Befugnisse sollen nicht geschaffen werden. In der

Bewertung ist den verfassungsgerichtlichen Vorgaben damit besonders Rechnung zu tragen. Einige Bestandteile des Gesetzentwurfes tragen eigenständigeren Charakter. Sie sind in den verfassungsrechtlichen Zusammenhang einzubetten und weiter gehend zu würdigen.

2. Systematik und verfassungsrechtliche Grundzüge in Ansehung des Urteils des Bundesverfassungsgerichts vom 24.01.2012

Der Entwurf enthält nicht nur Änderungen des TKG, sondern auch einer Reihe von Sicherheitsgesetzen des Bundes. Die neuen Regelungen sollen den Zugriff auf die Bestandsdaten nach TKG eröffnen. Systematisch handelt es sich um ein zweistufiges Verfahren. Die Erhebung der Daten durch den Telekommunikationsdienstleister richtet sich nach dem TKG, das auch den Auskunftsanspruch gegen ihn festlegt; der Abruf durch die Sicherheitsbehörden richtet sich nach den Sicherheitsgesetzen. Dieser Abruf stellt für die Sicherheitsbehörde eine eigene Datenerhebung dar und damit einen zu rechtfertigenden Grundrechtseingriff. Die Regelung des Abrufs obliegt den zuständigen Gesetzgebern in Bund und Ländern nach der Kompetenzordnung des Grundgesetzes (Art. 70 ff. GG).

Das Bundesverfassungsgericht hat entschieden, dass die Zuordnung von Telekommunikationsnummern zu ihren Anschlussinhabern einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und qualifizierter Rechtsgrundlagen bedarf (BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Abs.Nr. 121 ff.). Dies soll auch für Daten der Zugangssicherung gelten (PIN usw.).
Die Zuordnung dynamischer IP-Adressen greift dagegen in Art. 10 GG ein, denn die Telekommunikationsunternehmen müssen insoweit auf Verbindungsdaten zurückgreifen und damit auf den Vorgang der Telekommunikation, wodurch der Schutzbereich des Art. 10 GG eröffnet wird (BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Abs.Nr. 116).

Der § 113 Abs. 1 Satz 1 TKG war nach Ansicht des Bundesverfassungsgerichts verfassungskonform auszulegen, also nicht per se verfassungswidrig. Die Änderungsvorschläge des Gesetzentwurfes greifen die Vorgaben des Bundesverfassungsgerichts auf. Das Bundesverfassungsgericht fordert in ihrer Reichweite begrenzende, spezifische Eingriffsschwellen, deren Ausformung in der alten Regelung es als „noch hinnehmbar“ bezeichnet (BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Abs.Nr. 176, 178).

Die alte Regelung des § 113 Abs. 1 Satz 2 TKG betreffend Daten über Schutzvorkehrungen, insbesondere PIN und PUK, wurde in ihrer Ausgestaltung als inkonsistent gesehen. Einen solchen Abruf von Daten der Zugangssicherung hält das Bundesverfassungsgericht für möglich, aber nur dann, wenn auch die Voraussetzungen für eine Nutzung der Daten vorliegen (BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Abs.Nr. 182, 185). Diesen eher systematischen Bedenken kann in der Neuregelung durch gesetzgeberische Umgestaltungen Rechnung getragen werden. Das Erfordernis angemessener Eingriffsschwellen ist in den Fachgesetzen hinreichend zu berücksichtigen.

Die Zuordnung von dynamischen IP-Adressen stellt für den Gesetzentwurf insoweit einen weit reichenden Regelungsgegenstand dar, als ein Eingriff in Art. 10 GG vorliegt und damit nicht nur eine hinreichend klare Regelung erforderlich ist, sondern auch den Rechtfertigungsanforderungen an Eingriffe in das Telekommunikationsgeheimnis Rechnung getragen werden muss.

Der Kernbereich privater Lebensgestaltung muss vom einschlägigen Fachrecht geschützt werden. Aus der verfassungsgerichtlichen Rechtsprechung folgen Anforderungen, deren Reichweite im Einzelnen umstritten ist (vgl. Johannes Barrot, Der Kernbereich privater Lebensgestaltung, 2012; Ilmer Dammann, Der Kernbereich der privaten Lebensgestaltung, 2011). Entsprechende Schutznormen sind in den Sicherheitsgesetzen zumindest dann vorzuhalten, wenn und soweit in Art. 13

GG eingegriffen werden kann (BVerfGE 109, 279 – 1 BvR 2378/98, 1084/99).
Auch bei Eingriffen in Art. 10 GG kann der Kernbereichsschutz zum Tragen kommen. Im Fall der Zuordnung von dynamischen IP-Adressen werden Verbindungsdaten hinzugezogen, um die Bestandsdaten zu ermitteln. Die Eingriffstiefe ist begrenzt, da auf die Inhalte der Kommunikation von Seiten der Behörden kein Zugriff erfolgt. Daher greift insoweit der Kernbereichsschutz nicht.
Einen besonderen Schutz von Vertrauenspersonen enthält der Gesetzentwurf nicht. Dieser ist insoweit nicht notwendig, als er von den Fachgesetzen zu leisten und dort regelmäßig bereits vorhanden ist.

1. Gegenstände und Ausgestaltung der Auskunftspflicht

Der Gesetzentwurf ändert die Vorschrift des § 113 Abs. 1 TKG, indem der Anwendungsbereich zugleich erweitert und konkretisiert wird. Satz 1 betrifft die Erfüllung von Auskunftspflichten. Satz 2 trifft eine neue Regelung im Hinblick auf Daten betreffend Passwörter und ähnliche Schutzvorkehrungen, die sich auf die Einbeziehung in die Auskunftspflicht beschränkt. Die Voraussetzungen des Abrufs, die in der alten Regelung noch enthalten waren, werden in das Fachrecht verschoben. Die bisher nicht enthaltene Neuregelung des Satz 3 umfasst dynamische IP-Adressen. Satz 4 verpflichtet die Unternehmen, alle unternehmensinternen Datenquellen zu berücksichtigen.

Die Voraussetzungen für die Auskunftserteilung regelt nach dem Gesetzentwurf der § 113 Abs. 2 und 3 TKG-E. Danach ist eine ausdrückliche Zugriffsnorm erforderlich, die eine Datenerhebung gem. § 113 Abs. 1 TKG erlaubt. Diese ausdrücklichen Zugriffsnormen sind ebenfalls Gegenstand des Gesetzentwurfs (s.u. 2.). Bei Gefahr im Verzug müssen die Voraussetzungen gleichermaßen erfüllt sein, lediglich die formale Anforderung des Verlangens in Textform wird insoweit modifiziert als das Verlangen auch anders

übermittelt werden kann, z.B. fernmündlich oder per E-mail Anfrage, dann aber in Textform bestätigt werden muss.
Eine Eingrenzung der auskunftsberechtigten Stellen nimmt § 113 Abs. 3 TKG vor, der eine abschließende Aufzählung enthält. Die Strafverfolgungsbehörden, die Gefahrenabwehrbehörden sowie die Verfassungsschutzämter, der BND und der MAD sollen Zugriff auf die Bestandsdaten nehmen können. Die Folgen der Einrichtung einer elektronischen Schnittstelle in § 113 Abs. 5 Satz 2 TKG konnten nicht näher untersucht werden.

2. Die Anforderungen an die Erhebung durch Übermittlung der Bestandsdaten

Die Zugriffsregelungen der zu ändernden Bundesgesetze sind weitest gehend parallel konstruiert. Sie enthalten die ausdrücklichen Rechtsgrundlagen für die Behörden für einen Abruf. Dieser Ermächtigung entspricht dann die Regelung der Auskunftspflicht im TKG (vgl. BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Abs.Nr. 123). Alle Ermächtigungsgrundlagen setzen sich aus drei Absätzen zusammen. Im ersten Absatz ist in einem Satz 1 das Recht auf ein Auskunftsverlangen enthalten, das regelmäßig auf die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes einer Person gerichtet ist. In einem zweiten Satz ist die Auskunft über Zugangssicherungscodes festgehalten, die voraussetzt, dass die weiteren gesetzlichen Voraussetzungen für die Nutzung der Daten erfüllt sind. Im zweiten Absatz ist die Auskunftsberechtigung im Hinblick auf dynamische IP-Adressen geregelt. Der dritte Absatz normiert eine Mitwirkungspflicht der Telekommunikationsdienstleister. Einige Regelungen umfassen die Entschädigungspflicht nach § 23 des Justizvergütungs- und Entschädigungsgesetzes. Die Angemessenheit der Eingriffsschwellen konnte aus Zeitgründen nicht im Detail geprüft werden.

Die Zugriffsregelung des geplanten § 100j Strafprozessordnung ist schon deshalb zu begrüßen, wie sie eine hinreichend bestimmte Regelung für den Abruf von Bestandsdaten trifft und damit die strafprozessuale Generalklausel für Ermittlungsmaßnahmen der §§ 161, 163 StPO als Ermächtigungsgrundlage ablöst. Die Änderungen des Bundeskriminalamtgesetzes führen das Zugriffsrecht dreimal ein: Zur Erfüllung der Zentralstellenfunktion, zur Bekämpfung des internationalen Terrorismus und zum Schutz der Mitglieder von Verfassungsorganen.
Bundespolizeigesetz und Zollfahndungsdienstgesetz betreffen polizeiliche und strafverfolgende Aufgaben. Die nachrichtendienstlichen Aufgaben des Bundesamtes für Verfassungsschutz, des Bundesnachrichtendiensten und des MAD können ebenfalls durch den Zugriff auf Bestandsdaten erfüllt werden.

3. Grundrechtsschutz durch Verfahren und Rechtsschutzgewährleistung: Richtervorbehalt und Mitteilungspflichten

Grundrechtsschutz durch Verfahren ist im Recht der Gefahrenabwehr und Strafverfolgung von erheblicher Bedeutung, weil eine Vielzahl von Maßnahmen in erheblichem Maße in Grundrechte eingreift und zugleich für den Betroffenen nicht erkennbar oder in ihrer Reichweite schwer einzuschätzen ist (vgl. Irina Bonin, Grundrechtsschutz durch verfahrensrechtliche Kompensation bei Maßnahmen der polizeilichen Informationsvorsorge, 2012).

Der Gesetzentwurf enthält weder für das TKG noch die Fachgesetze verfahrensrechtliche Vorkehrungen zum Schutz der Betroffenen. In anderen sicherheitsrechtlichen Zusammenhängen werden Behördenleitervorbehalte oder Richtervorbehalte angewendet, um Eingriffe besonderer Intensität in die Grundrechtssphäre der Betroffenen verfahrensrechtlich abzufedern. Sie bezwecken vorbeugenden Rechtsschutz. Allerdings kann ein Richtervorbehalt nicht die Unbestimmtheit gesetzlicher Ermächtigungsgrundlagen ausgleichen (Kathrin Weber, Die Sicherung

rechtsstaatlicher Standards im modernen Polizeirecht, 2011, S. 121 m.N. zur verfassungsgerichtlichen Rechtsprechung).

Zur Sicherung des nachträglichen Rechtsschutzes dienen Mitteilungspflichten. Nur wenn der Betroffene von der Maßnahme weiß, kann er sich gegen sie wehren. Zur Kompensation der Schwere von Informationseingriffen können auch Maßnahmen der Datensicherheit unter Einbeziehung der Datenschutzbeauftragten beitragen.

Unter dem Vorzeichen der Verhältnismäßigkeit ist das Bundesverfassungsgericht in seinem Urteil vom 24.01.2012 auf Rechtsschutz gegen Auskünfte eingegangen und hat die Auffassung vertreten, der Rechtsschutz gegenüber der abschließenden Behördenentscheidung reiche aus (BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Abs.Nr. 186). Diese Äußerung betrifft den nachträglichen Rechtsschutz und lässt keine Rückschlüsse auf die Notwendigkeit eines Richtervorbehalts zu.
Mitteilungspflichten hält das Bundesverfassungsgericht nicht flächendeckend für erforderlich (BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Abs.Nr. 187). Da es insoweit auf das Fachrecht verweist, ist aber zumindest für Differenzierungen Raum, die von den Gegebenheiten der Zugriffsnormen bestimmt werden. Diese konnte das Bundesverfassungsgericht nicht bewerten, da es ihre Einführung gerade fordert. Eine Bewertung der Notwendigkeit von Mitteilungspflichten ist demnach für Auskunftspflichten und Abrufrechte hinsichtlich von Bestandsdaten ebenso wenig vorentschieden wie die Notwendigkeit von Richtervorbehalten. Es kommen daher die allgemeinen verfassungsrechtlichen Anforderungen zum Tragen.

a. Die Intensität des Grundrechtseingriffs

Die Auskunft über Bestandsdaten und der Zugriff auf diese Daten erfordern ausgleichende Maßnahmen dann, wenn die Eingriffe in die Grundrechte eine besondere Intensität erreichen. Die Intensität des Grundrechtseingriffs hängt

von mehreren Faktoren ab. Dabei spielt das Grundrecht in seiner Ausgestaltung eine Rolle, indem bereits ausdrücklich geforderte Vorkehrungen wie z.B. in den Konstellationen des Art. 13 GG notwendig auf die gesetzlichen Eingriffsschwellen durchschlagen. Da keine Hierarchie der Grundrechte besteht, ist aber grundsätzlich jedes Grundrecht geeignet, im Fall eines intensiveren Eingriffs die Notwendigkeit gesteigerter gesetzlicher Schutzvorkehrungen zu begründen. Allerdings ist zu beachten, dass Art. 10 GG die Verkehrsdaten schützt und damit den Bezug zu konkreten Kommunikationsvorgängen herstellt (BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Abs.Nr. 116). Die Ausprägungen des § 113 TKG, die das Recht auf informationelle Selbstbestimmung berühren, betreffen dagegen allein die Bestandsdaten und damit nicht einzelne Kommunikationsvorgänge.

Eine erhöhte Eingriffsintensität liegt insbesondere dann vor, wenn der Eingriff heimlich erfolgt (BVerfG 120, 274, 348 – 1 BvR 370, 595/07). Falls die Daten besonders sensibel sind, äußert die Datenerhebung ein größeres Gewicht, was das Bundesverfassungsgericht im Fall von Kontostammdaten angenommen hat (BVerfGE 118, 168, 198 - 1 BvR 1550/03, 2357/04, 603/05)

b. Richtervorbehalt

Sinn des Richtervorbehalts ist nach Auffassung des Bundesverfassungsgerichts die vorbeugende Kontrolle durch eine unabhängige und neutrale Instanz (BVerfGE 109, 279, 357 f. – 1 BvR 2378/98, 1084/99) (Überblick zu den Funktionen Malte Rabe v.Kühlewein, Richtervorbehalt in Polizei- und Strafprozessrecht, 2001, S. 410 ff.). Er ist Voraussetzung für die Verhältnismäßigkeit der eingreifenden staatlichen Maßnahme. Die gesetzlichen Neuerungen sind nur dann verfassungsgemäß, wenn sie verfassungsrechtlich erforderliche Vorkehrungen auch enthalten.
Das Erfordernis eines Richtervorbehalts wäre in die Fachgesetze aufzunehmen, nicht in das TKG. Das TKG ist im Schwerpunkt ein Gesetz, das sich an diejenigen wendet, die auf dem Gebiet der Telekommunikation

wirtschaftlich tätig sind. Dies folgt aus seinen Zwecken, Wettbewerb und zugleich angemessene Dienstleistungen zu gewährleisten (§ 1 TKG). Eingriffe in die Grundrechte durch informatorische Maßnahmen staatlicher Stellen regeln die Sicherheitsgesetze. Dort sind die Anforderungen an die Rechtmäßigkeit dieser Eingriffe festzulegen. Das gilt auch für die Verfahrensvorkehrungen und die Gewährleistung von Rechtsschutz.

Die Frage, ob ein verfassungsrechtliches Erfordernis der Einführung eines Richtervorbehaltes besteht, ist für die drei Konstellationen des § 113 TKG einzeln zu prüfen.

Besondere Anforderungen sind für den Eingriff in Art. 10 GG durch die Zuordnung der dynamischen IP-Adressen zu errichten. Der Betroffene erfährt von dem Vorgang zunächst nichts. Im Zusammenhang der Ermittlungs- oder Erforschungstätigkeit der Behörde handelt es sich um einen heimlichen Eingriff. Die vorbeugende Kontrolle der Rechtmäßigkeit ist bei heimlichen Eingriffen in Art. 10 GG in aller Regel verfassungsrechtlich geboten (Baldus, in: Epping/Hillgruber, Beck-OK, GG, Art. 10, Rn. 45). Denn der Betroffene kann seine Interessen nicht selbst wahrnehmen, wofür die Einbeziehung des Gerichts einen Ausgleich bietet (BVerfGE 120, 274 – 1 BvR 370/ 07 und 595/07, Abs.Nr. 258 mit Verweis auf SächsVerfG, Vf. 44-II-94, JZ 1996, 957, 964). Die Erhebung von Daten unter Zuhilfenahme der dynamischen Zuweisung von IP-Adressen und damit der Verkehrsdaten führt zur Notwendigkeit eines Richtervorbehalts.

Die Auskunft über Bestandsdaten, bei denen es sich um Zugangssicherungsdaten (PIN, PUK u.ä.) handelt, greift in das Recht auf informationelle Selbstbestimmung ein (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Ein Richtervorbehalt ist dann verfassungsrechtlich geboten, wenn die heimliche Ermittlungstätigkeit der staatlichen Stellen besonders geschützte Zonen der Privatheit berührt oder besonders eingriffsintensiv ist (BVerfGE 120, 274 – 1 BvR 370/ 07 und 595/07, Abs.Nr. 257). Wenn eine Person den Zugang zu ihren Daten besonders sichert, dann hat sie diese Sphäre als besonders schutzwürdig festgelegt. Darin prägt sich das Recht, über die

eigenen personenbezogenen Daten selbst bestimmen zu können und zu wollen, klar aus. Personen, die der Datensicherheit hohes Gewicht beimessen, treffen Selbstschutzmaßnahmen, die rechtlich zulässig sind (vgl. Julia Gerhards, (Grund-)Recht auf Verschlüsselung?, 2010, S. 78 ff., 381 zu IT-Sicherheit und zum Selbstschutz bei fehlenden staatlichen Schutzkonzepten). Diese Konstellation unterscheidet sich erheblich von der Freigabe einer Telefonnummer im Telefonbuch. Damit wird eine besonders geschützte Zone der selbstdefinierten Privatheit verletzt, wenn Zugriff auf die Zugangssicherungscodes genommen wird. Die Abfederung durch einen Richtervorbehalt ist verfassungsrechtlich geboten.

Die dritte Konstellation der Auskunft ist diejenige über die nach §§ 95, 111 TKG erhobenen Daten. Nach § 111 TKG sind die Telekommunikationsdienstleister verpflichtet, bestimmte Daten zu erheben und zu speichern. Diese Daten werden vom Betroffenen abgefragt, der damit weiß, dass diese Daten dem Telekommunikationsdienstleister zur Verfügung stehen. Die Einwilligung liegt vor. Das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) findet zu Gunsten des Betroffenen Anwendung und wird durch die Auskunft über die Bestandsdaten auch berührt BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Abs.Nr. 121). Für die Einschaltung vorbeugenden Rechtsschutzes spricht dessen Warnfunktion. Eine Verletzung der Privatheit in erhöhter Intensität liegt aber nicht vor. Es geht um die bei Verträgen üblichen Daten, die nicht als besonders sensibel bewertet werden können. Der Grundrechtseingriff ist verhältnismäßig, wenn eher niedrige Eingriffsschwellen erreicht sind. Damit besteht kein verfassungsrechtliches Gebot, einen Richtervorbehalt einzuführen.

Die Ausgestaltung des Richtervorbehalts kann in den unterschiedlichen Fachgesetzen unterschiedlich vorgenommen werden. Nach § 20v BKAG ist für Maßnahmen nach den § 20a ff. BKAG das Amtsgericht zuständig. Daran könnte insoweit angeknüpft werden. Entsprechendes gilt für § 28 BPolG, der bei besonderen Mitteln der Datenerhebung ebenfalls das Amtsgericht heranzieht. Aufgrund der Sachnähe könnte grundsätzlich eine Zuweisung zu

den Verwaltungsgerichten sinnvoll sein, dies ist für jedes Gesetz gesondert zu untersuchen.
Im Hinblick auf die Nachrichtendienste könnten spezifische Ausgestaltungen angebracht sein. Nach § 9 BVerfSchG ist das Amtsgericht im Fall akustischer Wohnraumüberwachungen zuständig. Die Einfügung des § 8d BVerfSchG legt eher einen Zusammenhang mit den Verfahrensregeln des § 8b BVerfSchG nahe, der vorbeugenden Rechtsschutz durch die G 10-Kommission vorsieht. Letztlich sind hier Grundfragen der Kontrolle der Nachrichtendienste angesprochen, die nicht vertieft werden können.

c. Mitteilungspflichten

Der Grundrechtsschutz durch Verfahren führt regelmäßig zu einem Gleichklang der Erfordernisse des Richtervorbehalts und der Mitteilungspflichten. Aus verfassungsrechtlicher Sicht ist allerdings eine differenzierende Beurteilung vorzunehmen, da der Richtervorbehalt vorbeugenden Rechtsschutz, die Mitteilungspflichten nachträglichen Rechtsschutz betreffen. Die Mitteilung an den Betroffenen dient seinem Schutz bei heimlichen Maßnahmen der Behörden. Sie kann aber erst erfolgen, wenn der Erfolg der Maßnahme nicht mehr gefährdet ist. Eine Mitteilung über die Maßnahme an den Betroffenen bezweckt den effektiven Rechtsschutz, der durch Art. 19 Abs. 4 GG i.V.m. mit dem jeweils berührten Grundrecht gewährleistet wird.

Die Eröffnung des Schutzbereiches von Art. 10 GG i.V.m. Art. 19 Abs. 4 GG im Fall der Zuordnung dynamischer IP-Adressen erfordert effektiven Rechtsschutz zur Absicherung des Telekommunikationsgeheimnisses. Durch den Rückgriff auf die Verkehrsdaten werden konkrete Kommunikationsvorgänge in die Auskunft einbezogen. Eine heimliche Datenabfrage, die einzelne Kommunikationsvorgänge betrifft, ist ein erheblicher Eingriff in das Grundrecht (vgl. BVerfGE 125, 260, Urt.v.02.03. 2010 – 1 BvR 256/08 u.a., Abs.Nr. 244). In dieser Konstellation sind daher Mitteilungspflichten zwingend in den Fachgesetzen vorzusehen.

Für die Auskunft über Zugangssicherungsdaten (PIN, PUK u.ä.), die das Recht auf informationelle Selbstbestimmung berührt (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ist an die besondere faktische Gestaltung anzuknüpfen. Der Betroffene erfährt zunächst nicht, dass die von ihm errichteten Zugangshindernisse zur Kenntnis staatlicher Stellen gelangt sind. Sein Wille ist aber gerade, besondere Sicherungen seiner Daten einzubauen. Bereits der effektive Schutz des Rechts auf informationelle Selbstbestimmung erfordert die nachträgliche Mitteilung, damit der Betroffene neue Zugangssicherungen erstellen kann. Der Rechtsschutz tritt hinzu. Auch insoweit ist damit das Aufstellen von Mitteilungspflichten in den Fachgesetzen verfassungsrechtlich geboten.

Die Auskunft über die Daten nach §§ 95, 111 TKG weist auch aus der Perspektive nachträglichen Rechtsschutzes keine erhebliche Eingriffstiefe auf. Der Betroffene hat in die Preisgabe der Vertragsdaten eingewilligt. Zwar ist insoweit zu beachten, dass alle Telekommunikationsunternehmen nach §§ 95, 11 TKG verpflichtet sind, die entsprechenden Daten zu erheben, der Betroffene also gar keine andere Wahl hat, als seine Einwilligung zu erteilen, will er nicht auf die Nutzung von Telekommunikationsendgeräten verzichten. Im Zusammenhang der Untersuchung, ob das Recht auf informationelle Selbstbestimmung intensiv berührt oder die Privatheit besonders betroffen ist, spielt dieser Aspekt aber keine Ausschlag gebende Rolle. Der Gesetzgeber ist von Verfassungs wegen nicht gezwungen, Mitteilungspflichten einzuführen.

Gründe der Praktikabilität können dafür sprechen, alle Fälle des § 113 TKG einheitlich zu behandeln. Wenn in zwei von drei Konstellationen besondere gesetzliche Vorkehrungen erforderlich sind, ist es Sache des Gesetzgebers, die Ausgestaltung der Fachgesetze im Einzelnen vorzunehmen.

4. Technische Entwicklungen - IPv 6

Die rechtliche Einschätzung technischer Erscheinungsformen begegnet angesichts der Dynamik gerade informationstechnischer Entwicklungen nicht unerheblichen Schwierigkeiten. Dies trifft auch auf den IPv6 Standard zu. Die Anwendung dieses Standards in der Breite ist technisch möglich, aber praktisch in seinen Ausprägungen noch nicht gesichert. Welche Designs von unterschiedlichen Telekommunikationsunternehmen gewählt werden, ist nicht im Einzelnen absehbar. Im Kern geht es darum, dass statt der Zuweisung dynamischer IP-Adressen vermehrt oder überwiegend mit statischen IP-Adressen gearbeitet wird. Ein Telekommunikationsendgerät hat eine bestimmte IP-Adresse und ist damit identifizierbar. Das Bundesamt für Sicherheit in der Informationstechnik hat von der Nutzung zumindest der mobilen IPv6 abgeraten (Leitfaden 2012).

Der IPv6 Standard beinhaltet die Möglichkeit von Privacy Extensions. Durch die Anwendung dieser Zusatzoptionen wird ein Teil der Adresse wieder dynamisch, so dass sich nach Ansicht einiger Experten im Vergleich zum aktuellen IPv4 Standard an den rechtlichen Bewertungen wenig ändern würde. Allerdings wird von anderen Experten insoweit die Sorge geäußert, die feste Hälfte der Adresse könne doch zur Identifikation des Nutzers führen und das Rotieren des anderen Teils der Adresse sei für eine Anonymisierung nicht hinreichend. Die Zusatzoptionen der Privacy Extensions können vom Telekommunikationsdienstleister standardmäßig zugeschaltet oder vom Nutzer individuell gewählt werden. Im Fall der Kommunikation zwischen technischen Einrichtungen können Privacy Extensions nicht verwendet werden.

Aus rechtlicher Sicht stellt sich die Frage, ob eine eventuelle statische Adresse nach IPv6 einer Telefonnummer gleichzustellen ist oder ob eine rechtliche Behandlung in Parallele zu den dynamischen Adressen nahe liegt. Die IP-Adresse kann für die Identifizierung des Nutzers herangezogen werden. Im Gegensatz zu Telefonnummern sind diese Daten nicht mit Willen des Nutzers veröffentlicht. Es handelt sich vielmehr um technische Standards, die der Nutzer wenig beeinflussen kann. Der Grundrechtsschutz

des Betroffenen kann aber nicht von sich schnell ändernden technischen Rahmenbedingungen abhängen, deren Gestaltung nicht in seiner Sphäre liegt.

Eine statische IP-Adresse ist einem konkreten Kommunikationsvorgang ohne Weiteres zuzuordnen und führt einfacher als eine dynamische IP-Adresse zur Identifikation des Anschlussinhabers. Dies beantwortet nicht die Frage, welche grundrechtlichen Bestimmungen Anwendung finden. Die IP-Adresse lässt den Rückschluss auf die Identität der Person zu und ist damit ein personenbezogenes Datum. Das Recht auf informationelle Selbstbestimmung ist bei der Ermittlung statischer IP-Adressen jedenfalls berührt (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) (so auch BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Abs.Nr. 115).

Ob der Schutzbereich des Art. 10 GG eröffnet ist, hängt nicht zuletzt von technischen Ausgestaltungen ab, die den geschützten konkreten Vorgang der Telekommunikation prägen. Ein Rückgriff auf Verbindungsdaten wird vom Bundesverfassungsgericht als hinreichende Begründung für die Anwendbarkeit der Telekommunikationsfreiheit des Art. 10 GG erachtet (BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, Abs.Nr. 116). Nehmen die Telekommunikationsunternehmen eine Rotation der Hälfte des Internetprotokolls vor, spricht viel dafür, dass eine Identifikation des Anschlussinhabers nur unter Hinzuziehung von Daten über konkrete Kommunikationsvorgänge erfolgen kann. Dann greift Art. 10 GG. Unterschiedliche Telekommunikationsdienstleister können unterschiedliche Ausgestaltungen vornehmen. Diese Unwägbarkeit kann rechtlich keine Aufteilung des Grundrechtschutzes nach sich ziehen. Es ist zur Effektivität des grundrechtlichen Schutzes von einer einheitlichen Eröffnung des Schutzbereiches von Art. 10 GG auszugehen.

Diese Bewertungen mögen bei geänderten technischen Rahmenbedingungen zu modifizieren sein. In einer Zeit technischer Umstellungen und damit Unsicherheiten ist für den Grundrechtsschutz von hohen Standards auszugehen. Statische IP-Adressen sind den dynamischen IP-Adressen rechtlich gleich zustellen. Sie fallen unter § 113 Abs. 2 TKG und die darauf bezogenen Abrufnormen des Fachrechts. Eine klarstellende

Ergänzung des Gesetzestextes im jeweiligen Abs. 2 wäre angebracht („Satz 1 gilt bei fest zugewiesenen Internetprotkoll-Adressen sinngemäß“).