Anlage
zum Schreiben an den Bundespräsidenten vom 06.11.2015

Die Verschwiegenheit der Rechtsanwälte ist für deren Mandanten von existenzieller Bedeutung. Die vorgesehene Speicherpflicht von Verkehrsdaten darüber, wer, wann, von welchem Stand aus und wie lange mit dem Strafverteidiger und Rechtsanwalt seines Vertrauens kommuniziert hat, durchbricht diese Verschwiegenheit. Damit widerspricht die Regelung dem verfassungsrechtlichen Gebot, das Verhältnis zwischen dem rechtsuchenden Bürger und dem Beistand und Schutz gewährenden Strafverteidiger und Rechtsanwalt unbeobachtet und unangetastet zu lassen (BVerfGE 109, 279, 322; BVerfG Beschl. v. 30.04.2007 – 2 BvR 2151/06 – Rz. 22 (El Masri)). Dieser Vertrauensschutz ist eine Ausprägung des Menschenrechts auf eine freie Lebensgestaltung und hat wenigstens die gleiche Qualität wie die kirchliche und die freie Seelsorge oder Notrufberatung.

Das Argument, es sei angeblich unmöglich, Telekommunikationsanschlüsse von Rechtsanwälten zu identifizieren, die von vornherein aus der Speicherpflicht ausgenommen werden könnten, überzeugt nicht. Eine solche Identifizierung ist den verpflichteten Telekommunikationsanbietern genauso gut möglich wie bei den von der Speicherpflicht ausgenommenen Seelsorge- und Notrufeinrichtungen. Die Ausnahmen erstrecken sich nicht nur auf bestimmte Nummernkreise in der Telekommunikation, sondern sind weitergehend auch von Eigenangaben der jeweiligen Anschlussinhaber abhängig. Im laufenden Vertragsverhältnis kann den Telekommunikationsbetreibern ohne weiteres zugemutet werden, ihre Kunden nach Merkmalen über den Berufsgeheimnisschutz zu befragen und diese Merkmale dann als Ausschlusskriterium für die Vorratsdatenspeicherung zu verwenden. Im Übrigen kann sich der Telekommunikationsanbieter bei Vertragsabschluss oder Vertragsänderung einen von den Rechtsanwaltskammern ausgestellten Anwaltsausweis vorzeigen lassen.

Weiter wäre es möglich, Daten aus dem elektronischen Rechtsanwaltsregister der Bundesrechtsanwaltskammer mit denen der Telekommunikationsanbieter abzugleichen. Die Telekommunikationsunternehmen müssten ohnehin täglich die Höchstspeicherfrist überprüfen und alle Verbindungs- und Standortdaten, bei denen die Höchstspeicherfrist abgelaufen ist, löschen. An diese tägliche Fristenprüfung könnten die bei der BRAK dokumentierten Anschlussdaten der Rechtsanwälte und Kammermitglieder durch einen entsprechenden Datenaustausch angekoppelt werden, so dass der ohnehin eingerichtete Löschungsalgorithmus des Telekommunikationsanbieters nur um eine Datenabfrage bei der BRAK ergänzt werden müsste.

Jedenfalls kann auch erwogen werden, anstelle der Nichterfassung eine sofortige Löschung der Daten durch die täglich vorzusehende Löschungsroutine bei den Telekommunikationsanbietern vorzusehen. Da die Telekommunikationsbetreiber spätestens monatlich in eine vertragsbezogene Kommunikation durch die Rechnungsstellung (bspw. auch zu Werbezwecken) eintreten, können im laufenden Vertrag mit einer einfachen Abfrage solche Merkmale erfasst werden.

Bundesrechtsanwaltskammer
The German Federal Bar
Barreau Fédéral Allemand
www.brak.de

Büro Berlin – Hans Litten Haus
Littenstraße 9
10179 Berlin
Deutschland
Tel. +49.30.28 49 39 - 0
Fax +49.30.28 49 39 -11
Mail zentrale@brak.de

Büro Brüssel
Avenue des Nerviens 85/9
1040 Brüssel
Belgien
Tel. +32.2.743 86 46
Fax +32.2.743 86 56
Mail brak.bxl@brak.eu

Der Schutz der anwaltlichen Kommunikation kann bei anlasslos gespeicherten Verkehrsdaten zu Abrufzwecken (gem. §§ 113a ff. TKG-E) nicht ausreichend durch die strafprozessualen Verwertungs- und Verwendungsschranken des § 160a StPO geleistet werden.

Bereits mit der anlasslosen Speicherung von Verkehrsdaten zu Abrufzwecken ist der Schutz der Verschwiegenheit durchbrochen, denn bereits mit der Speicherung wird eine für die abrufende Stelle undifferenzierte Abruffähigkeit eröffnet, die ein nicht hinnehmbares Missbrauchspotential entfaltet. Ob nämlich eine befugt abrufende Stelle die in § 160a Abs. 1 StPO normierten Grenzen standardmäßig bereits mit der Erlangung solcher Daten beachtet, oder eine Ermittlungstätigkeit solange entfaltet, bis auf einen konkreten Hinweis oder Widerspruch hin, „zufällig“ oder „überraschend“ bekannt wird, dass die für die Ermittlungen genutzten Verkehrsdaten einer geschützten Telekommunikation mit einem Strafverteidiger, Rechtsanwalt oder einem anderen Kammermitglied zugeordnet ist, steht nicht von vornherein fest. Wahrscheinlich ist ein vorsorgliches „Aussortieren“ durch die Strafverfolgungsbehörden auf keinen Fall, weil sie nach der jetzt vorgeschlagenen Regelung unterschiedslos alle Daten abrufen und die damit gelegten Spuren weiter verfolgen dürfen.

Der Verweis auf das strafprozessuale Verwertungsverbot und die Begrenzung der Weiterverwendung von Daten in einem konkreten Ermittlungsverfahren gem. § 160a StPO ist im Übrigen ein schwacher Trost. Selbst wenn sich nachträglich herausstellt, dass bei dieser Arbeit nicht verwertbares Grundlagenmaterial verwendet wurde, ist der Umstand, dass eine Kommunikation zwischen Mandant und Berufsgeheimnisträger stattgefunden hat, nachträglich nicht mehr aus den Köpfen der Ermittler zu entfernen. Die Ermittler wissen zum einen um diese Kommunikation, denn sie befassen sich - auf den Hinweis hin - mit deren Verwertbarkeit. Zum anderen können die mittelbar aus diesem Wissen erworbenen Ermittlungsergebnisse ohne weiteres weiter verwertet werden, wenn diese Ergebnisse nicht vom Schutzbereich des § 160a StPO erfasst werden.

Dem kann nicht entgegen gehalten werden, dass nach dem geltenden Recht eine Abrufbarkeit von Daten, die für Abrechnungszwecke vorgehalten werden (§§ 96 ff. TKG), sowieso mit den bisherigen Eingriffsmaßnahmen der Verfassungsschutz-, Sicherheits- und Strafverfolgungsbehörden erreicht werden kann. Zum einen setzt dieser Abruf ebenfalls einen konkreten Verdacht voraus. Zum anderen entwickelt sich in der Praxis ein Verfahren dieser Behörden nicht entlang von Verkehrsdaten ohne Berufszuordnung als Spurenlage, sondern entlang anderer Anhaltspunkte, die in der Regel den Behörden zuerst Kenntnis vom vorhandenen und gebotenen Schutz des beruflichen Strafverteidiger- und Rechtsanwaltsgeheimnisses verschafft. Das schränkt schon von vornherein den Zugriff auf solche Daten ein.

Das Bundesverfassungsgericht hat zum Eingriff in vertrauliche Mandantendaten ausgeführt (Beschluss vom 12.4.2005 – 2 BvR 1027/02, BVerfGE 113, 29, 49):

> *„Dem Rechtsanwalt als berufenem unabhängigen Berater und Beistand obliegt es, im Rahmen seiner freien und von Art. 12 Abs. 1 Satz 1 GG geschützten Berufsausübung seinen Mandanten umfassend beizustehen. Voraussetzung für die Erfüllung dieser Aufgabe ist ein Vertrauensverhältnis zwischen Rechtsanwalt und Mandant (vgl. BVerfGE 110, 226 <252>). Von Bedeutung ist hierbei, dass das von dem Datenzugriff berührte Tätigwerden des Anwalts auch im Interesse der Allgemeinheit an einer wirksamen und geordneten Rechtspflege liegt (vgl. BVerfGE 15, 226 <234>; 34, 293 <302>; 37, 67 <77 ff.>; 72, 51 <63 ff.>; 110, 226 <252>). Das Bundesverfassungsgericht hat mehrfach die fundamentale objektive Bedeutung*

der „freien Advokatur“ hervorgehoben (vgl. BVerfGE 63, 266 <282> m.w.N.). Diese objektivrechtliche Bedeutung der anwaltlichen Tätigkeit und des rechtlich geschützten Vertrauensverhältnisses zwischen Rechtsanwalt und Mandant wird jedenfalls dann berührt, wenn wegen der Gefahr eines unbeschränkten Datenzugriffs ein Mandatsverhältnis von Anfang an mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet wird. Mit dem Ausmaß potentieller Kenntnis staatlicher Organe von vertraulichen Äußerungen wächst die Gefahr, dass sich auch Unverdächtige nicht mehr den Berufsgeheimnisträgern zur Durchsetzung ihrer Interessen anvertrauen.

Es besteht zudem die Gefahr, dass Mandanten, welchen der Zugriff der Strafverfolgungsbehörden auf auch sie betreffende und regelmäßig vertrauliche Daten bekannt wird, das Mandatsverhältnis zu ihrem Rechtsanwalt oder Steuerberater kündigen. Damit hat der Zugriff auf die Kanzleidaten beschränkende Auswirkungen auf die wirtschaftliche Entfaltung der Beschwerdeführer (vgl. BVerfGE 98, 218 <259>). Die wirtschaftliche Betätigung als Ausprägung der durch Art. 2 Abs. 1 GG geschützten allgemeinen Handlungsfreiheit genießt grundrechtlichen Schutz (vgl. BVerfGE 78, 232 <244>; 91, 207 <221>; 98, 218 <259>).“

Das Bundesverfassungsgericht hat bisher stets heimliche Überwachungsmaßnahmen gegenüber Rechtsanwälten, die selbst nicht einer Straftat verdächtigt werden, für verfassungsrechtlich unzulässig gehalten, zuletzt im Beschluss vom 30. April 2007 – 2 BvR 2151/06.

Die gleichen verfassungsrechtlichen Einwände bestehen gegenüber der anlass- und verdachtsunabhängigen Vorratsspeicherung von Telekommunikationsverbindungsdaten eines Rechtsanwalts nach § 113b TKG, die nach § 100g Abs. 2 StPO auch die Auswertung dieser Daten des unverdächtigen Rechtsanwalts ermöglichen, sofern anzunehmen ist, dass der Beschuldigte einer Straftat von erheblicher Bedeutung Verbindung mit ihm aufnimmt. Auch hier können sämtliche Telekommunikationsverbindungsdaten der letzten zehn Wochen ermittelt und ausgewertet werden, obwohl die Anrufer oder Angerufenen sämtlichst keiner Straftat verdächtigt werden und nur ein einziger Anruf letztlich für die Ermittlungsbehörden von Bedeutung ist. Hier liegt ein schon durch das Gesetz zementierter schwerer Eingriff in das Fernmeldegeheimnis und die darauf bezogene Verhältnismäßigkeit vor. Das Bundesverfassungsgericht hat mit Urteil des ersten Senats vom 27. Juli 2005 – 1 BvR 668/04 – BVerfGE 113, 348, 383 zur Verkehrsdatenerhebung durch das niedersächsische Sicherheits- und Ordnungsgesetz folgendes ausgeführt:

„Die Erhebung der Verbindungsdaten der Telekommunikation und die Standortkennung betreffen zunächst zwar nur die technische Abwicklung des Telekommunikationsvorgangs. Der Eingriff wiegt aber ebenfalls schwer. Verbindungsdaten lassen erhebliche Rückschlüsse auf das Kommunikationsverhalten zu (vgl. BVerfGE 107, 299, 318 ff.). Die Standortkennung eingeschalteter Mobilfunkendeinrichtungen kann zur Erstellung eines Bewegungsbildes führen, über das gegebenenfalls über Gewohnheiten des betroffenen Personen oder auf Abweichungen hiervon geschlossen werden kann.

Grundrechtlich bedeutsam ist ferner die große Streubreite der Eingriffe. Das Abhören oder die Aufzeichnung der Gesprächsinhalte und die Erhebung der Verbindungsdaten können eine große Zahl von Personen treffen. Erfasst sind nicht nur die potentiellen Straftäter, sondern alle, mit denen diese in dem betreffenden Zeitraum Telekommunikationsverbindungen nutzen. Dazu können Personen gehören, die in keiner Beziehung zu einer möglicherweise zu verhütenden oder später zu verfolgenden Straftat stehen, wie etwa Kontakt- und Begleitpersonen oder gänzlich unbeteiligte Dritte.

> *Zur Intensivierung des Eingriffs trägt außerdem bei, dass die Betroffenen den Überwachungsmaßnahmen in einer Situation vermeintlicher Vertraulichkeit ausgesetzt werden. Ahnungslosigkeit besteht insbesondere bei Kontakt- und Begleitpersonen oder sonstigen Dritten, von denen nicht angenommen wird, dass sie selbst die in Zukunft erwarteten Straftaten begehen werden.“*

Das Grundgesetz verbietet danach die heimliche Überwachung der Telekommunikation von Berufsgeheimnisträgern, die nicht selbst einer Straftat verdächtig sind, sondern ihren verfassungsrechtlich gebotenen Aufgaben als Organ der Rechtspflege nachkommen.

- - -