Dr. Hans G. Zeger

01/53115-2952 (FAX)

An
Datenschutzrat (DSR)
Bundeskanzleramt (BKA)
Ballhausplatz
1010 WIEN

Wien, 3. Mai 2002

Betreff: Votum Separatum Entwurf eines Strafrechtsänderungsgesetzes 2002

Sehr geehrte Damen! Sehr geehrte Herren!

Zur Stellungnahme des Datenschutzrates in der 159. Sitzung vom 2.5.2002 zum Beamtenentwurf des Strafrechtsänderungsgesetzes 2002 wird ein votum separatum mit dem Ersuchen es der mehrheitlichen Stellungnahme anzuschließen, abgegeben.

Grundlage des votum separatums

Grundsätzlich besteht Übereinstimmung mit vielen Teilen der Stellungnahme des Datenschutzrates, die sich äußerst kritisch mit den offensichtlich unzureichenden und in seinen grundrechtlichen Konsequenzen nicht ausreichend legitimierten Beamtenentwurf befaßt.

Die Stellungnahme ist jedoch nicht ausreichend, da die Frage der Legitimität der Grundrechtseingriffe als solche nicht berücksichtigt ist. Jeder neue Gesetzesentwurf ist nicht daran zu messen, ob die Verwendung von Daten (die Ermittlung, die Verarbeitung und die Übermittlung) rechtfertigbar ist und durch großzügige Auslegung der Grundrechte akzeptiert werden kann. Vielmehr ist zu prüfen, ob die durch den Gesetzesentwurf angestrebten politischen Ziele die gewünschten Eingriffe in das Grundrecht auf Wahrung des Privatlebens rechtfertigen.

Jede Stellungnahme zu einem neuen Gesetzesentwurf hat sich somit mit der Legitimität der gesamten Datenverwendung im Lichte der behaupteten und angestrebten Ziele des Entwurfes auseinander zu setzen. Diese Analyse wurde in der Mehrheitsstellungnahme des Datenschutzrates nicht geleistet.

Weder aus dem Gesetzestext, noch aus den Erläuterungen, noch aus den Ausführungen der informierten Vertreter konnte eine hinreichende Begründung der Legitimtät der zusätzlichen Datenverwendungen erkannt werden. Trotz umfangreicher Befragungen der informierten Vertreter konnten wesentliche Datenverwendungen nicht oder nur

A-1160 Wien, Redtenbacherg. 20, hans@zeger.at

unzureichend begründet werden. Der Entwurf wird daher mangels grundrechtlicher Legitimität abgelehnt.

Kritikpunkte im Detail

Kein Umsetzungsbedarf

Der Entwurf beruft sich auf die notwendige Umsetzung verschiedener internationaler Abkommen, wie EU-Recht (UN-Sicherheitsratsresolution 1373/2001, EU-Rahmenbeschluss zur Bekämpfung des Terrorismus, Protokoll vom 16. 10. 2001 zu dem Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedsstaaten der EU, UN-Terrorismusfinanzierungsübereinkommen [von Österreich am 24. 9. 2001 unterzeichnet], Cyber-Crime-Konvention des Europarates [von Österreich am 23. 11. 2001 unterzeichnet]). Der Entwurf verschweigt jedoch, daß diese Abkommen entweder nicht ratifiziert, nicht unterzeichnet, zum Teil nicht einmal beschlossen sind. Der Entwurf betreibt somit gezielte Irreführung.

Ausdehnung der Telekomüberwachung

Die Ausdehnung der Überwachungswünsche im Bereich Telekommunikation konnten nicht hinreichend klar begründet werden. Im besonderen konnte nicht begründet werden, in welcher Form die Anforderungen zur "Mitwirkung an der Überwachung der Telekommunikation" durch die verschiedenen Betroffenengruppen (kommerzielle und nichtkommerzielle Betreiber) zu erfüllen sind. Laut Aussagen des informierten Vertreters Dr. Pilnacek soll in Zukunft nicht nur die Mitwirkung der Betreiber an einer aktuellen Überwachung sichergestellt werden, sondern der Zugriff auf alle historischen Daten der Telekombetreiber gesichert werden. Da Telekommbetreiber aus diversen Gründen, etwa im Rahmen der Haftung, von Rechtsstreitigkeiten und der steuerrechtlichen Überprüfbarkeit Datenbestände (etwa Backups) wesentlich länger als 6 Monate aufbewahren (müssen), erlaubt diese Bestimmung die willkürliche Beschaffung jeder Art von Daten.

Ausdehnung des Kreises der zur Mitarbeit an der Überwachung verpflichteten Stellen auf alle Internetprovider

Trotz intensiver Recherchen des Datenschutzrates konnte nicht festgestellt werden, wie der Personenkreis der "Betreiber die an der Überwachung mitzuwirken haben" zu definieren ist. Die informierte Vertreterin des BMVIT, Dr. Weissenbruger konnte keine Abgrenzung zwischen Telekombetreibern, die zur Überwachung verpflichtet sind und jene die es nicht sind, geben. Die bisherige Abgrenzung, daß reine Wiederverkäufer nicht zur Überwachung verpflichtet sind, erwies sich als nicht praxistauglich.

Der vorgebrachte Standpunkt, jeder einzelne Betreiber möge im Rahmen eines Verfahrens des Auskunftspflichtgesetzes feststellen lassen, ob er unter die Bestimmungen fällt, ein zur Mitwirkung an der Überwachung verpflichteter Betreiber zu sein, ist absurd. rechtsstaatliches Handeln benötigt zumindest so klare Fundamente und Definitionen, daß für die meisten Anwendungsfälle klargestellt ist, welche Normen von welchen Betroffenen einzuhalten und zu vollziehen sind. Die bisherige und damit auch im Entwurf

vorgeschlagene Regelung stellt einen Offenbarungseid des Versagens rechtsstaatlichen Handels dar.

Im übrigen führt die Idee, den Betreiberbegriff unbestimmt zu lassen und erst im Anlaßfall durch ein APG-Verfahren feststellen zu lassen, ob Mitwirkungspflicht vorliegt, zu einer Verzögerung und dadurch Behinderung von, im Einzelfall sinnvoller, Ermittlungsmaßnahmen.

Wie jedoch anderen Meinungsäußerungen der informierten Vertreter zu entnehmen ist, soll der Betroffenenkreis bewußt allgemein gehalten werden, um jederzeit nicht nur Infrastrukturbetreiber, wie die klassischen Telekom-Firmen zu Überwachungsmaßnahmen heranziehen zu können, sondern jede Form von Internetbetreibern. Besonders der Vertreter des BMJ, Dr. Pilnacek bejahte diese Frage ausdrücklich. Der Entwurf bleibt in diesem Punkt offensichtlich absichtlich unklar. Damit wird Raum für willkürliche Interpretationen geschaffen.

Schaffung ungeeigneter neuer Strafbestimmungen

Im Bereich der neuen Strafbestimmungen werden bloß eine Fülle neuer, wiederum unbestimmter Definitionen und Tatbestände erfunden, die angestrebten Ziele der besseren Verfolgbarkeit krimineller Handlung jedoch nicht erreicht.

Dies insbesondere dadurch, daß die Beamten offenbar überhaupt keine klare Vorstellung darüber haben, welche Taten und Tätigkeiten in Zukunft als kriminell zu bewerten sind. Tatsächlich folgen diese neuen Straftatbestimmungen eher einem diffusen und durch autoritäres Denken geprägtem Weltbild, als dem klaren grundrechtspolitischen Gedanken, der Sicherung der bestmöglichen individuellen Freiheit.

Bisher existieren folgende Computerstraftatbestände:
- § 126a StGB "Beschädigung von Daten oder Computersysteme"
- § 148a StGB "Computerbetrug" und
- § 51 DSG 2000 "Datenverwendung in Gewinn- oder Schädigungsabsicht"

Trotz eher negativer Erfahrungen mit diesen Tatbeständen (bloß §126a hat in der kriminalistischen Praxis einige Relevanz gewonnen) soll durch eine Überfülle neuer Paragraphen legistischer Aktionismus einerseits und Gefährlichkeit der Online-Welt andererseits signalisiert werden.

Die bisherigen Computerstrafbestimmungen wurden sehr selten eingesetzt und spielen bei den bekannten Deliktsfeldern der letzten Zeit (Stichwort: Kinderpornographie, Rechtsextremismus, Gewaltverherrlichung, Beleidigung, gefährliche Drohung, ...) überhaupt keine Rolle. Mit gutem Grund. Zu all diesen Bereichen existieren seit langem materielle Strafbestimmungen, die technik- und medienunabhängig bestimmte Verhaltensweisen unter Strafe stellen. Es könnte sicher im Einzelfall diskutiert werden, ob die Strafdrohungen angemessen sind, ob alle Straftatbestände nocht zeitgemäß sind und ob ein inhaltlicher Anpassungsbedarf besteht.

Die technik- und medienneutrale Definition von Straftaten schafft jedoch Rechtssicherheit. Potentielle Täter finden keine technischen Hintertürchen, die aufgrund der raschen

technologischen Entwicklung von den Legisten übersehen wurden, Richter können sich auf den Inhalt, den Kern der Tat konzentrieren und müssen nicht technische Abwägungen machen oder durch Gutachter machen lassen und die Gesellschaft hat die Sicherheit, dass bei allem technischen Fortschritt der rechtliche Grundkonsens erhalten bleibt.

§ 118a Widerrechtlicher Zugriff auf ein Computersystem

'(1) Wer sich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen widerrechtlich Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen überwindet, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.'

Bisher war 'reines' Hacken, d.h. der Zugriff auf Computersysteme, ohne Beschädigungsabsicht, ohne Beschaffung personenbezogner Daten oder Auspähung von Betriebs-/Amtsgeheimnissen straffrei. Mit gutem Grund. Auch das bloße Drücken an einer Türklinke um zu sehen, ob eine Tür verschlossen ist, ohne Absicht in ein Haus einzudringen oder etwas zu entfernen, ist straffrei.

Diese neue Bestimmung schafft ein Hackerdelikt, der Teufel steckt im Detail. Unter Strafe steht bloß jemand, der eine spezifische Sicherheitseinrichtung, etwa ein Paßwortsystem überwindet. Professionelle Hacker versuchen jedoch Systemlücken zu finden, die nicht spezifisch geschützt sind, etwa bisher unentdeckte oder durch den Betreiber unbehobene Bugs im Betriebssystem. D.h. sie suchen jene Stellen, die keinen spezifischen Schutz aufweisen und sind damit nach dieser Bestimmung wieder straffrei. Übrig bleiben nur die naiven Cyberkids, die sich vor einem abgesicherten Computer mit dem endlosen Eingeben von Benutzercodes abplagen.

Absatz 2 definiert die Systeme, die geschützt sind: 'Unter einem Computersystem sind sowohl einzelne als auch miteinander vernetzte oder auf andere Weise verbundene Vorrichtungen zu verstehen, die der automationsunterstützten Datenverarbeitung dienen.' Übersehen wurde, daß alle Telekommunikationssysteme längst Computersysteme sind und daher auch hackbar sind, aber nicht in diese Bestimmung fallen.

§ 126a. Beschädigung von Daten oder Computersystemen

Der bestehende Paragraph soll um den Absatz 2 ergänzt werden: '(2) Wer die Funktionsfähigkeit eines Computersystems (§ 118a Abs. 2), über das er nicht oder nicht allein verfügen darf, in erheblichem Ausmaß dadurch stört, dass er Daten eingibt, übermittelt, löscht, verändert oder sonst unbrauchbar macht oder unterdrückt, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.'
Wieder eine Formulierung, die nach mehr klingt, als sie tatsächlich hält. Der Blick in die Erläuterungen macht die Konfusion der Legisten deutlich.Ein IT-Fachmann würde meinen, diese Bestimmung sollte sog. DoS-Attacken (Denial-of-Service-Attacks) pönalisieren. Weit gefehlt! Die Legisten dachten gemäß Erläuterungen an: "Computerviren, Spamming, Trojaner". Eine eigentümliche Troika. Nun gibt es kaum einen "Spammer" der Spam-Mails mit dem Vorsatz der Datenbeschädigung verschickt. Spamming ist eher als soziales und

wettbewerbsrechtliches Problem einzustufen. Spammer wollen ja ihre Produkte verkaufen oder Fremdpersonen mit bestimmten ideologischen Inhalten versorgen, Schädigungsabsicht liegt nicht vor und wird daher auch nicht von dieser Bestimmung erfaßt. Computerviren und Trojaner sind dagegen Programme bzw. Programmteile, die der rechtmäßige Inhaber des Computersystems selbst mit anderer Software mitinstalliert, auf diese Person wird die Bestimmung nicht anwendbar sein. Das eigentliche Problem der letzten Jahre, die 'Würmer' werden weder durch den Gesetzestext, noch durch die Erläuterungen angesprochen. Reichlich peinlich für die Legisten.

§ 126b. Missbrauch von Computerprogrammen oder Zugangsdaten

Die Herstellung von Computerprogrammen, '[die] hauptsächlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119) oder einer Beschädigung von Daten oder Computersystemen (§ 126a) geschaffen oder adaptiert worden [sind]', soll unter Strafe gestellt werden. Klingt abschreckend, geht jedoch an der Sache vorbei. Jedes Cracker-, Scanner- und Intruder-System kann genutzt werden, die Sicherheit seines eigenen Systems zu prüfen oder die Sicherheitslücken eines Fremdsystems aufzudecken. Oder umgekehrt. Abgesehen von bestimmten, taxativ aufgezählten 'verbotenen Waffen' und sonstigen Stoffen, findet sich bei keinem anderen Straftatbestand ein vergleichbares Werkzeugdelikt. Wer produziert schon Füllfedern, die "hauptsächlich" zum Scheckbetrug eingesetzt werden?

§ 119. Verletzung des Telekommunikationsgeheimnisses

Hier sollte bloß die TKG-Bestimmung (§88) ins Strafgesetzbuch übertragen werden. Nicht einmal das ist geglückt. Es wird zwar das 'abhören, aufzeichnen, abfangen oder sonst überwachen' unter Strafe gestellt, nicht jedoch das wesentlich häufigere und immer weiter verbreitete "Mithören', wie im TKG. Ob das nun zum "sonst überwachen" gehört oder doch legal sein soll, bleibt im Dunkeln.
Welche Daten tatsächlich geschützt werden sollen, bleibt ebenfalls unklar. Angesprochen wird die "Nachricht", die geschützt ist. Dies suggeriert, daß es sich um den Inhalt von Gesprächen oder übertragenen Informationen handelt, tatsächlich gewinnen die Vermittlungs-, Bewegungs- und Ortsdaten immer mehr an Bedeutung und sind immer öfter Ziel von Lauschangriffen. Statt den gesamten Angriff auf Kommunikationsfreiheit unter Strafe zu stellen, werden Teilaspekte herausgepickt.

§225a Fälschung von Computerdaten:

'Wer durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten (§ 126a Abs. 3) mit dem Vorsatz herstellt oder echte Daten (§ 126a Abs. 3) mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.'
Offenbar dem Straftatbestand Urkundenfälschung nachgebildetes Delikt, dass im Zusammenhang mit Signaturlösungen bedeutsam sein könnte. Wesentlich intelligenter wäre es, elektronisch signierte Dokumente anderen Urkunden gleich zu stellen, damit

wäre der Tatbestand Urkundenfälschung darauf anwendbar, anstatt immer neue legistische Teillösungen um technische Entwicklungen herum zu basteln.

Positive Aspekte der mehrheitlichen Stellungnahme des Datenschutzrates

Folgenden Detailanregungen der mehrheitlichen Stellungnahme des Datenschutzrates kann ebenfalls zugestimmt werden.

Zu § 118a StGB (widerrechtlicher Zugriff auf ein Computersystem:
Der Begriff "spezifische Sicherheitsvorkehrungen" ist unklar und extrem interpretationsbedürftig. Diesbezüglich sollte bereits im Gesetzestext eine Klarstellung erfolgen.

Zu § 149a Abs. 1 und 2 StPO :
Nach der nunmehr in Aussicht genommenen Regelung reicht es für die Zulässigkeit der Lokalisation eines Endgerätes unabhängig von einer Telekommunikation im strengen Sinn, wenn "zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung gefördert werden kann". Es erhebt sich die Frage, ob diese Regelung sachlich vor dem Hintergrund des Art. 8 EMRK haltbar ist. Es wird nämlich vom Gesetz weder gefordert, dass das Endgerät einem Tatverdächtigen selbst gehört bzw. von ihm verwendet wird, noch dass ein unmittelbarer Nahebezug des Endgerätes oder des Inhabers zu einer bestimmten Tathandlung besteht, noch das irgendeine Wahrscheinlichkeit dafür besteht, dass ein Verdächtiger mit dem Inhaber des Endgerätes kommunizieren werde. Grundsätzlich ist festzuhalten, dass die Überwachung der räumlichen Bewegung natürlicher Personen einen schwer wiegenden Eingriff die die Privatsphäre darstellt und daher entsprechende qualifizierte Voraussetzungen für deren Zulässigkeit gefordert werden muss. Zu fordern wäre etwa, dass eine solche Form der Überwachung nur gegenüber Verdächtigen selbst oder solchen Personen, von denen anzunehmen ist, dass sie mit der verdächtigen Person kommunizieren werden, zulässig ist (vgl. die Kriterien, die im geltenden § 149a Abs. 1 Z 2 StPO vorgesehen sind).
Diese einschränkenden Kriterien des geltenden § 149a Abs. 1 Z 2 StPO sind aber im vorliegenden Entwurf nur mehr bei der Überwachung von Inhaltsdaten, nicht aber bei der Überwachung von Standorten oder der Verbindungsdaten vorgesehen.
Im Hinblick darauf, dass auch die Erfassung derartiger Daten schwer wiegende Eingriffe in die Privatsphäre einer Person sein können, sollte eine Überwachung aber auch in diesen Fällen an zusätzliche Kriterien – wie dies bisher der Fall war - gebunden werden.
Aus den Formulierungen des § 149a Abs. 1 Z 1 lit a und b ("...**befindet oder befunden hat**"; ……..welche Teilnehmeranschlüsse Ursprung oder Ziel einer Telekommunikation **sind oder waren**") ist zu schließen, dass auch die rückwirkende Feststellungen von Funkzellen und Auswertung von Rufnummern möglich sein soll (siehe dazu auch die diesbzügliche explizite Regelung des § 149b Abs.3).
Dazu ist zum einen zu bemerken, dass ein Berechtigung zur Aufbewahrung von Vermittlungsdaten über die Abwicklung der Vermittlung hinaus dzt. nur in dem im TKG normierten Ausmaß (Abrechnungszwecke) besteht. Eine Datenspeicherung "auf Vorrat" wäre schon im Hinblick auf § 6 DSG 2000 unzulässig und im Übrigen auch unverhältnismäßig.

Eine “rückwirkende” Überwachung könnte daher wohl nur durch die Herausgabe solcher Daten erfolgen, die der Betreiber im Zeitpunkt der Herausgabe/Einsicht aus anderen Gründen (noch) zulässigerweise gespeichert hat.
§ 149a legt daher nur fest, wann eine (rückwirkende) Überwachung rechtmäßig ist; nicht aber, dass Betreiber zur Speicherung oder zur Herausgabe der Daten verpflichtet wären. Solches ergibt sich auch nicht aus dem TKG, da sich die Formulierung des § 89 TKG wohl nur auf das Zurverfügungstellen der notwendigen technischen Möglichkeiten bei der Überwachung bezieht.
§ 149a Abs. 2 Z 1 geht offenbar davon aus, dass eine ausdrückliche Zustimmung des Inhabers des Teilnehmeranschlusses rechtfertigt, dass hier schon bei geringfügigeren strafbaren Handlungen eine Überwachung stattfinden darf. Diese Annahme scheint aber nicht gerechtfertigt, da die Zustimmung des Inhabers eines Teilnehmeranschlusses in keiner Weise datenschutzrechtliche Relevanz bezüglich der Daten der anderen Gesprächsteilnehmer hat. Es ist daher nicht einzusehen, dass in derartigen Fällen sogar die Überwachung von Gesprächsinhalten zulässig sein soll. Diese Bestimmung scheint – auch wenn sie schon bisher bestanden hat – einen unverhältnismäßigen Eingriff in den Datenschutz anderer Betroffener, die mit dem Inhaber des Teilnehmeranschlusses Kontakt hatten oder etwa vom Telefon des Inhabers aus telefonierten, vorzusehen.
Abs. 2 Z 3 schränkt eine Überwachung von Gesprächsinhalten auf Verbrechen und bestimmte Vergehen ein. Dies ist wegen der Schwere des Eingriffs jedenfalls zu begrüßen, allerdings wird die hier normierte Einschränkung durch die Bestimmung des Abs. 2 Z 1, die bei Zustimmung des Inhabers des Teilnehmeranschlusses ohnehin in geringfügigeren Fällen eine Überwachung ermöglicht, gewissermaßen unterlaufen.
Eine Änderung oder Streichung des Abs. 2 Z 1 scheint aus diesen und den bereits oben genannten Gründen notwendig, umso mehr als aus den Erläuterungen ersichtlich ist, dass nunmehr im Gesetz klar zwischen der Überwachung von Verbindungsdaten und Standortdaten einerseits und Inhaltsdaten andererseits differenziert werden soll.

Zu § 149a Abs. 4 StPO:
In diesem Absatz wird ausdrücklich die Eingriffsschranke der Verhältnismäßigkeit statuiert. Die Überwachung soll nur zulässig sein, soweit die Verhältnismäßigkeit zum Zweck der Maßnahme gewahrt wird. Dabei ist insbesondere darauf Bedacht zu nehmen, dass der angestrebte Erfolg in einem vertretbaren Verhältnis zu den voraussichtlich bewirkten Eingriffen in die Rechte unbeteiligter Dritter steht und zu prüfen, ob nicht auch mit weniger eingreifenden Maßnahmen begründete Aussicht auf den angestrebten Erfolg besteht. Wenngleich diese ausdrückliche Bezugnahme auf den Grundsatz der Verhältnismäßigkeit positiv zu sehen ist, ist festzuhalten, dass auch ohne eine derartige ausdrückliche Festschreibung schon auf Grund von Art. 8 EMRK bzw. § 1 Abs.2 DSG nur eine verhältnismäßige Maßnahme zulässig wäre. Wesentlich bedeutsamer ist die in § 149b Abs. 2 vorgesehene Regelung, dass ein Beschluss, mit dem die Überwachung einer Telekommunikation angeordnet wird, unter anderem die Erforderlichkeit und die Verhältnismäßigkeit einer Überwachungsmaßnahme darzutun hat.
Bedauerlich ist allerdings, dass nunmehr nach § 149 b Abs. 1 für die Fassung eines Beschlusses im vorstehenden Sinn nicht mehr durchgehend die Ratskammer, sondern – für die Fälle der Lokalisation eines Endgerätes bzw. die Rufdatenrückerfassung – uzw auch ohne Gefahr in Verzug der Untersuchungsrichter zuständig ist. Außerdem entfällt in diesen Fällen das Erfordernis des dringenden Tatverdachts. Noch im Sommer 2001 ging das Justizministerium sehr wohl von dem Erfordernis einer durchgängigen

grundsätzlichen Ratskammergenehmigung aus. (vgl. die Fassung des § 149 b nach dem Konzept der Strafprozessnovelle 2001).
Begründet wird der Verzicht auf das Erfordernis des Ratskammerbeschlusses, aber auch auf das Erfordernis des dringenden Tatverdachtes für die Fälle der Rückrufdatenerfassung bzw. Lokalisation einfach mit der in der wissenschaftlichen Literatur vertretenen Ansicht, es handle sich bei der Offenlegung von Vermittlungsdaten um einen weniger schwer wiegenden Eingriff ins Fernmeldegeheimnis als dem Abhören von Inhalten. In dieser Pauschalität kann diesem Argument freilich nicht zugestimmt werden. Es ist keinesfalls ausgeschlossen, dass im Einzelfall auch eine Rufdatenrückerfassung einen Eingriff darstellt, der – etwa durch den Leumund des Kommunikationspartners - sogar eine inhaltliche Überwachung an Brisanz übertrifft.

Zusammenfassung

Der Entwurf läßt nicht erkennen, wie das behauptete Ziel einer verbesserten Strafverfolgung kriminellen Handelns aufgrund unbestimmter Definitionen, Schaffung unkarer Tatbestände, Rechtsunsicherheit der Normunterworfenen und zusätzliche Eingriffe in die Privatsphäre, erreicht werden könnte. Der Entwurf wird daher abgelehnt.

Mit vorzüglicher Hochachtung

Dr. Hans G. Zeger
(in der elektronischen Fassung nicht unterzeichnet)