

ANPASSUNG DER §§ 100G, 100H STPO AN DIE RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES ÜBER DIE VORRATSSPEICHERUNG VON DATEN

1. Einleitung

Von der Europäischen Gemeinschaft wurde Anfang dieses Jahres die Richtlinie 2006/24/EG erlassen, nach der die Anbieter von öffentlich zugänglichen Kommunikationsdiensten sowie die Betreiber von öffentlichen Kommunikationsnetzen zur Speicherung von Verbindungsdaten für einen Zeitraum von mindestens 6 und bis zu 24 Monaten verpflichtet werden sollen. Diese Richtlinie wurde am 14.12.2005 vom Parlament und am 21.02.2006 vom Rat verabschiedet.

In dieser Richtlinie ist ausführlich geregelt, wie die Speicherung zu erfolgen hat und welche Daten gespeichert werden müssen. Unter welchen Voraussetzungen ein Zugriff auf diese Daten möglich sein soll, ist jedoch nicht festgelegt. Insoweit fehlt der EG die erforderliche Regelungskompetenz. Der Zugriff auf die Verbindungsdaten ist ein wichtiges Werkzeug zur Bekämpfung der Kriminalität. Er ist in den §§ 100g, 100h StPO geregelt. Die erhebliche Bedeutung der Telekommunikation in der heutigen Gesellschaft wird vor allem deutlich, wenn man sich vor Augen führt, dass im Jahr 2002 täglich rund 216.000.000 Telefonverbindungen hergestellt wurden¹. Diese Zahl dürfte bis heute noch erheblich gestiegen sein.

Dadurch, dass die Verbindungsdaten mit Umsetzung der Richtlinie der EG mindestens 6 Monate gespeichert werden müssen, ist eine Anpassung der §§ 100g, 100h StPO an diese neue Situation erforderlich. Wer wie und unter welchen Voraussetzungen auf die gespeicherten Daten zugreifen darf, muss angemessen geregelt werden. Dieser Aufsatz befasst sich mit der Fragestellung, wie der Zugriff auf die auf Vorrat gespeicherten Verbindungsdaten durch deutsche Strafverfolgungsbehörden neu geregelt werden sollte.

2. Betroffenes Grundrecht

Die Telekommunikationsverbindungsdaten fallen in den Schutzbereich des Art. 10 Abs. 1 GG. Das Fernmeldegeheimnis umfasst neben dem Inhalt der Kommunikation auch deren Umstände, somit auch die Verbindungsdaten. Art. 10 Abs. 1 GG schützt insbesondere die Information ob, wann, wie oft und zwischen welchen Personen Telekommunikation stattgefunden hat oder versucht worden ist².

3. Grundrechtseingriff

Bereits die Speicherung der Verbindungsdaten ist ein Eingriff in die Grundrechte der Betroffenen. Der Zugriff auf die gespeicherten Daten stellt einen erneuten, noch deutlich intensiveren Eingriff in das Grundrecht dar, der ebenfalls einer Rechtfertigung bedarf.

¹ BVerfG, Urteil vom 12.03.2003, 1 BvR 330/96, Rn. 94.

² BVerfG, Urteil vom 27.07.2005, 1 BvR 668/04, Rn. 82.

4. Rechtfertigung

Der Eingriff ist dann gerechtfertigt, wenn er aufgrund eines Gesetzes erfolgt und er geeignet, erforderlich und angemessen ist, um einem legitimen Zweck zu dienen. Fraglich ist also, wie die §§ 100g, 100h StPO zu gestalten sind, damit Eingriffe aufgrund dieser Vorschriften einem legitimen Zweck dienen und geeignet, erforderlich sowie angemessen sind, um diesen Zweck zu erreichen.

a) Legitimer Zweck

Ein legitimer Zweck für die Übermittlung der Verbindungsdaten an die Strafverfolgungsbehörden ist die Ermittlung, Feststellung, Verfolgung und Vermeidung von Straftaten. Die Strafverfolgungsbehörden werden zwar primär präventiv aber zum Teil auch repressiv tätig. Das Bundesverfassungsgericht hat festgestellt, dass ein unabweisbares Bedürfnis nach einer wirksamen Strafverfolgung besteht, dessen Befriedigung ein wesentlicher Auftrag des rechtsstaatlichen Gemeinwesens ist³. Somit bestehen keine Zweifel hinsichtlich der Legitimität des Zwecks.

b) Geeignetheit

In der Praxis hat sich gezeigt, dass die Auskunft über Telekommunikationsdaten ein wirkungsvolles Mittel zur Bestimmung des Standorts eines Beschuldigten und zur Erforschung und Aufklärung von Straftaten ist. Das Mittel ist somit zur Erreichung des angestrebten Zwecks auch geeignet.

c) Erforderlichkeit

Das Gesetz muss so gestaltet sein, dass der jeweilige Eingriff erforderlich ist. Bereits jetzt enthält § 100g Abs. 2 StPO die Regelung, dass eine Maßnahme nur dann zulässig ist, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Der hier festgehaltene Subsidiaritätsgrundsatz stellt sicher, dass der jeweilige Eingriff erforderlich ist und es kein milderes Mittel zur Erreichung des Zwecks gibt. Diese Klausel muss daher unbedingt beibehalten werden.

Daneben ist zu berücksichtigen, dass Auskunft nur soweit zu erteilen ist, wie es erforderlich ist. Die Anordnung muss also so konkretisiert werden, dass ersichtlich ist, für welchen Zeitraum welche Art der Verbindungsdaten (Quelle, Adressat, Datum, Uhrzeit, Dauer, Art der Kommunikation, Endeinrichtung, Standort) über welche betroffene Personen mitzuteilen sind. Dies ergibt sich bereits aus § 100g Abs. 1 S. 1 StPO. Faktisch werden jedoch häufig zunächst sämtliche Verbindungsdaten für einen bestimmten Zeitraum erhoben. Um hier ein höheres Problembewußtsein für den Eingriff in das Grundrecht zu schaffen, sollte die Anordnung zukünftig eine ausführliche Begründung enthalten, aus der sich ergibt, welches konkrete Ermittlungsziel mit der Maßnahme verfolgt wird und wieso die angeforderten Daten in diesem Umfang zur Erreichung dieses Ziels erforderlich sind. Eine entsprechende Pflicht sollte ausdrücklich im Gesetz genannt werden. Um den Standort eines Verdächtigen zu ermitteln, ist es nicht erforderlich, Daten bezüglich des Adressaten oder der Art der

³ BVerfG, Urteil vom 12.03.2003, 1 BvR 330/96, Rn. 57.

Kommunikation zu erheben. Gleichwohl werden diese Daten häufig mit erhoben. Die getroffene Maßnahme darf aber eben nicht zu einer Rundumüberwachung des Betroffenen führen, mit der ein umfassendes Persönlichkeitsprofil erstellt werden könnte. Diese Möglichkeit muss ausgeschlossen sein⁴.

d) Angemessenheit

Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG müssen weiterhin angemessen sein. Bei der Prüfung der Angemessenheit ist zu berücksichtigen, dass Ermittlungsmaßnahmen nach § 100g StPO typischerweise nicht in den unantastbaren Kernbereich privater Lebensgestaltung eingreifen, da lediglich die Verbindungsdaten, nicht jedoch der Inhalt der Kommunikation betroffen ist. Unter Umständen kann durch die Auswertung der Verbindungsdaten sogar ein noch tiefer gehender Eingriff in die Rechte des Betroffenen vermieden werden.

Auf der anderen Seite ist jedoch auch zu berücksichtigen, dass aufgrund der Auswertung der Telekommunikationsverbindungsdaten tiefe Einblicke in das Kommunikationsverhalten, das soziale Umfeld sowie persönliche Angelegenheiten und Gewohnheiten des Betroffenen beziehungsweise Abweichungen von diesen Gewohnheiten möglich sind. Ebenso kann ein umfangreiches Bewegungsprofil erstellt werden.

Da die Telekommunikationsverbindungsdaten nunmehr auf Vorrat gespeichert werden sollen, ist die Auswertung dieser Daten über einen erheblichen Zeitraum auch im Nachhinein noch möglich. Dies war bisher nicht in diesem Umfang der Fall. Eine Maßnahme nach den §§ 100g, 100h StPO stellt somit im Gegensatz zur bisherigen Situation, einen deutlich schwerwiegenderen Eingriff in die Rechte des Betroffenen dar. Um die Angemessenheit zu wahren, kann eine solche Maßnahme daher auch nur noch unter strengeren Voraussetzungen als bisher zulässig sein. Wenn ein Eingriff in das Grundrecht schwerer wiegt als ein anderer, kann er nur durch einen ebenfalls schwerer wiegenden Zweck gerechtfertigt werden. Aus diesem Grund sind die §§ 100g, 100h StPO an die neue Situation anzupassen.

Neben dem Verdächtigen selbst können bei Eingriffen nach §§ 100g, 100h StPO auch zahlreiche Personen betroffen sein, die in keiner Beziehung zu einem konkreten Tatvorwurf stehen und die den Eingriff durch ihr Verhalten auch in keiner Weise veranlaßt haben. Aus diesen Gründen bedarf der Eingriff einer besonderen Rechtfertigung⁵.

Der Eingriff kann somit nur zulässig sein, wenn hinreichende Anhaltspunkte für eine drohende Gefahr und für eine nicht unerhebliche Straftat vorliegen. Je geringer dabei das Gewicht des gefährdeten Rechtsguts ist, umso höher sind die Anforderungen an die Prognosesicherheit hinsichtlich des Grades der Gefährdung und ihrer Intensität⁶. Für die Gefährdung eines konkreten Rechtsgutes muss eine gesicherte Tatsachenbasis sprechen. Bloße Vermutungen oder die abstrakte Möglichkeit einer Gefährdung reichen nicht aus⁷.

Auch wenn die Wahrscheinlichkeit der Gefährdung des Rechtsguts und ihre Intensität stark sind, muss das gefährdete Rechtsgut ein bestimmtes Gewicht haben. Ein Eingriff ist also nur bei bestimmten Straftaten angemessen. Das Bundesverfassungsgericht hat angedeutet, dass ein Eingriff nach § 100g StPO nur dann angemessen sein kann, wenn es sich um eine Straftat

⁴ BVerfG, Urteil vom 12.04.2005, 2 BvR 581/01, Rn. 60.

⁵ BVerfG, Urteil vom 12.03.2003, 1 BvR 330/96, Rn. 73.

⁶ BVerfG, Urteil vom 27.07.2005, 1 BvR 668/04, Rn. 149.

⁷ BVerfG, Urteil vom 12.03.2003, 1 BvR 330/96, Rn. 78.

aus dem Bereich der mittleren Kriminalität handelt, also um eine solche, die den Rechtsfrieden empfindlich stört und dazu geeignet ist, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen⁸. Unter diesem Gesichtspunkt ist es also unbedingt erforderlich, dass die Eingriffsbefugnis auf bestimmte Straftaten, wie zum Beispiel die in § 100a Satz 1 StPO genannten oder andere Straftaten von erheblicher Bedeutung, beschränkt wird, wie es in § 100g Abs. 1 S. 1 Alt. 1 StPO der Fall ist. Dabei genügt die Bezugnahme auf sonstige Straftaten von erheblicher Bedeutung in der derzeitigen Fassung auch dem Bestimmtheitsgrundsatz⁹. Die aufzuklärende Straftat muss jedoch nicht nur allgemein, sondern auch im konkreten Einzelfall eine erhebliche Bedeutung haben.

aa) Mittels Endeinrichtung begangene Straftaten

Nicht alle mittels einer Endeinrichtung begangenen Straftaten haben eine solche erhebliche Bedeutung. Diese Alternative des § 100g Abs. 1 S. 1 StPO sollte daher aufgehoben, oder muss zumindest eingeschränkt werden. Da die 1. Alternative des § 100g Abs. 1 S. 1 StPO auch andere Straftaten von erheblicher Bedeutung erfasst, kann aufgrund dieser Vorschrift ebenfalls auf Verbindungsdaten im Zusammenhang mit mittels Endeinrichtung begangener Straftaten zugegriffen werden, wenn diese von erheblicher Bedeutung sind. Die im Katalog des § 100a S. 1 StPO aufgeführten Normen sind nahezu alle mit einer Freiheitsstrafe von bis zu fünf Jahren oder mehr belegt. Wenn also ein Straftatbestand erfüllt ist, der ebenfalls mit einer Freiheitsstrafe von bis zu fünf Jahren bewährt und nicht im Katalog des § 100a S. 1 StPO aufgeführt ist, ist eine Maßnahme nach § 100g StPO in der Regel zulässig.

Es ist jedoch unangemessen und somit rechtswidrig, wenn aufgrund einer einfachen mittels einer Endeinrichtung begangenen Beleidigung, die voraussichtlich nur mit einer Geldstrafe in Höhe von 10 Tagessätzen bestraft werden wird, eine Maßnahme nach § 100g StPO angeordnet wird, die in erheblichem Maße in die Grundrechte eingreift.

Fraglich ist daher nur, ob man die 2. Alternative des § 100g Abs. 1 S. 1 StPO gänzlich aufhebt oder sie lediglich einschränkt. Denkbar wäre neben der Aufhebung dieser Alternative auch eine Einschränkung auf Straftaten, für die vom Gesetz eine Freiheitsstrafe von bis zu drei Jahren oder mehr angedroht wird. Bei dieser Variante wären völlig unangemessene Eingriffe nicht mehr möglich, aber die Ermittlungsmöglichkeiten sind nicht so stark eingeschränkt, dass Straftaten, die mittels Endeinrichtungen begangen werden, nur noch aufklärbar wären, wenn sie von erheblicher Bedeutung im Sinne der 1. Alternative dieser Vorschrift sind. Ebenfalls denkbar wäre eine Einschränkung der Anwendbarkeit in Bezug auf die im Einzelfall zu erwartende Strafe. Dies würde eine Angemessenheitsprüfung ermöglichen, die den sich gegenüberstehenden Interessen am besten gerecht werden würde. Allerdings wird eine sachgerechte Einschätzung der zu erwartenden Strafe zu diesem frühen Zeitpunkt der Ermittlungen in der Regel nicht möglich sein. Es bleibt also lediglich die Möglichkeit der Einschränkung unter Berücksichtigung der vom Gesetz angedrohten Strafe.

bb) Berufsgeheimnisträger (Speicherung oder nur Zugriff verbieten?)

Zum einen bei der Speicherung der Verbindungsdaten, zum anderen auch beim Zugriff auf diese Daten ist zu berücksichtigen, dass bestimmte Berufsgeheimnisträger (Presse, Abgeordnete, Richter, Pfarrer, Anwälte, Ärzte...) einen speziellen Grundrechtsschutz genießen. Zwischen ihnen und den Bürgern besteht ein besonderes Vertrauensverhältnis, das

⁸ BVerfG, Urteil vom 12.04.2005, 2 BvR 581/01, Rn. 48.

⁹ BVerfG, Urteil vom 12.03.2003, 1 BvR 330/96, Rn. 76.

angemessen berücksichtigt werden muss. Ein Zugriff auf die Verbindungsdaten dieser Personen stört dieses besondere Vertrauensverhältnis und führt daher zu einer Gefährdung bestimmter Grundrechte, wie zum Beispiel der Presse- oder Religionsfreiheit. Ein Zugriff kann demnach nur dann angemessen sein, wenn der Geheimnisträger in der konkreten Situation nicht als solcher fungiert oder er selbst an einer Straftat von erheblicher Bedeutung beteiligt ist. Die in § 100h Abs. 2 StPO angeordnete Unzulässigkeit der Datenerhebung bei Zeugnisverweigerungsberechtigten nach § 53 Abs. 1 StPO sollte daher auf alle dort genannten Berufsgruppen ausgedehnt werden. Nur so kann das Vertrauen der Bürger in die Berufsgeheimnisträger gewahrt bleiben. Gerade dadurch, dass ein Kommunikationsvorgang auch noch nach sechs Monaten nachvollzogen werden kann, werden die Bürger gezwungen auf die Inanspruchnahme der Berufsgeheimnisträger zu verzichten oder andere Wege der Kommunikation zu suchen, wodurch sie erheblich in ihren Grundrechten eingeschränkt werden.

cc) Richtervorbehalt

Die Anordnung der Herausgabe der Verbindungsdaten ist dem Richter vorbehalten. Dieser Grundsatz muss unbedingt beibehalten werden. Allerdings gibt es derzeit die Ausnahme, dass es bei Gefahr im Verzug der Anordnung durch den Richter nicht bedarf. Diese Einschränkung sollte nunmehr auf die Fälle beschränkt werden, in denen die Herausgabe der Verbindungsdaten präventiven Zwecken dienen soll. Da die Daten sechs Monate gespeichert werden, sind Fälle der Gefahr im Verzug bei der Aufklärung von Straftaten nur noch schwer vorstellbar. Es besteht nicht mehr die Gefahr, dass die Daten gelöscht werden könnten und somit verloren sind.

Weiterhin ist zu Berücksichtigen, dass der Betroffene keine Möglichkeit hat, zum Antrag der Staatsanwaltschaft Stellung zu nehmen. Aus diesem Grund besteht die Gefahr, dass der Antrag nicht kritisch genug geprüft wird oder es gar zu einer pauschalen Anordnung aufgrund jedweden Antrags der Staatsanwaltschaft kommt. Um dem vorzubeugen und den Blick sowohl der Staatsanwaltschaft als auch der Ermittlungsrichter in Hinblick auf das Recht aus Art. 10 GG zusätzlich zu schärfen, sollte eine weitere unabhängige Instanz eingeschaltet werden, die die berechtigten Interessen des Betroffenen wahrt, soweit sein Grundrecht betroffen ist. Hierfür bieten sich die für den Datenschutz zuständigen Stellen der Länder an. Ihnen sollte Gelegenheit zur Stellungnahme zum Antrag der Staatsanwaltschaft gegeben werden. In der Regel wird eine solche Stellungnahme zwar entbehrlich sein, aber in kritischen Fällen kann so einfach und effektiv ein rechtswidriger Eingriff vermieden werden.

Durch die Stellungnahme der für den Datenschutz zuständigen Stellen der Länder wird darüber hinaus auch die Arbeit des Ermittlungsrichter erleichtert, da die Prüfung einfacher ist und er sich gegebenenfalls auch die Argumente aus der Stellungnahme zu eigen machen kann. Grundsätzlich werden durch die damit verbundenen Verzögerung auch nicht die Ermittlungen beeinträchtigt, da die Verbindungsdaten lange genug gespeichert werden, um eine angemessene Frist – etwa von einer Woche – auf die Stellungnahme zu warten. Gerade aus diesem Grund bietet sich ein solches Vorgehen im Fall der Herausgabe der Verbindungsdaten an. Eine Beteiligung der für den Datenschutz zuständigen Stellen ist in der StPO bisher noch nirgends vorgesehen. Dies ist damit zu erklären, dass bei allen anderen Ermittlungsmaßnahmen eine solche Beteiligung entweder nicht erforderlich ist, da der Betroffene von den Maßnahmen Kenntnis hat und sich somit selbst verteidigen kann, oder nicht möglich, da eine vorherige Anhörung der für den Datenschutz zuständigen Stellen zu einer Verzögerung führen würde, die die Ermittlungen gefährden könnte. Dies ist jedoch, sobald die Telekommunikationsverbindungsdaten auf Vorrat gespeichert werden, bei

Maßnahmen nach §§ 100g, 100h StPO nicht der Fall. Hier bietet sich also eine Beteiligung der für den Datenschutz zuständigen Stellen geradezu an.

Sollte ausnahmsweise keine Zeit zum Abwarten der Stellungnahme vorhanden sein, kann dem Richter die Möglichkeit eingeräumt werden, die Anordnung auf Antrag der Staatsanwaltschaft auch ohne vorherige Stellungnahme zu treffen. In diesem Fall sollte den für den Datenschutz zuständigen Stellen die Gelegenheit gegeben werden, die Stellungnahme nachzuholen. Praktisch relevant wird dieser Fall wohl auch nur bei präventiven Maßnahmen.

dd) Verwertungsverbote, Löschungsgebote

In § 100g Abs. 2 StPO ist auch ein Verwertungsverbot normiert, das für den Fall gilt, dass Verbindungsdaten erlangt worden sind, obwohl dies wegen einem dem Betroffenen zustehenden Zeugnisverweigerungsrecht unzulässig war. Um einen effektiven Schutz vor rechtswidrigen Eingriffen zu erreichen, ist dies unbedingt erforderlich. Auch die Richtlinie verpflichtet die Mitgliedsstaaten in Art. 13 Abs. 2 für einen solchen effektiven Schutz zu sorgen. Diese Pflicht gebietet es, dass für jegliche rechtswidrig erlangte Verbindungsdaten ein Verwertungsverbot besteht. Ansonsten wäre eine rechtswidrige Anordnung ohne Folgen. Das Verwertungsverbot muss daher insoweit ausgedehnt werden, dass es nicht nur bei Verstößen gegen das Zeugnisverweigerungsrecht sondern immer gilt, wenn Verbindungsdaten rechtswidrig erlangt worden sind.

Um eine Nutzung trotz eines Verwertungsverbotes zu vermeiden, muss ebenfalls die sofortige Löschung der Daten angeordnet werden, wenn diese rechtswidrig erlangt worden sind. Die Daten müssen auch dann gelöscht werden, wenn und soweit sie nicht (mehr) zur Strafverfolgung erforderlich sind. Insbesondere sind selbst dann, wenn die Verbindungsdaten eines bestimmten Telefonats für die Ermittlungen von Bedeutung sind, die übrigen aufgrund derselben Anordnung erhobenen Verbindungsdaten zu löschen. Ein solches Gebot ergibt sich aus §§ 100h Abs. 2 S. 3, 100b Abs. 6 StPO. Es sollte jedoch noch um den Fall der rechtswidrig erlangten Verbindungsdaten ergänzt werden.

ee) Offenlegungspflichten

Der Betroffene ist gemäß § 101 StPO über die Maßnahme zu informieren. Dies dient dem Schutz vor einem Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung der Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß¹⁰. Die Bürger haben ein Recht auf Information darüber, wer aus welchem Grund und wie häufig auf ihre Nachrichtenübermittlung zugreift, und Zugang zu öffentlichen oder privaten Datenbanken, die Angaben über Vorgänge dieser Art enthalten, haben¹¹. Nur so kann der Furcht vor der Überwachung der unbefangenen Telekommunikation begegnet werden, so dass die Ausübung der Grundrechte möglich bleibt. An dieser Vorschrift muss daher unbedingt festgehalten werden.

¹⁰ BVerfG, NJW 2005, 1917.

¹¹ vgl. Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses (2006/C 69/04), Ziffer 2.4.4.

5. Zusammenfassung

Zusammenfassend lässt sich feststellen, dass die Zugriffsmöglichkeiten gemäß §§ 100g, 100h StPO insoweit beschränkt werden müssen, dass ein Zugriff auch bei mittels Endeinrichtungen begangenen Straftaten nur dann zulässig sein kann, wenn für sie eine Strafe von bis zu drei Jahren Freiheitsstrafe oder mehr angedroht wird.

Der Zugriff auf die Verbindungsdaten darf dann nicht zulässig sein, wenn ein Zeugnisverweigerungsrecht nach § 53 Abs. 1 StPO betroffen wäre.

Die jetzt in §§ 100h Abs. 1 S. 3, 100b Abs. 1 S. 2 StPO genannte Möglichkeit der Datenerhebung durch die Staatsanwaltschaft bei Gefahr im Verzug muss auf die Anwendung bei präventiven Maßnahmen beschränkt werden. Bei repressiven Maßnahmen besteht kein hinreichender Anwendungsbereich mehr.

Es ist ausdrücklich zu fordern, dass die Anordnung des Richters mit einer ausführlichen Begründung zu versehen ist, aus der sich ergibt, wozu bestimmte Daten erhoben werden sollen und warum die Erhebung gerade dieser Daten erforderlich ist.

Um der Gefahr der schematische Anordnung der Herausgabe der Verbindungsdaten durch den Richter vorzubeugen, und der fehlenden Stellungnahmemöglichkeit des Betroffenen gerecht zu werden, sollte eine Kontrollmöglichkeit geschaffen werden. Die für den Datenschutz zuständigen Stellen der Länder sollten vor der Anordnung daher die Möglichkeit zur Stellungnahme erhalten, um den Richter in kritischen Fällen auf die eventuelle Bedenklichkeit einer von der Staatsanwaltschaft beantragten Anordnung hinzuweisen.

Für rechtswidrig erlangte Daten ist ein umfangreiches Verwertungsverbot einzuführen. Verbindungsdaten sind unverzüglich zu löschen, wenn sie rechtswidrig erlangt oder für Ermittlungen nicht mehr erforderlich sind.

6. Schlusswort

Dieses Dokument ist ein kostenloser Service von:

PHILIPP GABRYS
RECHTSANWALT

Neue Straße 12-15
24768 Rendsburg

www.gabrys.com
info@gabrys.com
+49 (0) 4331 708 274

Für weiterführende Fragen stehe ich Ihnen gerne zur Verfügung. Dieses Dokument ist urheberrechtlich geschützt. Die nicht geschäftsmäßige Weitergabe dieser Datei in unverändertem Zustand ist zulässig.

Stand: 15.03.2006