Reform der Telekommunikationsüberwachung

Stellungnahme zum Entwurf eines Gesetzes zur Reform der Telekommunikationsüberwachung der Fraktion Bündnis 90/Die Grünen (http://www.gruene-bundestag.de/cms/innen_recht/dokbin/153/153565.pdf)

Vorbemerkung

Der Entwurf ist zu begrüßen und geht in die richtige Richtung. Gegenüber der bestehenden, teilweise verfassungswidrigen Rechtslage enthält er eine Reihe wichtiger Verbesserungen. Im Folgenden werden einige Verbesserungsvorschläge und Kritikpunkte angesprochen. Diese ändern nichts an der grundsätzlich positiven Beurteilung des Entwurfs.

A. § 100a Abs. 1 StPO-E - Anwendungsbereich

Der staatliche Zugriff auf Informationen über die Kommunikation und die Kommunizierenden („Verkehrsdaten“, „Bestandsdaten“) sollte den gleichen Voraussetzungen unterliegen wie der Zugriff auf die Inhalte der Kommunikation. Dazu sind Verkehrs- und Bestandsdaten in den Anwendungsbereich der §§ 100a, 100b StPO einzubeziehen.

Wenn verbreitet angenommen wird, der Zugriff auf TK-Inhalte sei eingriffsintensiver als der Zugriff auf Verkehrsdaten, beruht dies auf einem Irrtum. Die Eingriffstiefe bestimmt sich dem Bundesverfassungsgericht zufolge entscheidend nicht nach der Art der Daten, sondern nach deren Nutzbarkeit und Verwendungsmöglichkeiten. Die Verwendungsmöglichkeiten von Verkehrsdaten sind enorm und größer als bei Inhaltsdaten. Die automatisierte Verarbeitung und Verknüpfung der computerlesbaren Verkehrsdaten ermöglicht die Abbildung von Freundschafts- und Beziehungsnetzwerken, die Erstellung von Bewegungsprofilen, die Identifizierung von Interessen, politischer Einstellung usw. anhand der Kommunikationspartner (z.B. Partei, Arzt für Geschlechtskrankheiten). Auch können Verkehrsdaten in großen Mengen mit geringem finanziellen oder personellen Aufwand erhoben und analysiert werden. All dies ist bei Inhaltsdaten nicht möglich. Insgesamt sind Verkehrsdaten nicht weniger schutzwürdig als Kommunikationsinhalte und bedürfen des gleichen Schutzes. Zur näheren Begründung wird auf Breyer, Vorratsspeicherung, Seiten 211 ff. (www.vorratsspeicherung.de.vu) verwiesen. Die österreichische Strafprozessordnung verfolgt diesen richtigen Ansatz bereits (§ 149a öStPO).

Auch für Bestandsdaten muss die gleiche Eingriffsschwelle gelten, denn Bestandsdaten ermöglichen erst die Zuordnung bekannter Kommunikationsinhalte zur Person der Beteiligten oder die Erhebung weiterer Kommunikationsinhalte (durch Überwachungsmaßnahmen oder – bei PINs und Passwörtern – durch unmittelbaren Zugriff). Die Identität der Kommunikationspartner ist integraler Bestandteil der Kommunikation selbst. Zur näheren Begründung wird auf Breyer, RDV 2003, 218 f. (http://www.starostik.de/downloads/anwalt-berlin-tkg-verfassungsbeschwerde.pdf, Seite 10 f.) verwiesen. Die geltenden Regelun-

gen der §§ 112, 113 TKG sind verfassungswidrig und dringend überarbeitungsbedürftig. Unter anderem sehen sie keinerlei Erheblichkeitsschwelle vor. Das Bundesverfassungsgericht hat eine entsprechende Verfassungsbeschwerde bereits zur Entscheidung angenommen (Az. 1 BvR 1299/05).

Formulierungsvorschlag § 100a Abs. 1 StPO-E: *Zur Aufklärung einer Straftat oder zur Ermittlung des Aufenthaltsortes einer Person, nach der für Zwecke eines Strafverfahrens gefahndet wird, darf die Erhebung, Speicherung oder Übermittlung bestimmter Telekommunikationsinhalte, Verkehrs- oder Bestandsdaten angeordnet werden, wenn bestimmte Tatsachen den Verdacht begründen… (sodann unverändert)*

Die §§ 100g, 100h StPO-E werden damit obsolet.

B. § 100a Abs. 1a und 3 StPO-E – Eingriffsvoraussetzungen

Sehr zu begrüßen ist das Abstellen auf die konkrete Straferwartung anstelle eines Straftatenkatalogs. Der heimliche Zugriff auf die Telekommunikation zwecks Strafverfolgung sollte jedoch beschränkt sein auf Fälle organisierter Kriminalität, in denen eine höhere Strafe als vier Jahre Freiheitsstrafe zu erwarten ist. Die in § 100a Abs. 1a und 3 StPO-E vorgesehenen Eingriffsvoraussetzungen sind zu niedrig angesetzt. Ist „eine Freiheitsstrafe von mindestens einem Jahr zu erwarten“, liegt noch keine schwere Straftat vor, sondern lediglich eine Straftat im mittleren Kriminalitätsbereich. Eine solche rechtfertigt nicht den schwerwiegenden Eingriff der heimlichen TK-Überwachung, die eine Vielzahl Unschuldiger betrifft.

In Schweden setzte eine TK-Überwachung generell eine zu erwartende Freiheitsstrafe von mindestens drei Jahren voraus. Erst im Zuge der terroristischen Anschläge des 11.9.2001 wurde diese Schwelle auf zwei Jahre abgesenkt. In Großbritannien ist eine TK-Überwachung bei gewerbs- oder bandenmäßig begangenen Straftaten oder alternativ bei einer zu erwartenden Freiheitsstrafe von mindestens zwei Jahren zulässig, wobei die Straferwartung unter Außerachtlassung von Vorstrafen bemessen wird. Bei vorbestraften Tätern entspricht dies somit eher einer Straferwartung von drei Jahren. In Deutschland ist der Vergleich zur akustischen Wohnraumüberwachung angebracht, weil abgehörte Telekommunikation typischerweise in Wohnungen stattfindet und Gespräche betrifft, die ohne Telekommunikation im Schutz von Wohnungen geführt werden würden.

Maßgeblich für die Eingriffsschwelle muss neben der Schwere der Straftat sein, welches Maß an Rechtsgüterschutz die Strafverfolgung für die Zukunft gewährleisten kann. Der schwerwiegende Eingriff einer heimlichen TK-Überwachung ist nur zu rechtfertigen, wenn er dem Rechtsgüterschutz dient. Voraussetzung muss danach sein, dass aufgrund bestimmter Tatsachen im Einzelfall zu befürchten ist, dass der Beschuldigte Straftaten dieser Art erneut begehen wird (z.B. bei gewerbs- oder bandenmäßiger Begehung, organisierte Kriminalität).

Formulierungsvorschlag § 100a Abs. 1a StPO-E: *Straftat im Sinne des Absatzes 1 ist eine Tat,*

1. bei der aufgrund bestimmter Tatsachen im Einzelfall anzunehmen ist, dass der Beschuldigte Straftaten dieser Art erneut begehen wird ***und***

2. die im Höchstmaß mit Freiheitsstrafe von über fünf Jahren bedroht ist ***und***

3. die sich gegen Leib, Leben oder Freiheit eines anderen richtet oder aufgrund bestimmter Tatsachen im Einzelfall eine höhere Strafe als vier Jahre Freiheitsstrafe oder die Unterbringung des Beschuldigten in einem psychiatrischen Krankenhaus, allein oder neben einer Strafe, oder in der Sicherungsverwahrung erwarten lässt.

Dadurch wird § 100a Abs. 3 StPO-E obsolet. Satz 1 dieser Vorschrift ist ohnehin zu unbestimmt, soweit er eine „Straftat von erheblicher Bedeutung" voraussetzt, und überschneidet sich darin auch mit dem darauf folgenden Satz.

C. § 100a Abs. 5 StPO-E – Zeugnisverweigerungsrechte

Das Zeugnisverweigerungsrecht muss der Verwertung von Überwachungserkenntnissen generell entgegen stehen, wenn nicht der Kommunikationspartner einer Tatbeteiligung verdächtig ist (ebenso Entschließung der 66. Konferenz der Datenschutzbeauftragten). Außerdem sollte der aus dem Datenschutzrecht bekannte Begriff der „Nutzens" gewählt werden, um klarzustellen, dass auch die Nutzung zu anderen Zwecken als Beweiszwecken untersagt ist (z.B. zur Gewinnung weiterer Beweismittel).

Formulierungsvorschlag § 100a Abs. 5 StPO-E: *Erkenntnisse aus der Überwachung der Telekommunikation dürfen nicht genutzt werden, soweit Kommunikation mit einer zeugnisverweigerungsberechtigten Person erfasst wird und soweit das Zeugnisverweigerungsrecht reicht. Absatz 4 Satz 2 gilt entsprechend.*

Dadurch wird § 100a Abs. 7 StPO-E obsolet. Die Regelungen bezüglich zeugnisverweigerungsberechtigter Personen sollten auch für Verkehrs- und Bestandsdaten gelten, wobei eine einheitliche Regelung vorzugswürdig ist. Ohnehin wäre es wünschenswert, für alle Formen der heimlichen Datenerhebung einheitliche, „vor die Klammer" gezogene Erhebungs- und Verwertungsverbote in der StPO zu verankern.

D. § 100b Abs. 4 StPO-E – Mitteilungspflichten

Die Mitteilungspflichten (§ 100b Abs. 4 Sätze 2 und 3 StPO-E) müssen auch dann gelten, wenn die TK-Überwachung nicht fortgesetzt wird, obwohl die Voraussetzungen des § 100a StPO noch vorliegen. Die Staatsanwaltschaft kann sich nach dem Auslaufen einer Anordnung aus vielerlei Gründen gegen einen Verlängerungsantrag entscheiden.

Formulierungsvorschlag § 100b Abs. 4 StPO-E: *Liegen die Voraussetzungen des §*

*100a nicht mehr vor, so sind die sich aus der Anordnung ergebenden Maßnahmen unverzüglich zu beenden. **Jede** Beendigung ist dem Richter und dem nach Absatz 3 Verpflichteten mitzuteilen. Bei der Mitteilung an den Richter ist auch anzugeben, ob und welche Erkenntnisse durch die Maßnahme gewonnen wurden.*

Die Regelung sollte auch für Verkehrsdaten gelten, wobei deren Einbeziehung in den Anwendungsbereich der §§ 100a, 100b StPO vorzugswürdig ist.

E. § 100b Abs. 5 StPO-E – Zweckbindungsgebot, Protokollierung

Dem grundrechtlichen Gebot der Zweckbindung trägt der Entwurf nicht ausreichend Rechnung. Grundsätzlich dürfen die gewonnenen Daten nur zu dem Zweck verwendet werden, zu dem ihre Erhebung erfolgte, also zu Verfolgung der jeweiligen Anlasstat. Diese Zweckbindung ist gesetzlich anzuordnen (BVerfGE 100, 385 f.; 65, 46). Sie hat für jede unmittelbare oder mittelbare Verwendung zu gelten. Durchbrechungen dieser Zweckbindung bedürfen einer normenklaren gesetzlichen Grundlage.

Das Gebot effektiven Rechtsschutzes erfordert ferner, dass die Verwendung der gewonnenen Daten protokolliert wird (BVerfGE 100, 395). Der Begriff der Verwendung deckt die Speicherung, Übermittlung und Nutzung der Daten ab. Gerade wegen der Heimlichkeit der TK-Überwachung ist dies wichtig, um eine nachträgliche Überprüfung zu ermöglichen.

Formulierungsvorschlag § 100b Abs. 5 StPO-E: *Nach den §§ 100a, 100b erhobene personenbezogene Informationen dürfen nur zu dem Zweck verwendet werden, zu dem ihre Erhebung angeordnet worden war. Die Verwendung zu anderen Zwecken der Strafverfolgung ist zulässig, wenn die Erhebung zu diesen Zwecken hätte angeordnet werden dürfen. Die Verwendung zu Zwecken der Gefahrenabwehr bestimmt sich nach § 481. Im Falle des Absatzes 1 Satz 2 Halbsatz 2 ist § 100f Abs. 1 entsprechend anzuwenden. Eine Verwendung zu anderen als den ursprünglichen Zwecken ist zu protokollieren.*

Diese Regelung muss auch für die §§ 100g, 100h StPO gelten. Die dortigen Regelungen genügen den vorgenannten verfassungsrechtlichen Anforderungen nicht (im Einzelnen Breyer, Vorratsspeicherung, 107 f., www.vorratsspeicherung.de.vu). Vorzugswürdig ist es, den Zugriff auf TK-Inhalte und Verbindungsdaten einheitlich zu regeln (siehe oben). Ansonsten muss § 100b Abs. 5 StPO-E jedenfalls entsprechende Anwendung finden.

F. § 100b Abs. 6 StPO-E – Verwertungsverbot, Vernichtung

Es fehlt ein Verwertungsverbot und Vernichtungsgebot im Fall der unzulässigen Datenerhebung (vgl. Entschließung der 66. Konferenz der Datenschutzbeauftragten). Ferner ist eine Ausnahme von der Vernichtungspflicht zu machen, soweit dies zur Benachrichtigung der Betroffenen erforderlich ist (BVerfGE 100, 362).

Formulierungsvorschlag § 100b Abs. 6 StPO-E: *Sind die durch die Maßnahmen er-*

langten Unterlagen zur Strafverfolgung und für eine etwaige gerichtliche Überprüfung nach § 101 Abs. 5 nicht mehr erforderlich oder war ihre Gewinnung rechtswidrig, so sind sie unverzüglich unter Aufsicht der Staatsanwaltschaft zu vernichten; der persönlichen Anwesenheit eines Staatsanwalts bedarf es hierbei nicht. Über die Vernichtung ist eine Niederschrift anzufertigen. Soweit die Vernichtung lediglich für eine etwaige Überprüfung nach § 101 Abs. 5 zurückgestellt ist, sind die Daten zu sperren; sie dürfen nur zu diesem Zweck verwendet werden. Rechtswidrig erlangte Informationen dürfen nicht genutzt werden.

Diese Regelung muss auch für Verkehrs- und Bestandsdaten gelten.

G. § 101 Abs. 1 StPO-E – Ausnahmen von der Benachrichtigungspflicht

Im Urteil zur akustischen Wohnraumüberwachung hat das Bundesverfassungsgericht beanstandet, dass die Begriffe „Gefährdung der öffentlichen Sicherheit“ und „Möglichkeit der weiteren Verwendung eines eingesetzten nicht offen ermittelnden Beamten“ zu weit gehende Ausnahmen statuieren. Dies gilt auch für andere heimliche Überwachungsmaßnahmen.

Formulierungsvorschlag § 101 Abs. 1 StPO-E: *Von den nach §§ 81e, 99, 100a, 100b, 100f Abs. 1 Nr. 2, Abs. 2, §§ 100g und 100h durchgeführten Maßnahmen sind die Betroffenen (Absatz 1a) zu benachrichtigen, sobald dies ohne Gefährdung des Untersuchungszwecks sowie Leib oder Leben einer Person geschehen kann. Bei der Benachrichtigung ist auf die Möglichkeit nachträglichen Rechtsschutzes hinzuweisen. Erfolgt die Benachrichtigung nicht binnen sechs Monaten… (sodann unverändert)*

H. § 101 Abs. 1a StPO-E – Kreis der zu Benachrichtigenden

Wer „Inhaber der überwachten Anschlüsse“ sind, sollte präzisiert werden. Ausweislich der Begründung sind mit „überwachten Anschlüssen“ offenbar auch die Anschlüsse der Kommunikationspartner gemeint. Das muss klargestellt werden. Die mitbetroffenen Anschlussinhaber dürfen nicht nur unter Buchstabe c fallen, zumal das Bundesverfassungsgericht bereits entschieden hat, dass die Vielzahl der betroffenen Personen der Benachrichtigungspflicht nicht entgegen steht (BVerfGE 100, 397 ff.). Zur Benachrichtigung ist es auch nicht erforderlich, dass die Staatsanwaltschaft Name und Kontaktdaten der Betroffenen kennt (siehe unten).

Formulierungsvorschlag § 101 Abs. 1a Nr. 2 StPO-E: *im Fall der §§ 100a, 100b:*

a) Beschuldigte;

b) Inhaber der Anschlüsse, über die Daten erhoben wurden;

c) sonstige von der Überwachung betroffene Personen, soweit diese bekannt sind und

ihre Benachrichtigung ohne weitere Ermittlungen möglich ist; die Benachrichtigung dieser Personen unterbleibt, wenn ihr überwiegende schutzwürdige Belange des Beschuldigten oder der Anschlussinhaber gegenüberstehen;

Entsprechend ist § 101 Abs. 1a Nr. 5 StPO-E zu ändern.

I. § 101 Abs. 1b – neu – StPO-E – Praktische Durchführung der Benachrichtigung

Benachrichtigungen bereiten heutzutage keinen nennenswerten Aufwand mehr, wenn man die technischen Möglichkeiten einsetzt, die man sich auch für die Überwachung selbst zunutze macht. Möglich ist erstens eine Benachrichtigung an den überwachten Anschluss selbst (per SMS, Email, Telefonautomat). Möglich ist zweitens eine Benachrichtigung in der Telefonrechnung. Diese Möglichkeiten machen auch Massenbenachrichtigungen praktikabel, gerade, wenn das Verfahren automatisiert wird.

Sinnvoll erscheint die folgende Vorgehensweise: Die Staatsanwaltschaft übermittelt der Bundesnetzagentur eine Liste der betroffenen Anschlüsse, deren Inhaber zu benachrichtigen sind. Dies verursacht keinen erheblichen Aufwand, da derartige Listen der Staatsanwaltschaft aufgrund der Überwachungsmaßnahme bereits vorliegen. Die Bundesnetzagentur nimmt sodann die Benachrichtigung entweder selbst vor (per Brief, SMS, Email oder Telefonautomat) oder ersucht den jeweiligen Diensteanbieter, die Benachrichtigung in die nächste Rechnung aufzunehmen. Dies kann automatisiert erfolgen und verursacht ebenfalls keinen erheblichen Aufwand. Die Diensteanbieter der Betroffenen können im Wege des automatisierten Auskunftsverfahren nach § 112 TKG ermittelt werden, auf das die Bundesnetzagentur ohnehin Zugriff hat.

Formulierungsvorschlag § 101 Abs. 1b – neu – StPO-E: *Auf Ersuchen der Staatsanwaltschaft veranlasst die Bundesnetzagentur die Benachrichtigung der Inhaber von Telekommunikationsanschlüssen. In dem Ersuchen der Staatsanwaltschaft sind die Kennungen der betroffenen Anschlüsse anzugeben. Auf Verlangen der Bundesnetzagentur sind Diensteanbieter im Sinne der §§ 100b und 100g der Strafprozessordnung verpflichtet, ihren Kunden eine Benachrichtigung zu übermitteln. Den Diensteanbietern sind die hierzu erforderlichen Aufwendungen zu erstatten; § 110 Abs. 9 TKG gilt entsprechend. Zur Ermittlung des jeweiligen Diensteanbieters darf die Bundesnetzagentur das automatisierte Auskunftsverfahren nach § 112 TKG nutzen.*

J. Anlage zu § 100b Abs. 7 StPO – Berichtspflicht

Nicht nachvollziehbar ist, was mit den „in Absatz 9 genannten Kategorien“ gemeint ist.

Bei der vorgesehenen Berichtspflicht ist zu beachten, dass sich der Gesetzgeber bereits anhand repräsentativer Studien wie derjenigen des Max-Planck-Instituts ein Bild von Umfang, Ausmaß und Effektivität der Überwachung machen kann. Sinnvoll ist eine allgemeine

Berichtspflicht daher nur unter dem Aspekt des Rechtfertigungsdrucks. In den USA ist insoweit die Veröffentlichung von Wiretap-Reports der anordnenden Richter vorgesehen. Es erscheint fraglich, ob eine statistisch kumulierte Berichtspflicht wie in dem Entwurf vorgesehen einen ausreichenden Rechtfertigungsdruck erzeugt.

Ferner muss auch der Zugriff auf Verkehrs- und Bestandsdaten durch wissenschaftliche Untersuchungen oder durch Berichtspflichten evaluiert werden. Das Gleiche gilt für Eingriffe in das Fernmeldegeheimnis durch andere Behörden (z.B. Nachrichtendienste). Wichtig wäre weiter eine unabhängige Untersuchung der positiven und negativen Auswirkungen der TK-Überwachung auf die Gesellschaft insgesamt (Senkung der Kriminalitätsrate? Behinderung der freien Meinungsäußerung oder der Tätigkeit von Berufsgeheimnisträgern?). Entsprechende Regelungen sieht der Entwurf noch nicht vor.