Schleswig-Holsteinischer Landtag
Umdruck 16/1857

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

ULD • Postfach 71 16 • 24171 Kiel

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Herr Bergemann
Durchwahl: 988-1216

Aktenzeichen:
LD5-73.03/99.091

Vorsitzenden
des Innen- u. Rechtsausschusses
des Schleswig-Holsteinischen Landtags
Herrn Werner Kalinka
Postfach 7121
24171 Kiel

Kiel, 12. März 2007

Referentenentwurf des Bundesministeriums der Justiz für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG
Sitzung des Innen- und Rechtsausschusses vom 17.01.2007

Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

in seiner Sitzung am 17.01.2007 hat der Innen- und Rechtsausschuss das Unabhängige Landeszentrum für Datenschutz gebeten, zu dem o. g. Gesetzesentwurf Stellung zu nehmen. Dieser Bitte kommen wir gerne nach.

Das mit dem Entwurf verfolgte Ziel, ein in sich schlüssiges Gesamtsystem strafprozessualer heimlicher Ermittlungsmethoden zu schaffen sowie die umfassende aktuelle Rechtsprechung des Bundesverfassungsgerichts umzusetzen, ist ausdrücklich zu begrüßen. Dieses Ziel erreicht der Entwurf jedoch nur unzureichend (dazu I.).

Die mit dem Entwurf vorgeschlagene Einführung der Vorratsdatenspeicherung durch Umsetzung der EG-Richtlinie (Richtlinie 2006/24/EG) ist verfassungsrechtlich äußerst bedenklich. Dies hatten wir in unserer Stellungnahme vom 04.10.2006 (Umdruck 16/1267) dargelegt (dazu II.).

I. Reform der verdeckten Ermittlungsmethoden in der Strafprozessordnung

1. Die notwendige konsequente Umsetzung der Rechtsprechung des Bundesverfassungsgerichts beginnt mit einer an den Grundsätzen der Verhältnismäßigkeit sowie der Normenklarheit und -bestimmtheit orientierten Überarbeitung der *Eingriffsvoraussetzungen* verdeckter Ermittlungsmaßnahmen. Weiterer Schwerpunkt der Neuregelung muss ein umfassender *Schutz des Kernbereichs privater Lebensgestaltung* sowie der rechtsstaatlich notwendige möglichst einheitliche *Schutz von Zeugnisverweigerungsrechten* sein. Die Einhaltung der materiellen Eingriffsvoraussetzungen des Kernbereichsschutzes und des Schutzes von Zeugnisverweigerungsrechten bedarf *effektiver Verfahrenssicherungen*. Verfahrenssicherungen,

wie etwa Richtervorbehalte, können jedoch eine rechtsstaatlich saubere Ausgestaltung der Eingriffsvoraussetzungen und der Eingriffsbegrenzungen nicht ersetzen, sondern müssen diese ergänzen.

2. Die Regelungen des Gesetzesentwurfs senken **Eingriffsschwellen** und sonstige Eingriffsvoraussetzungen, nicht nur bei der Telekommunikationsüberwachung. Im Ergebnis wird es voraussichtlich zu einer erheblichen Ausweitung von Eingriffen in das grundrechtlich geschützte Telekommunikationsgeheimnis und in das Recht auf informationelle Selbstbestimmung kommen. Der Entwurf räumt tatsächlichen oder vermeintlichen Sicherheitsinteressen den Vorrang ein.

3. Wichtiges Beispiel dafür ist die *Telekommunikationsüberwachung*. Bereits der bisherige Straftatenkatalog des § 100a Strafprozessordnung (StPO) hat inzwischen eine kaum überschaubare Weite. Dies wirkt sich auf die Anwendungspraxis aus, wie die gestiegenen Fallzahlen deutlich zeigen. Statt auf diese Entwicklung einschränkend zu reagieren, wurden aus dem Straftatenkatalog lediglich solche Delikte herausgestrichen, die in der Praxis ohnehin gar nicht oder kaum vorkommen, so etwa die Fahnenflucht (vgl. § 100a Satz 1 Nr. 1d StPO). Zugleich sind die Erweiterungen beträchtlich, z.B. durch die Aufnahme bestimmter Urkunds- oder Betrugsdelikte. Die Gestaltung des Anlasstatenkataloges in § 100a StPO-E wirkt sich auf verschiedene *weitere Vorschriften* aus. Betroffen sind etwa die Vorschriften zum Abhören des außerhalb von Wohnungen nicht öffentlich gesprochenen Wortes gem. § 100 f. StPO-E.

4. Die mit Artikel 2 des Entwurfs verfolgte Einführung der Vorratsspeicherung von Telekommunikationsverbindungsdaten führt zugleich zur Unverhältnismäßigkeit der in Artikel 1 des Entwurfs vorgesehenen Überarbeitung der *Verbindungsdatenabfrage* (§ 100g StPO-E). Während die EU-Richtlinie zur Vorratsdatenspeicherung vorsieht, dass die aufgrund dieser Speicherungsverpflichtung gespeicherten Daten nur zur Verfolgung schwerer Straftaten eingesetzt werden dürfen, will der Entwurf in § 100g Abs. 1 Nr. 2 StPO-E eine Verbindungsdatenabfrage bereits bei jedem Verdacht einer „mittels Telekommunikation“ begangenen Straftat ermöglichen. Der Gesetzentwurf fordert nicht, dass diese auch schwere Straftaten bzw. Straftaten von erheblicher Bedeutung sein müssen und geht damit über die Vorgaben der Richtlinie hinaus (vgl. Art. 1 Abs. 1 der Richtlinie).

   Nach der Entwurfsbegründung (S. 57 f.) soll die Herausgabe von Verbindungsdaten im Falle *dynamischer IP-Adressen* sogar praktisch voraussetzungslos möglich sein, da diese pauschal als sog. Bestandsdatum eingestuft werden. Damit werden IP-Adressen datenschutzrechtlich in die Nähe von einfachen Telefonbucheinträgen gerückt. Eine Abfrage bedarf dann nicht mehr der Voraussetzungen des § 100g StPO-E, sondern ist nach § 113 TKG möglich und kann z.B. zur Aufklärung von Ordnungswidrigkeiten eingesetzt werden. Dies wird der Sensibilität des Datums nicht gerecht. Die IP-Adresse wird in der Praxis faktisch von den meisten Internetanbietern „mitgeloggt“. Erhalten die Behörden Zugriff auf Logdateien, so lassen sich umfassende Interessenprofile des Betroffenen abbilden. So ließe sich etwa bei einem Besuch einer Online-Zeitung genau nachvollziehen, für welche Zeitungsartikel er sich interessiert hat. Verknüpft man die Log-Dateien verschiedener Anbieter, lässt sich mit Hilfe der Vorratsdatenspeicherung ein umfassendes Persönlichkeitsbild erstellen. Hierauf soll nach der Gesetzesbegründung –

abgesehen vom einfachen Tatverdacht, der sehr leicht gegeben sein kann – ohne jede Eingriffsschwelle zugegriffen werden können. Ein Richtervorbehalt besteht in diesem Falle ebenfalls nicht.

5. Deutlich abgesenkt werden durch die neue Fassung des § 100g StPO-E die Voraussetzungen für die so genannte *Zielwahlsuche*, die eine Vielzahl unbeteiligter Personen erfasst. Auch die so genannte *Funkzellenabfrage* wird nur rudimentär mit wenigen Worten im Rahmen der allgemeinen Verkehrsdatenerhebung erwähnt. Hierbei handelt es sich um einen tief greifenden Grundrechtseingriff, der in erster Linie unverdächtige Bürgerinnen und Bürger betrifft, die durch ihr Verhalten keinen Anlass für strafrechtliche Ermittlungseingriffe gegeben haben (s. hierzu etwa 28. Tätigkeitsbericht des ULD, Ziff. 4.3.2). Die weitgehende Regelung ohne Begrenzung auf schwere Straftaten ist unverhältnismäßig. Nicht nachzuvollziehen ist auch, weshalb das Gesetz auf eine Regelung des Umgangs mit den erlangten Daten vollständig verzichtet. Beispiel für eine kleine Veränderung mit großer Wirkung ist auch der Verzicht auf das Tatbestandsmerkmal *„im Falle einer Verbindung“*. Dies führt dazu, dass in Zukunft die Erhebung von Standortdaten bei Mobiltelefonen in Echtzeit für zulässig erklärt wird. Damit können die Strafverfolgungsbehörden in Zukunft Bewegungsbilder einer Person in Echtzeit erstellen. Dies zeigt die besondere Eingriffsintensität der Vorschrift zur Verbindungsdatenabfrage.

6. Auch im Strafprozessrecht können **Kontakt- oder Begleitpersonen** Ziel verdeckter Ermittlungsmaßnahmen sein. Dies betrifft etwa Telekommunikationsüberwachung (§ 100a StPO-E), akustische Wohnraumüberwachung (§ 100c StPO-E), Abhören des außerhalb von Wohnungen nicht öffentlich gesprochenen Wortes (§ 100 f StPO-E), längerfristige Beobachtung (§ 100h StPO-E), Einsatz des IMSI-Catchers (§ 100i StPO-E), Ausschreibung zur polizeilichen Beobachtung (§ 163e StPO-E), längerfristige Observation (§ 163f StPO-E). Um als Nichtverdächtiger zum Ziel verdeckter Ermittlungsmaßnahmen zu werden, reicht die Annahme der Strafverfolgungsbehörden aus, mit dem Beschuldigten in Verbindung zu stehen. Freunde und Bekannte des Verdächtigen können schon dann ins Visier der Richtmikrofone, Wanzen und Abhöreinrichtungen geraten, wenn die Polizei sich aus deren Gesprächen einen Aufschluss über den Aufenthaltsort des Verdächtigen erhofft (vgl. etwa § 100 c Abs. 3 StPO-E). Eine wesentlich präzisere Fassung bzw. gesetzliche Abgrenzung des Kreises der Kontakt- und Begleitpersonen wäre ebenso zu wünschen gewesen wie eine deutliche Anhebung der Eingriffsschwellen. Es ist fraglich, ob die bloße Ermittlung des Aufenthaltsorts eines Verdächtigen auch das heimliche Abhören von Gesprächen Nichtverdächtiger rechtfertigen kann.

7. Die verwendeten **Subsidiaritätsklauseln** zeigen, dass der Gesetzesentwurf das selbst proklamierte Ziel einer Harmonisierung und Präzisierung der verdeckten Ermittlungsmaßnahmen nicht erreicht. Die Subsidiaritätsklauseln dienen der Entscheidung, ob andere, weniger in die Grundrechte eingreifende Ermittlungsmethoden vorrangig anzuwenden sind. Diese sind im Entwurf jedoch für die einzelnen Ermittlungsmaßnahmen höchst unterschiedlich geregelt; teilweise gilt keinerlei Subsidiaritätsklausel, sondern es wird lediglich die sachliche Erforderlichkeit einer Ermittlungsmethode verlangt. Subsidiaritätsbestimmungen, wie „wesentlich erschwert“ oder „unverhältnismäßig erschwert“, stellen in der Praxis keine hinreichend bestimmte Begrenzung für den Einsatz verdeckter Ermittlungsmaßnahmen dar.

8. Verdeckte Ermittlungsmaßnahmen dürfen niemals in den **Kernbereich privater Lebensgestaltung** eingreifen. Dies hat das Bundesverfassungsgericht in seinen Entscheidungen vom 03.03.2004 (Großer Lauschangriff) und vom 27.07.2005 (präventive Telekommunikationsüberwachung) mit aller Deutlichkeit klargestellt. Diese Entscheidungen des Bundesverfassungsgerichts dürfen nicht als spezielle Entscheidungen zum in Art. 13 Grundgesetz garantierten Grundrecht auf Unverletzlichkeit der Wohnung bzw. zum in Art. 10 Grundgesetz garantierten Fernmeldegeheimnis gesehen werden. Das Bundesverfassungsgericht hat die Frage des Kernbereichsschutzes vielmehr an dem für sämtliche heimliche Ermittlungsmaßnahmen zentralen Maßstab des Grundgesetzes, nämlich an der Menschenwürdegarantie – und dem damit verbundenen allgemeinen Persönlichkeitsrecht – gemessen.

   Der durch Art. 1 Abs. 1 GG absolut geschützte Achtungsanspruch verbietet zwar nicht sämtliche heimlichen Beobachtungen, es ist jedoch stets ein unantastbarer Kernbereich privater Lebensgestaltung zu wahren (Urteil vom 03.03.2004, Abs. 118). Würde der Staat in diesen unantastbaren Kernbereich eindringen, verletzte dies die jedem Menschen unantastbar gewährte Freiheit zur Entfaltung in den ihn betreffenden höchstpersönlichen Angelegenheiten. Dieser Kernbereich ist *nicht relativierbar*. Das heißt: Auch überwiegende Interessen der Allgemeinheit können einen Eingriff nicht rechtfertigen.

   Damit steht der *Inhalt der Kommunikation bzw. der Interaktion* im Vordergrund, nicht der Ort der Kommunikation und auch nicht das Mittel der Kommunikation. Ein intimes Gespräch zwischen engsten Vertrauten – etwa Ehe- oder Lebenspartnern – berührt nicht nur in einer Wohnung den Kernbereich der persönlich-vertraulichen Kommunikation, sondern z. B. auch während einer gemeinsamen Autofahrt oder in einem Telefongespräch. Auswirkungen ergeben sich daher nicht nur für die akustische Wohnraumüberwachung – den Großen Lauschangriff i.S.d. § 100c StPO – , sondern daneben auch für weitere verdeckte Maßnahmen, bei denen ein Eingriff in den Kernbereich der privaten Lebensgestaltung bzw. der persönlich-vertraulichen Kommunikation möglich ist:

   - Überwachung der Telekommunikation - § 100a Abs. 1 StPO-E
   - Aufzeichnung des nicht öffentlich gesprochenen Wortes außerhalb von Wohnungen, § 100f StPO-E
   - Postbeschlagnahme, §§ 99, 100 StPO
   - Einsatz verdeckter Ermittler, §§ 110a ff StPO
   - (Heimliche) Herstellung von Bildaufnahmen, § 100f Abs. 1 Nr. 1 StPO-E
   - Einsatz technischer Mittel, § 100 f Abs. 1 Nr. 2 StPO-E
   - Längerfristige Observation, § 163f StPO

   Dass im Ergebnis lediglich zur akustischen Wohnraumüberwachung und zur Telekommunikationsüberwachung Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung eingeführt werden, ist angesichts der klaren Ausführungen des Bundesverfassungsgerichts zur Betroffenheit der Menschenwürde bzw. zum Schutz der persönlich-vertraulichen Kommunikation unverständlich. Aus unserer Sicht ist es daher

erforderlich, zumindest für die genannten Maßnahmen einen *„vor die Klammer gezogenen“* Kernbereichsschutz zu regeln.

9. Soweit der Entwurf kernbereichsschützende Vorschriften enthält, sind diese aus unserer Sicht unzureichend. Zum Schutz des Kernbereichs hat das Bundesverfassungsgericht ein gestuftes Vorgehen vorgezeichnet. Vor Durchführung der Maßnahme ist auf der *ersten Stufe* eine *Prognoseentscheidung* zu treffen, ob das abgehörte Gespräch bzw. das überwachte Verhalten den Bereich des Höchstpersönlichen betreffen wird. Hierfür sollte das Gesetz Kriterien nennen, um den Ermittlungsbeamten eine Prognoseentscheidung zu ermöglichen.

   Die überwachten *Gespräche sind „in der Regel durch eine Gemengelage unterschiedlicher Inhalte geprägt“* (Bundesverfassungsgericht, Urteil vom 03.03.2004, Abs. 178). Ein absolutes Verbot der Datenerhebung besteht nach Ansicht des Bundesverfassungsgerichts daher bereits dann, wenn nur ein *Teil des Gesprächs* diesen Bereich betreffen wird. Daher ist es verfassungsrechtlich nicht hinnehmbar, wenn der Entwurf den Kernbereichsschutz erst dann gewährt, wenn das Gespräch <u>*allein*</u> (!) den Kernbereich privater Lebensgestaltung betrifft, wie dies in § 100a Abs. 4 Satz 1 StPO-E nunmehr geregelt sein soll. Damit bleiben die klaren Vorgaben aus Karlsruhe schlicht unbeachtet.

10. Erscheint angesichts der Prognoseentscheidung die Überwachungsmaßnahme möglich, dann ist auf der *zweiten Stufe* das Abhören und die Aufzeichnung der Gespräche *ständig zu kontrollieren,* auf der *dritten Stufe* ist der Gesetzgeber verpflichtet, für den Fall einer versehentlichen Erlangung von Kenntnissen aus dem Kernbereich privater Lebensgestaltung das Gebot der sofortigen *Löschung* dieser Erkenntnisse zu regeln. Für die Telekommunikationsüberwachung formuliert das Bundesverfassungsgericht: „Hinzu müssen Vorkehrungen kommen, die sichern, dass die Kommunikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert […] werden dürfen, sondern unverzüglich gelöscht werden, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist“ (Urteil vom 27.07.2005, Abs. 163). Die Regelung in § 100a Abs. 4 StPO-E sieht jedoch für bereits laufende Abhörmaßnahmen kein ausdrückliches Gebot zum Abbruch der Überwachung vor und entspricht daher nicht den verfassungsgerichtlichen Vorgaben. Wir schlagen daher vor, folgende Formulierung aufzunehmen:

    „Die beteiligten Stellen haben die Datenerhebung sowie die Auswertung der erhobenen Daten sofort abzubrechen, sofern unerwartet erkennbar wird, dass auch Daten erfasst werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Während der Datenerhebung ist dies ständig zu kontrollieren.“

11. Das Ziel, einen einheitlichen **Schutz der Zeugnisverweigerungsberechtigten** auch bei verdeckten Ermittlungsmaßnahmen zu schaffen, ist grundsätzlich sehr zu begrüßen. Die Schutzansprüche der Zeugnisverweigerungsberechtigten drohen jedoch durch weiche Abwägungsklauseln verwässert zu werden. Die im Entwurf vorgenommene Differenzierung nach verschiedenen Klassen von Zeugnisverweigerungsberechtigten ist nicht nachvollziehbar und untergräbt einen wirksamen Grundrechtsschutz. Der Entwurf unterscheidet zwischen Geistlichen, Strafverteidigern sowie Abgeordneten auf der einen Seite (§ 53b Abs. 1 StPO-E) und Rechtsanwälten, Steuerberatern, Ärzten und ähnlichen Personen sowie Journalisten auf der

anderen Seite (§ 53b Abs. 2 StPO-E). Nur bei der ersten Gruppe sind die verdeckten Ermittlungsmaßnahmen unzulässig. Bei der zweiten Gruppe sind die Zeugnisverweigerungsrechte bei der heimlichen Überwachung lediglich „im Rahmen der Prüfung der Verhältnismäßigkeit und der Würdigung des öffentlichen Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen“. Diese wortreiche Abwägungsklausel lässt jeden *objektiv messbaren Maßstab* vermissen. Aus welchem Grund wird ein Arzt oder Rechtsanwalt weniger geschützt als ein Strafverteidiger oder Geistlicher? Die Sachentscheidung wird damit faktisch der Exekutive überlassen, eine Entscheidung frei von subjektiver Willkür ist – auch bei bestem Willen der handelnden Beamten – kaum möglich.

12. Im Rahmen der **Verfahrenssicherungen** fällt zunächst der **Vorbehalt einer richterlichen Entscheidung** vor Durchführung der einzelnen Überwachungsmaßnahme ins Auge. Hierfür sollte der Entwurf jedoch durchgängig *Begründungspflichten* vorsehen. Das Max-Planck-Institut für Ausländisches und Internationales Strafrecht hat in einer Studie von 2003 lediglich 23,5 % der Beschlüsse zur Durchführung einer Telekommunikationsüberwachung als substantiell begründet gewertet. Die Untersuchung von Backes und Gusy konstatiert eine Erosion des Richtervorbehalts und den „weitgehenden Verzicht der Richter selbst, die ihnen vom Gesetz aufgegebene eigenständige und grundrechtsorientierte Prüfung der staatsanwaltschaftlichen Anträge auf Telefonüberwachung vorzunehmen“ (Backes/Gusy u. a., StV 2003, 249, 252). Daher ist nicht verständlich, dass der Entwurf – außer in den Fällen der akustischen Wohnraumüberwachung, § 100d StPO-E – auf eine gesetzlich normierte Pflicht zur einzelfallbezogenen Begründung verzichten will.

13. Die geplante Neuregelung der **Benachrichtigungspflichten** in § 101 Abs. 4-7 StPO-E sollte nachgebessert werden. Die Vorschrift spricht bei den zu benachrichtigenden Personen in Nr. 4b von „sonstigen überwachten Personen“ und in Nr. 5 ff von „erheblich mit betroffenen Personen“. Diese Begriffe sind unklar. Zu benachrichtigen sind sämtliche Personen, die in irgendeiner Weise durch die Überwachungsmaßnahme betroffen worden sind, in deren Grundrechte also eingegriffen worden ist. Die Benachrichtigungspflicht ist die Grundlage für die Möglichkeit der Betroffenen, die Rechtmäßigkeit der Maßnahme durch ein Gericht überprüfen lassen zu können. Wer nicht weiß, ob eine Maßnahme gegen ihn durchgeführt wurde, hat keinerlei Möglichkeit, sich vor Gericht gegen eine ungerechtfertigte Datenverarbeitung zur Wehr zu setzen und etwa Berichtigung, Löschung oder Sperrung zu verlangen. Die Garantie, dass jeder die Gerichte anrufen kann, wenn er sich durch die öffentliche Gewalt in seinen Rechten verletzt fühlt, würde ohne Auskunft und Benachrichtigung ins Leere führen. Benachrichtigung und Auskunft sind also direkter Ausfluss der Rechtsweggarantie in Artikel 19 Abs. 4 des Grundgesetzes, die nur in äußerst eng begrenzten Ausnahmefällen Einschränkungen zulässt. Darüber hinaus handelt es sich „… um ein spezifisches Datenschutzrecht, das gegenüber der Informations- und Daten verarbeitenden staatlichen Stelle geltend gemacht werden kann“ (BVerfGE 100, 313, 361).

Inakzeptabel ist, dass beim Einsatz verdeckter Ermittler die Verschiebung der Benachrichtigung auch dann zulässig sein soll, wenn sonst der weitere Einsatz des Ermittlers gefährdet werden kann. Das Bundesverfassungsgericht hat beim Lauschangriff eine solche Einschränkung für

verfassungswidrig erklärt. Nicht nachvollziehbar ist weiterhin, aus welchem Grund mit einer Benachrichtigung bis zu 12 Monate gewartet werden kann, ehe ein Gericht eingeschaltet werden muss. Eine länger als sechs Monate andauernde Frist ist nicht gerechtfertigt. Verfassungsrechtlich äußerst bedenklich ist schließlich das Ende der Benachrichtigungspflicht nach fünf Jahren, wie § 101 Abs. 7 StPO-E dies vorsieht. Es ist in aller Deutlichkeit hervorzuheben: Die *Strafverfolgungsbehörden dürfen nicht zu Geheimdiensten gemacht werden*, indem ihnen eine dauerhafte Heimlichkeit ihrer Maßnahmen zugebilligt wird. Jede Bürgerin und jeder Bürger hat nach Abschluss der Maßnahmen – spätestens nach Abschluss der Ermittlungen – einen Anspruch auf vollständige Transparenz. Einschränkungen sind nur zum Schutz höchstrangiger Rechtsgüter zulässig, etwa bei Gefahr für Leib oder Leben einer Person.

14. Sehr zu begrüßen ist, dass die Möglichkeit des **Rechtsschutzes** gegen verdeckte Ermittlungsmaßnahmen nunmehr ausdrücklich geregelt werden soll (§ 101 Abs. 9 StPO-E). Die *Frist von 14 Tagen* für den Antrag auf Überprüfung der Rechtmäßigkeit der Maßnahme erscheint allerdings als *zu kurz*. Die Benachrichtigung dürfte für die Betroffenen in der Regel äußerst überraschend kommen. Anders als im laufenden gerichtlichen Verfahren hatten die Betroffenen daher in der Regel zunächst keine Gelegenheit, sich anwaltlich beraten zu lassen oder einen Verteidiger zu suchen. Viele Betroffene, denen oft jede juristische Vorbildung fehlt, dürften mit einer solch kurzen Frist überfordert sein.

15. Eine Überarbeitung der Vorschriften über verdeckte Ermittlungsmaßnahmen ist grundsätzlich zu begrüßen. Allerdings sollte diese Überarbeitung auf Grundlage einer umfassenden **wissenschaftlichen Evaluation** durch eine unabhängige Stelle erfolgen. Eine solche Evaluation ist bislang nur für die Telekommunikationsüberwachung und für den Großen Lauschangriff durchgeführt worden. Ob alle in den bisherigen Studien festgestellten Defizite durch die Neuregelung beseitigt wurden, erscheint nach den obigen Ausführungen fraglich. Erforderlich ist wenigstens eine auch in Zukunft regelmäßig vorzunehmende Evaluation der verdeckten Ermittlungsmaßnahmen.

II. Umsetzung der Richtlinie zur Vorratsdatenspeicherung

1. Das Unabhängige Landeszentrum für Datenschutz hat zur Umsetzung der EG-Richtlinie 2006/24/EG vom 15.03.2006 über die Vorratsspeicherung von Daten gegenüber dem Europaausschuss und dem Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtags mit Datum vom 04.10.2006 Stellung genommen (Umdruck 16/1267). Zur Vermeidung unnötiger Wiederholungen verweisen wir vollinhaltlich auf diese Stellungnahme.

2. Daraus ergibt sich insbesondere, dass die Einführung einer verdachtsunabhängigen Vorratsdatenspeicherung gegen **Verfassungsrecht** verstößt (siehe dazu Ziff. 6 ff der Stellungnahme). Darüber hinaus ist die Richtlinie erheblichen **europarechtlichen Bedenken** ausgesetzt, weil sie auf der falschen Rechtsgrundlage erlassen worden ist. Die Richtlinie stützt sich auf Art. 95 EGV mit der Begründung, sie diene der Angleichung von Rechts- und Verwaltungsvorschriften zur Verbesserung des Binnenmarktes. Art. 95 EGV ist jedoch keine ausreichende Rechtsgrundlage für eine Maßnahme, die als Rahmenbeschluss der justiziellen Zusammenarbeit in der so genannten „dritten Säule“ hätte beschlossen werden müssen (dazu

Ziff. 18 der Stellungnahme). Die Richtlinie ist zwischenzeitlich Gegenstand einer Nichtigkeitsklage vor dem Europäischen Gerichtshof. Schon vor diesem Hintergrund sollte zunächst auf eine Umsetzung verzichtet und der Ausgang des gerichtlichen Verfahrens abgewartet werden.

3. Die erheblichen Zweifel an der Verfassungsmäßigkeit der Vorratsdatenspeicherung werden durch die im Entwurf vorgesehenen weiten **Zugriffsmöglichkeiten** (siehe oben I.5 f.) und den unzureichenden Schutz der Zeugnisverweigerungsberechtigten (siehe oben I.13) nochmals gesteigert. Beispielsweise im Falle der *Funkzellenabfrage* werden Unverdächtige besonders betroffen (s.o. I.6). Ebenso fällt der nicht ganz klare Adressatenkreis der Regelung ins Auge.

4. Der Entwurf geht teilweise über die Umsetzung der Richtlinie hinaus. Beispiel ist der Bereich der E-Mail-Dienste. Nach der Gesetzesbegründung sind zudem etwa die Betreiber von **Anonymisierungsdiensten** von der Speicherungsverpflichtung umfasst. Der Sinn dieser Dienste wird damit zumindest teilweise ad absurdum geführt. Bevor durch die aktuelle Gesetzgebung in das Recht der Bürgerinnen und Bürger, sich unbeobachtet im Internet zu bewegen, durch ein praktisches Verbot solcher Dienste eingegriffen wird, sollten die bereits vorhandenen Möglichkeiten ausgeschöpft werden. So ist etwa der Diensteanbieter ANON heute technisch in der Lage, die Strafverfolgung bei Vorliegen einer richterlich angeordneten Überwachung zu unterstützen. Diese bezieht sich jeweils auf einen konkreten Tatverdacht und konkret verdächtige kriminelle Inhalte, verzichtet aber auf eine Pauschalverdächtigung aller unbescholtenen Nutzerinnen und Nutzer. Leider werden die bereits heute bestehenden Möglichkeiten von den Strafverfolgungsbehörden kaum angenommen. Ein praktisches Verbot von Anonymisierungsdiensten kann aus der Richtlinie nicht abgeleitet werden. Diese bezieht sich auf Telekommunikationsdienste, nicht jedoch auf Teledienste, zu denen Anonymisierungsserver zu zählen sind.

Auf die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 „Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsverfahren“ weise ich ausdrücklich hin; ich habe sie als Anlage beigefügt. Insgesamt empfehlen wir, dem Entwurf im Bundesrat nicht zuzustimmen.

Mit freundlichen Grüßen

Dr. Thilo Weichert

Anlage: Entschließung der DSB-Konferenz vom 8. März 2007

73. Datenschutzkonferenz des Bundes und der Länder
Erfurt, den 8. - 9. März 2007

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen . Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z. B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.

- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.

- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.

- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.

- Für Angehörige i.S.v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.

- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i.S.v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise

ungeschützt.

- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.

- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht - wie im Entwurf vorgesehen - auf Beweiszwecke begrenzt werden.

- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.

- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.

- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.

- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.