Humanistische Union

Zwischen Ignoranz und Nebelkerzen versinkt ein Grundrecht

Die Einführung der Vorratsdatenspeicherung in Deutschland, Mitteilungen Nr. 199, Seite 1 - 5

Zwischen Ignoranz und Nebelkerzen versinkt ein Grundrecht

Vor einem Jahr hat das Bundesjustizministerium mit einem Referentenentwurf eine lang erwartete Gesamtreform der Telekommunikationsüberwachung eingeleitet. Ein Gesetzentwurf zur „*Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*" sollte die zahlreichen Vorschriften für heimliche Ermittlungsmaßnahmen harmonisieren. Die Ministerin versprach, es gäbe künftig mehr Grundrechtsschutz: Die Telefone würden nur noch zur Verfolgung schwerer Straftaten überwacht, die Betroffenen einen besseren nachträglichen Rechtsschutz erhalten und ihr Kernbereich privater Lebensgestaltung umfassender geschützt. Der Bedarf für eine Begrenzung heimlicher Überwachungsmaßnahmen lässt sich kaum von der Hand weisen. Jede Woche werden neue Fälle bekannt, in denen die Sicherheitsbehörden fantasiereiche Begründungen für das Abhören von Telefonen oder das heimliche Filzen der Post Verdächtiger aufbringen. Bei der Ausführung dieser „Maßnahmen“ legen die Ermittler gern selbst Hand an. Dass dabei Zeugnisverweigerungsrechte von Journalisten und Anwälten missachtet oder das Post- und Fernmeldegeheimnis unbeteiligter Dritter verletzt wird, scheint die Ermittler nicht zu stören. Das Vertrauen, gelegentlicher Übereifer der Ermittler ließe sich rechtsstaatlich geordnet beheben, ist derzeit schwer beschädigt. Umso höher sind die Erwartungen an ein Gesetz, dass sich genau diesem Problem verschrieben hat. Am 9. November 2007 hat der Bundestag das Gesetz verabschiedet. Das mit ihm eine wirkliche Begrenzung der zuletzt 42.000 Anordnungen zur Telefon-überwachung stattfinden wird, kann niemand ernsthaft erwarten. Dabei stellen die bekannten Zahlen zur Überwachung der Telefon- und Internetnutzer nur die Spitze des Eisbergs heimlicher Ermittlungsmethoden dar. Über die heimliche Beschlagnahmung von Postsendungen, den Einsatz verdeckter Ermittler, das längerfristige Observieren und dergleichen Methoden ist kaum bekannt, wie oft, wie lange und wie erfolgreich sie angewandt werden.

Wenn wir es nicht besser wüssten...

Dies gilt insbesondere für eine zweite Form der Telekommunikationsüberwachung: die Auswertung sogenannter Verkehrsdaten. Diese entstehen bei jedem Anruf, jedem Fax, jeder SMS oder jeder E-Mail. Aus ihnen geht hervor, wer, wann, mit wem, wie und von wo aus kommunizierte. Nach dem am 9. November verabschiedeten Gesetz sollen diese Daten sowohl beim Dienstleister des Anrufers/Senders, als auch beim Dienstleister des Angerufenen/Empfängers für sechs Monate lang gespeichert werden. Die Bundesregierung beruft sich dabei auf ihre Pflicht, eine europäische Richtlinie über die Vorratsdatenspeicherung (2006/24/EG) umzusetzen - mit der Umsetzung der europäischen Datenschutzrichtlinie ließ man sich dereinst mehr Zeit. Die Auswertung solcher Verkehrsdaten für die Verfolgung von Straftaten, aber auch zur Gefahrenabwehr ist nicht neu. Die bis zum Jahresende befristete Regelung der Strafprozessordnung (§ § 100g, 100h StPO) über den Zugriff auf solche Daten wurde vom Bundestag Ende 2004 verabschiedet.

Bereits damals forderte die Humanistische Union die Abgeordneten des Rechtsausschusses auf, für den Zugriff auf die Kommunikationsdaten eine Berichtspflicht im Gesetz zu verankern, damit vor einer erneuten Verlängerung der Regelung zunächst einmal geprüft werden könne, wie oft die Ermittler Verkehrsdaten bisher nutzen, welchen Beitrag die Daten zur Aufklärung von Straftaten leisten und wie viele Personen davon betroffen sind. Darüber fehlten bisher jegliche Angaben. Die Abgeordneten griffen diese Forderung der Humanistischen Union auf und beauftragten die Bundesregierung, bis zum 30. Juni 2007 einen Erfahrungsbericht über die tatsächliche Nutzung der Verbindungsdaten vorzulegen, in dem „*auch auf Anlass, Ergebnisse und Anzahl der Betroffenen der Maßnahmen eingegangen*" wird. (BT-Drs. 15/3971, S. 3)
Im Sommer dieses Jahres veröffentlichte die Deutsche Telekom erstmals Zahlen, wonach bei ihnen 2006 ca. 27.000 Anfragen nach Telefon- verbindungen und 94.000 Anfragen nach Internet-verbindungen eingingen. Darüber, wie viele Personen von einer solchen Anordnung betroffen sind, kann man nur mutmaßen. Rekordverdächtig scheint ein Fall zu sein, den der Bundesrat zur Begründung anführte, warum ein standardisiertes Datenformat für die Auswertung der Verkehrsdaten notwendig sei: „So waren z.B. in einem Ermittlungsverfahren zur Aufklärung von Tötungsdelikten mehrere Millionen Daten zu verarbeiten und auszuwerten." (BR-Drs. 275/07-Beschluss, S. 13) Inzwischen legte Frau Zypries ihren Gesetzentwurf vor, der erstmals eine unbefristete Regelung für den Zugriff auf die Verkehrsdaten enthielt (§ 100g StPO neu). Mit der im Telekommunikationsgesetz eingeführten Vorrats- datenspeicherung wird das Reservoir an verfügbaren Kommunikationsdaten erheblich ausgeweitet. Zwei Gründe mehr, die für eine sorgfältige Prüfung der bisherigen Überwachung des Kommunikationsverhaltens sprechen. Der 30. Juni verstrich, ohne dass der Bericht vorlag. Die Abgeordnete Petra Pau (Die Linke) fragte auf Anregung der Humanistischen Union bei der Bundesregierung nach. Am 2. Juli antwortete der zuständige Staatssekretär des Justizministeriums, Alfred Hartenbach, dass die Bundesregierung dem Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg einen entsprechenden Untersuchungsauftrag erteilt habe, der Bericht stehe kurz vor dem Abschluss. „Sobald die Endfassung vorliegt, wird diese dem Deutschen Bundestag zugeleitet werden." (BT-Drs. 16/6079, S. 53)
Glaubten bis in den Herbst hinein alle, die Forscher wären noch mit der Erstellung des Berichts beschäftigt, so wurde Ende Oktober bekannt, dass der Bericht längst an die Auftraggeber übermittelt worden war. Mit Schreiben vom 1. November 2007 teilte Frau Zypries den Mitgliedern des Rechtsausschusses mit, dass der „Entwurf eines Schlussberichts" inzwischen vorliege, sich die Abnahme des 472seitigen Gutachtens aber noch verzögere. Den Abgeordneten wurden mit gleichem Schreiben vier Seiten mit den Empfehlungen der Wissenschaftler zur Kenntnis gegeben - der „Rest" solle später folgen. Die Zusammenfassung enthielt jedoch eine konkrete Zahlenangabe über die bisherige Praxis, die aufmerksame Leser zum Aufhorchen brachte: „Doch weist die Aktenanalyse selbst unter den heutigen rechtlichen Bedingungen nur für etwa 2% der Abfragen nach, dass sie wegen der Löschungen ins Leere gehen.“ Mit einer Ermittlungslücke von 2% lässt sich die geplante Speicherung aller Verkehrsdaten kaum begründen, die pauschale Außerkraftsetzung des Fernmeldegeheimnisses nicht rechtfertigen. Damit lag es bei den Abgeordneten, die Entscheidung über einen Gesetzentwurf zu vertagen, der auf unbestimmte Dauer das Fernmeldegeheimnis einschränken würde, um sich vorher über die Notwendigkeit und die Auswirkungen dieser Regelung zu informieren. Die Humanistische Union erinnerte die Abgeordneten an ihren Beschluss von 2004, die Abgeordneten von Bündnis 90/Die Grünen stellten im Rechtsausschuss einen entsprechenden Antrag (BT-Drs. 16/6979, S. 56). Allein der Wille, sich gründlich mit den Fakten über die Reichweite der Verkehrsdatenauswertung zu beschäftigen, fehlte den Koalitionären.

Verdunkelungsgefahr?

Bis in die abschließende Plenardebatte konnte sich der interessierte Betrachter nicht sicher sein, dass alle Beteiligten über ein und denselben Gesetzentwurf sprachen. Insbesondere die Justizministerin Brigitte Zypries, die im Vorfeld der Entscheidung Kritikern ein mangelndes Verständnis des Gesetzes und Panikmache vorgeworfen hatte, warf in der Plenardebatte selbst eine ganze Reihe von Nebelkerzen, mit

denen sie das Ausmaß der Überwachung des Kommunikationsverhaltens kleinreden wollte.

Einige Beispiele:

Keine Zwangserhebung von Kommunikationsdaten? Die Bundesjustizministerin wurde nicht müde, immer wieder zu betonen, bei der Vorratsdatenspeicherung gehe es nur darum, ohnehin anfallende Daten etwas länger zu speichern. Die Anbieter von Telekommunikationsdiensten würden weder mit der Richtlinie zur Vorratsdatenspeicherung noch nach dem deutschen Umsetzungsgesetz explizit verpflichtet, personenbezogene Daten zu erheben und zu speichern, die bisher nicht anfielen.

Diese Daten, die für Abrechnungszwecke gebraucht werden, werden gespeichert, nicht mehr und nicht weniger." (Brigitte Zypries lt. Plenarprotokoll der 124. Sitzung des Deutschen Bundestages vom 9.11.2007, S. 12995)

Ein Blick in den verabschiedeten Gesetzentwurf verrät jedoch etwas anderes: Bei der Erhebung von sogenannten Bestandsdaten (Angaben zum Vertragsverhältnis) nach § 111 Absatz 1 des Telekommunikationsgesetzes (TKG) werden die Diensteanbieter künftig dazu verpflichtet, auch die Gerätenummern (IMEI) der verkauften Handys zu registrieren, obwohl sie diese Nummern für ihre Abrechnungen gar nicht benötigen: „*Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat ... in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes ... vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind...*" (BT-Drs. 16/5846, S. 17). Aber auch für die Kommunikationsdaten im engeren Sinne (Verkehrsdaten) ist die Aussage irreführend, die Diensteanbieter müssten nur ohnehin anfallende Daten speichern. Nach §113a Absatz 1 TKG werden alle Anbieter verpflichtet, die Verbindungsdaten für sechs Monate zu speichern, sofern sie solche Daten erzeugen oder verarbeiten. Zwischen der Tatsache, dass jemand Verkehrsdaten erzeugt/verarbeitet und der Frage, ob diese Daten für Abrechnungszwecke benötigt bzw. gespeichert werden, besteht ein großer Unterschied. Dieser Unterschied wird insbesondere bei der elektronischen Weiterleitung von Nachrichten und den sogenannten Anonymisierungsdiensten deutlich, deren Verpflichtung zur Vorratsdatenspeicherung in §113a Absatz 6 TKG ausdrücklich erwähnt wird: „*Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.*" (BT-Drs. 16/5846, S. 18) Bei Anonymisierungsdiensten wie The Onion Router (TOR) oder Java Anon Proxy (JAP), bei denen auf zwischengeschalteten Rechnern der Kommunikationskette eine „Umschreibung" der Verbindungsdaten (IP-Adressen) stattfindet, müssen die Verbindungsdaten der Internetnutzer technisch bedingt immer verarbeitet und für die Dauer einer aktiven Internetverbindung (z.B. 60 Minuten) gespeichert werden. Die Verkehrsdaten werden hierbei üblicherweise aber nicht zu Abrechnungszwecken benötigt, die gebräuchlichsten Anonymisierungsdienste sind kostenfrei nutzbar. Nach dem jetzt verabschiedeten Gesetz müssten die Anbieter von Anonymisierungsdiensten dennoch die Verbindungsdaten ihrer Kunden speichern, auch wenn dies dem Ziel der Anonymisierungsdienste, eine unbeobachtete Kommunikation im Internet zu gewähren, zuwiderläuft. Ähnlich sieht es bei den Anbietern von E-Mail-Diensten aus: Auch hier werden die Verbindungsdaten (wer, wann an wen eine Nachricht schrieb) bisher zu Abrechnungszwecken weder erhoben noch gespeichert. Es ist kein Anbieter von E-Mail-Diensten bekannt, bei dem diese Angaben abrechnungsrelevant wären. Die Einrichtung der elektronischen Postfächer ist entweder kostenfrei (durch Werbung finanziert) oder ihr Preis bestimmt sich nach dem verfügbaren Speichervolumen. Nirgends ist der Preis von der Anzahl der empfangenen Nachrichten, geschweige denn den Absendern abhängig. Die Adressdaten müssen zwar von den Mailservern verarbeitet werden (um etwa zu entscheiden, ob es sich beim Empfänger um ein Postfach auf dem eigenen Server handelt oder die Nachricht alternativ an einen anderen Mailserver weiterzuleiten), jedoch begründet sich daraus kein Recht der Provider, die Absender und

Empfänger der Nachrichten außerhalb dieses Sortierprozesses separat zu erfassen und zu speichern.

Zugriff auf die Vorratsdaten nur bei schwerer Kriminalität?

Einen Zugriff auf diese Daten [gemeint sind die TK Verbindungsdaten] kann es nur geben, wenn man den Verdacht auf eine erhebliche Straftat hat und ein richterlicher Beschluss vorliegt." (Brigitte Zypries lt. Plenarprotokoll, S. 12995)

Leider stimmt weder das erste noch das zweite Kriterium wirklich. In der Neufassung des § 100g Absatz 1 Strafprozessordnung heißt es klipp und klar: „*Begründen bestimmte Tatsachen den Verdacht, das jemand als Täter oder Teilnehmer ... eine Straftat mittels Telekommunikation begangen hat, so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten ... erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist*." (BT-Drs. 16/5846, S. 13) Die Begründung des Gesetzentwurfs weist ausdrücklich darauf hin, dass hier durchaus an Delikte wie die Bedrohung oder Beleidigung am Telefon gedacht wurde. Wohl sieht die Regelung vor, dass in solchen Fällen eine andere Erforschung des Sachverhaltes ausgeschlossen und die Verkehrsdatenabfrage „ *in einem angemessenen Verhältnis zur Bedeutung der Sache*" stehen müsse. Darunter mag jeder verstehen, was sie oder er will – das ändert aber nichts an der Tatsache, dass Verkehrsdaten künftig auch für die Aufklärung leicht- und mittelschwerer Kriminalität verwendet werden.
Der notwendige richterliche Beschluss wackelt, sobald man dem Verweis auf die allgemeinen Verfahrensregeln für Telekommunikationsüberwachungen (§ 100b Absatz 1 StPO) folgt. Dort steht geschrieben, dass Überwachungen der Telekommunikation i.d.R. durch ein Gericht anzuordnen sind. Allerdings ist dies eine Regel mit Ausnahme: „Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden." Ursprünglich sah der Gesetzentwurf vor, dass für den Fall, ein Gericht bestätige nicht die „Gefahr im Verzug", die bis dato erlangten Daten nicht für Beweiszwecke verwendet werden dürfen. Dieses an sich schon weiche Verwertungsverbot (Verbindungsdaten werden oft als Ermittlungsansatz, aber kaum als Beweis verwendet) wurde jedoch in der letzten Beratung des Rechtsausschusses wieder gestrichen. Die Ermittler haben also nichts zu verlieren, sollte ein Gericht dem Eilzugriff auf die Verkehrsdaten widersprechen.

Was dürfen die Geheimdienste?

Entgegen dem vorgeblichen Ziel einer Binnenharmonisierung des europäischen Telekommunikationsmarktes lässt die Richtlinie zur Vorratsdatenspeicherung den Mitgliedsstaaten freie Hand, welche Behörden unter welchen Voraussetzungen auf die Kommunikationsdaten zugreifen dürfen. Da als Ziel der Vorratsdatenspeicherung die Aufklärung terroristischer bzw. schwerer Straftaten ausgegeben wurde, stand in der deutschen Diskussion von Beginn an die Frage im Raum, ob und wie die Geheimdienste auf diese Daten zugreifen dürfen. Frau Zypries behauptete in der Plenardebatte:

Dieses Gesetz enthält überhaupt keine Regelungen über künftige Kompetenzen der Geheimdienste. ... Damit wir uns darüber klar sind: Aufgrund dieses Gesetzes ist kein Zugriff möglich." (Brigitte Zypries lt. Plenarprotokoll, S. 12994)

Auf den ersten Blick scheint diese Aussage richtig: Mit der Änderung des Telekommunikationsgesetzes wird ein grundsätzlicher Zugriff auf die Verkehrsdaten für die Verfolgung von Straftaten, zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit oder zur Erfüllung der gesetzlichen Aufgaben der

Geheimdienste erlaubt, „soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a vorgesehen und die Übermittlung im Einzelfall angeordnet ist". (§ 113b TKG) Dieser Verweis auf den neu geschaffenen § 113a TKG (die Vorratsdatenspeicherung) existiert bisher nur in der Strafprozessordnung (§ 100g Absatz 1 StPO), somit wäre der Zugriff nur den Strafverfolgern bzw. der Polizei zur Gefahrenabwehr erlaubt.
Sofort stellt sich aber die Frage, wie diese Rechtslage praktisch umgesetzt werden soll. Das Bundesamt für Verfassungsschutz, der Militärische Abschirmdienst und der Bundesnachrichtendienst verfügen seit dem Inkrafttreten des Terrorismusbekämpfungsgesetzes (9.1.2002) über weit reichende Befugnisse, um die Bestandsdaten (ohne besondere Voraussetzungen) und die Verkehrsdaten (mit ministerieller Anordnung) von Telekommunikationskunden auszuwerten. Im vergangenen Jahr bekam das Bundesamt für Verfassungsschutz 14 Anordnungen zur Verkehrsdatenauskunft genehmigt, wobei die Kommunikationsdaten von 71 Bürgerinnen und Bürgern betroffen waren (Bericht des Parlamentarischen Kontrollgremiums für 2006, BT-Drs. 16/5982). Auf diese Befugnisse werden die genannten Dienste künftig kaum verzichten wollen, zumal der Gesetzgeber mit dem Terrorismusbekämpfungsergänzungsgesetz die Sonderrechte für den Antiterrorkampf erst Ende 2006 für weitere fünf Jahre verlängert hat. Wie aber kann ein Provider in Zukunft entscheiden, ob er einem Auskunftsersuchen der Geheimdienste folgen und die Daten übermitteln soll? Er müsste dazu unterscheiden, ob diese Daten bei ihm zu Abrechnungszwecken erhoben und gespeichert wurden (was für einige Kunden eine Zeit lang zutrifft), oder ob die Daten aufgrund der Vorratsdatenspeicherung gespeichert wurden (was besonders im Bereich der E-Mail- und Internetkommunikation für die Mehrzahl, für die anderen Kunden nach 3 Monaten gilt). In den bisher bekannt gewordenen Richtlinien über die technische Umsetzung der Vorratsdatenspeicherung ist nicht vorgesehen, bei den jeweiligen Datensätzen zu vermerken, aus welchem Anlass die Speicherung erfolgte bzw. aktuell noch aufrecht erhalten wird. Da das Abrufverfahren für die Nutzung der Verkehrsdaten jedoch automatisiert ablaufen soll (s. Beitrag auf S. 9), eine automatische Erkennung des Speichergrundes nicht möglich ist, steht zu befürchten, dass sich die Geheimdienste aus dem verfügbaren Datenschatz frei bedienen werden. Außerdem dürfte es nur eine Frage der Zeit sein, bis die entsprechenden Verweise auf die Vorratsdatenspeicherung (§113a TKG) in den gesetzlichen Regelungen der Geheimdienste nachgetragen werden.
Damit aber nicht genug: Für den Zugriff der Geheimdienste handelten die Koalitionäre in der abschließenden Beratung des Rechtsausschusses noch eine Hintertür aus. Demnach gilt der Vorbehalt eines gesetzlichen Verweises für den Zugriff auf die Vorratsdaten nicht für das sogenannte manuelle Auskunftsverfahren über die Bestandsdaten der Kunden (§113 TKG), in den § 113b TKG wurde noch folgende Ausnahmeregelung aufgenommen: „... für andere Zwecke mit Ausnahme einer Auskunftserteilung nach § 113 darf er die Daten nicht verwenden." (BT-Drs. 16/6979, S. 34 – Hervorhebung im Original) Das heißt nichts anderes, als dass die Geheimdienste im Verfahren der sogenannten „manuellen Auskunftserteilung" über Bestandsdaten nach §113 TKG auch auf die auf Vorratsdaten zugreifen dürfen. Die manuelle Auskunftserteilung beinhaltet normalerweise die Abfrage von Name, Adresse und Vertragsgrundlagen eines Beschuldigten. Da es sich nicht um Informationen über einen konkreten Kommunikationsvorgang handelt, gelten für sie keine besonderen Anforderungen. Mit dem Gesetzentwurf soll aber, so die Begründung, zugleich die umstrittene Benutzeridentifikation bei dynamischen IP-Adressen (welchem Nutzer war zum Zeitpunkt X die IP-Adresse Y zugeordnet?) als Abfrage nach den Bestandsdaten durchgesetzt werden. Provider hatten sich in der Vergangenheit mehrfach geweigert, derartige Auskünfte ohne die richterliche Anordnung zur Herausgabe von Verbindungsdaten (bisherige § § 100g, 100h StPO) zu erteilen, da mittels einer dynamischen IP-Adresse konkrete Kommunikationsverbindungen eines Internetnutzers ausgewertet werden können. Sollte sich die mit dem Gesetz beabsichtigte Ausweitung der Bestandsdatenabfrage tatsächlich durchsetzen, hieße dies auch, dass die Geheimdienste über diesen Weg die Internetkommunikation ausforschen können.

Alles wird besser?

Davon ist zumindest die Justizministerin überzeugt:

Die TKÜ-Novelle ist eine Novelle, die nur dazu führt, dass die Rechte der deutschen Bundesbürgerinnen und Bundesbürger im Hinblick auf Datenüberwachung oder Abhörmöglichkeiten verbessert werden. Sie werden überhaupt nicht verschlechtert." (Brigitte Zypries lt. Plenarprotokoll, S. 12995)

Lassen wir die grundsätzliche Frage, ob die umfassende Speicherung des Telekommunikationsverhaltens der gesamten Bevölkerung bei den Diensteanbietern wirklich eine Verbesserung des grundrechtlichen Schutzes vor Überwachungsmaßnahmen darstellt, einmal Außen vor. Selbst die in der Strafprozessordnung aufgestellten Regeln, unter welchen Bedingungen und in welchem Umfang die Strafverfolger auf solche Kommunikationsdaten zugreifen dürfen, haben sich mit der verabschiedeten Novelle nicht unbedingt zum Besseren entwickelt:

- Die Verbindungsdatensätze enthalten künftig nicht nur Angaben über die abgehenden Telefonate, Faxnachrichten, SMS-Mitteilungen und E-Mails, sondern auch alle Daten über ankommende Mitteilungen. Damit entfällt das bisher so aufwändige Verfahren der sogenannten Zielwahlsuche bei der Auswertung von Telefondaten (wer hat einen überwachten Anschluss angerufen?). Außerdem genügt jetzt ein Blick in das Verbindungsdatenkonto eines Betroffenen, um sämtliche (gewollten oder ungewollten) Kommunikationspartner von ihm offen zu legen. Wehe dem, der versehentlich von einem Mitglied der militanten Gruppe angerufen wurde!
- Bisher war die Erhebung von Verkehrsdaten an eine laufende Kommunikation gebunden - in § 100g Absatz 3 Nummer 1 StPO wurden die Verkehrsdaten als Daten „im Falle einer Verbindung" definiert. Das verführte findige Strafverfolger bisweilen dazu, einem Verdächtigen sogenannte „stille SMS" (eine auf dem Handy nicht erkennbare Nachricht) zu senden, um die gesetzlich notwendige Telekommunikations-verbindung unbemerkt anzustoßen. Die neue Regelung der „Verkehrsdatenabfrage" setzt keine (menschliche) Kommunikation mehr voraus, sondern erlaubt es, jede technische Signalübertragung mit dem Endgerät zu nutzen. Somit können die Standortdaten eines Mobiltelefons im eingeschalteten Zustand ermittelt werden, ohne dass die Benutzer auch nur ein Gespräch führen müssten, die „Anmeldung" des Handys bei der nächstgelegenen Funkzelle reicht aus. Gleiches gilt für Computer, die sich über eine Netzwerkschnittstelle mit ihrer Umgebung verbinden.
- Bisher regelten die § § 100g und 100h der Strafprozessordnung einen umfassenden Auskunftsanspruch der Strafverfolger gegenüber den Dienstleistern: Jene mussten auf Anfrage sämtliche gespeicherten Verbindungsdaten eines Anschlusses mitteilen oder wurden verpflichtet, für die nächsten drei Monate alle Kommunikationsverbindungen an die Strafverfolger weiterzugeben. Die neue Fassung des § 100g enthält darüber hinaus eine allgemeine Befugnis, Verkehrsdaten zu erheben. In der Praxis bedeutet dies, dass die Erhebung und Speicherung der Daten nicht mehr durch die Telekommunikationsdienstleister erfolgen muss, vielmehr die Ermittler auch selbsttätig mit entsprechender Technik die Daten erheben und sofort („live") auswerten dürfen. Der Wunsch ist verständlich – es gab in der Vergangenheit Provider, die offensichtlich rechtswidrige Überwachungsanordnungen nicht umgesetzt haben. Das gleiche gilt für die „klassische" Telekommunikationsüberwachung nach den § § 100a, 100b der Strafprozessordnung. Auch hier dürfen die Ermittler die Telekommunikation künftig selbst überwachen und aufzeichnen (s. BT-Drs. 16/5846, S. 47).

Das Telekommunikationsgesetz diente einst dem Schutz der vertraulichen, durch Artikel 10 Grundgesetz geschützten Kommunikation. Mit der jetzt beschlossenen Novelle droht es, zu einem Fahndungs- und Überwachungsgesetz der Sicherheitsbehörden zu verkommen, für das die Diensteanbieter als „Hilfsbeamte" eingespannt werden.

Sven Lüders
ist Geschäftsführer der Humanistischen Union

https://www.humanistische-union.de/publikationen/mitteilungen/199/publikation/zwischen-ignoranz-und-nebelkerzen-versinkt-ein-grundrecht/
Abgerufen am: 26.11.2026