Ref. Ares(2011)181113 - 17/02/2011

Eckpunktepapier
zur
Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet

Die anlasslose umfassende Vorratsdatenspeicherung war politisch von Anfang an heftig umstritten und stieß ursprünglich auf den Widerstand aller im Deutschen Bundestag vertretenen Parteien (Beschlussempfehlung und Beschluss des Innenausschusses auf BT-Drs. 15/4597 vom 22. Dezember 2004, einstimmig vom Deutschen Bundestag angenommen am 17. Februar 2005). Die erhebliche Verunsicherung in weiten Teilen der Bevölkerung wurde durch das größte Massenklagenverfahren in der Geschichte der Bundesrepublik Deutschland mit über 30.000 Beschwerdeführern gegen das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I S. 3198) eindrucksvoll dokumentiert. Die unterschiedslose, umfassende und anlasslose Speicherung der Telekommunikationsverkehrsdaten von über 80 Millionen Bürgern sowohl bei Telefonaten als auch im Internet führte zu erheblichen Einschränkungen in grundrechtlich besonders geschützten und höchst sensiblen Lebensbereichen.

Das Bundesverfassungsgericht hat diese Regelungen zur Umsetzung der Vorratsdatenspeicherungsrichtlinie komplett aufgehoben. Auch in anderen Mitgliedstaaten haben die Verfassungsgerichte die jeweiligen nationalen Regelungen als verfassungswidrig kassiert. Derzeit ist die Richtlinie in einer größeren Anzahl von Mitgliedstaaten nicht umgesetzt und wird auch dort lebhaft und kontrovers diskutiert. Eine inhaltliche Überprüfung der Richtlinie am Maßstab der Anfang letzten Jahres - also erst nach der Richtlinie - in Kraft getretenen EU-Grundrechtecharta durch den EuGH steht weiterhin noch aus. Sie ist auf der Grundlage eines vom irischen High Court angekündigten Vorlageverfahrens aber absehbar.

Die Richtlinie besteht zwar fort. Sie ist jedoch Gegenstand einer umfassenden Evaluierung durch die EU-Kommission, die sich deutlich länger hinzieht als geplant und in deren Rahmen vor allem auch die Vereinbarkeit mit den Grundrechten der Bürger aller Mitgliedstaaten, deren sämtliche Verkehrsdaten betroffen sind, geprüft werden muss. Dabei ist bereits jetzt absehbar, dass es zu Änderungen der Richtlinie kommen wird, deren Umfang und Tragweite derzeit niemand verlässlich vorhersagen kann.

Vor diesem Hintergrund muss die Politik nach einer Lösung suchen, die die Einschränkung grundrechtlich geschützter Interessen auf das zur Sicherung der Belange von Strafverfolgung unabdingbare Maß begrenzt und gleichzeitig den wesentlichen Bedürfnissen der Strafverfolgungsbehörden angemessen Rechnung trägt. Angesichts der erheblichen Grundrechtsrelevanz muss unter strikter Anwendung des Verhältnismäßigkeitsgrundsatzes ein gezielter Ansatz gefunden werden. Nicht ausreichend erscheint es, lediglich die Speicherdauer in welchem Umfang auch immer zu verkürzen und es im Übrigen beim früheren Speicherumfang und dem anlasslosen Zugriff auf Verkehrsdaten zu belassen. Im Rahmen der gebotenen Güterabwägung müssen Schranken dort eingezogen werden, wo die Grundrechtsbeeinträchtigung schwerer wiegt als Sicherheitsbelange. Eine neue Regelung in Deutschland kann dabei auch eine Vorbildfunktion für die anstehende Diskussion auf europäischer Ebene entfalten.

Im Folgenden wird deshalb ein Lösungsansatz vorgeschlagen, der eine unterschiedslose Speicherung der Verkehrsdaten aller Bürger in Deutschland vermeidet. Im Vordergrund steht eine anlassbezogene Speicherungspflicht, bei der nur die Speicherung von Verkehrsdaten derjenigen Personen angeordnet wird, die einen hinreichenden Anlass dazu gegeben haben. Durch eine solche gezielte Maßnahme wird die Menge der zu speichernden Daten auf das notwendige Maß begrenzt. Zudem soll die Lösung sicherstellen, dass insbesondere bei der Bekämpfung der Kinderpornografie im Internet eine Ermittlung der handelnden Personen möglich ist.

Im Einzelnen:

- Die bei den TK-Unternehmen aus geschäftlichen Gründen bereits vorhandenen Verkehrsdaten werden anlassbezogen gesichert („eingefroren") und stehen den Strafverfolgungsbehörden unter Richtervorbehalt eine begrenzte Zeit zur Verfügung.

- Im Internetbereich erfolgt eine eng befristete Speicherung von Verkehrsdaten zu dem Zweck, Bestandsdatenauskünfte, d.h. eine Zuordnung dynamischer IP-Adressen zu Personen, insbesondere zur Bekämpfung von Kinderpornografie im Internet zu ermöglichen.

Dieser Vorschlag beschränkt sich auf den im Zuständigkeitsbereich des BMJ liegenden Bereich der Strafverfolgung. Ein anlassbezogenes schnelles Einfrieren vorhandener Verkehrsdaten könnte aber auch für bestimmte Fälle polizeilicher Gefahrenabwehr durch entsprechende Regelungen in den Polizeigesetzen, etwa dem BKAG, nutzbar gemacht werden.

I. Sicherung vorhandener Verkehrsdaten

Mit einer Sicherungsanordnung (sog. Quick-Freeze) wird bewirkt, dass aktuell bei einem TK-Unternehmen vorhandene (und während der Laufzeit einer Sicherungsanordnung noch anfallende) Verkehrsdaten bei Bestehen eines hinreichenden Anlasses nicht gelöscht werden und damit für ihre spätere Erhebung oder Verwendung noch zur Verfügung stehen.

Eine solche Sicherung von Daten ist im Vergleich mit dem ohnehin derzeit nach § 100g StPO möglichen Zugriff auf Verkehrsdaten nur dann vorteilhaft, wenn die Sicherung schneller und einfacher erfolgen kann als die Datenerhebung. Dies setzt tendenziell voraus, dass eine Sicherungsanordnung geringeren Anforderungen unterworfen wird, als sie für eine Erhebungsanordnung gelten.

1. Materielle Voraussetzung für die Sicherungsanordnung soll sein, dass die zu sichernden Verkehrsdaten „für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich" sind. Damit ist ein hinreichender Anlass vorgegeben, der den Umfang der zu sichernden Daten strikt begrenzt und verhindert, dass die Daten unverdächtiger Bürger für Strafverfolgungszwecke vorrätig gehalten werden.

2. Formelle Voraussetzung für eine Sicherungsanordnung ist eine Anordnung der zuständigen Polizeibehörde oder der Staatsanwaltschaft, um eine rasche Sicherung der vorhandenen Daten zu gewährleisten.

3. Bei den TK-Unternehmen werden Verkehrsdaten nach § 96 TKG zu geschäftlichen Zwecken gespeichert. Dies gilt auch, soweit sog. Flatrates vereinbart sind. Hier werden Verkehrsdaten zu Abrechnungszwecken gespeichert, die abrechnungsrelevant gegenüber anderen Diensteanbietern sind, z.B. für sog. Terminierungsentgelte bzw. Wholesale- oder Inter-Carrier-Abrechnungen. Ungeachtet von Unterschieden in der Handhabung bei einzelnen Unternehmen stehen damit Verkehrsdaten für Zeiträume bis zu sechs Monaten zur Verfügung. Die Speicherungsdauer ist dabei im Regelfall zumindest so lange, dass sie bei einer schnell wirkenden Zugriffsregelung und raschem Vorgehen der Polizeibehörden unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes ausreichend erscheint.

4. Die potentiell betroffenen TK-Diensteanbieter werden verpflichtet, auf eigene Kosten Vorkehrungen zu treffen, damit eine Sicherungsanordnung auch umgesetzt werden

kann. Für die Schnittstelle zwischen Polizeibehörden und TK-Unternehmen muss eine Verfahrensregelung gefunden werden, die eine schnelle und effektive Zusammenarbeit ermöglicht.

5. Der Zugriff auf die gesicherten Daten ist gemäß § 100g StPO nur unter Richtervorbehalt möglich.

6. Nach § 100g StPO ist eine Straftat von auch im Einzelfall erheblicher Bedeutung erforderlich, wozu insbesondere Katalogtaten nach § 100a Absatz 2 StPO gehören können. Daneben erfasst die vom BVerfG insoweit gebilligte Vorschrift auch mittels Telekommunikation begangene Straftaten, zu denen vor allem Kinderpornografie im Internet zählt.

7. Die Sicherungsanordnung soll gegenüber Anbietern von öffentlich zugänglichen Telefon- und Internetzugangsdiensten möglich sein.

8. Ihr sollen die Datenarten unterfallen, wie sie durch die EU-Richtlinie vorgegeben und seinerzeit im Rahmen der Verhandlung der EU-Richtlinie zur Vorratsdatenspeicherung von der Praxis als besonders relevant für die Strafverfolgung benannt wurden. Die TK-Unternehmen können sich dadurch auf Sicherungsmaßnahmen für diese Datenarten einrichten.

9. Die Sicherungsfrist muss so kurz wie möglich und so lang wie nötig bemessen sein.

10. Da die Voraussetzungen für eine Sicherungsanordnung im Interesse einer raschen Datensicherung niedrig angesetzt werden, bedarf es einer zusätzlichen Begrenzung der Anordnung durch eine „Negativklausel": Ist bereits bei Erlass einer Sicherungsanordnung voraussehbar, dass die Voraussetzungen für die Erhebung oder sonstige Verwendung der Daten nach § 100g StPO nicht eintreten werden, dann muss die Sicherungsanordnung unzulässig sein.

11. Die gesicherten Daten sind unverzüglich zu löschen sind, sobald die Sicherungsfrist abgelaufen ist.

12. Hinsichtlich der Sicherung der mittels Sicherungsanordnung eingefrorenen Daten gelten die allgemeinen Regelungen des Telekommunikationsrechts, wonach jeder Diensteanbieter angemessene technische Vorkehrungen oder sonstige Maßnahmen

zum Schutze des Fernmeldegeheimnisses und personenbezogener Daten sowie der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen hat, vgl. § 109 TKG.

II. Gewährleistung von Bestandsdatenauskünften im Internet

Das BVerfG hat in seinem Urteil vom 2. März 2010 zur Vorratsdatenspeicherung die Regelung zur Erhebung von Bestandsdaten grundsätzlich nicht beanstandet und vielmehr festgestellt: „*Auskünfte nach § 113 Abs. 1 TKG kann der Gesetzgeber – auch unter mittelbarer Nutzung der nach § 113a TKG gespeicherten Daten – für die Aufklärung aller Straftaten vorsehen.*" Unter Bestandsdatenauskünften versteht man die Mitteilung der TK-Unternehmen darüber, welchem Teilnehmer (unter Angabe von Name und Adresse) eine bestimmte, der Polizeibehörde bereits bekannte Internetprotokoll-Adresse zu einem bestimmten Zeitpunkt zugewiesen war. Um insbesondere zum Vorgehen gegen Kinderpornografie solche Bestandsdatenauskünfte zu ermöglichen, soll im Bereich von Internetzugangsdiensten eine eng befristete Speicherung von Verkehrsdaten vorgesehen werden, wobei die Strafverfolgungsbehörde keinen Zugriff auf die Verkehrsdaten selbst erhalten.

1. Zulässig ist danach allein die (betriebsinterne) Verwendung zur Auskunftserteilung über Bestandsdaten des Anschlussinhabers, die bereits heute nach § 113 TKG iVm §§ 161, 163 StPO zur Verfolgung von Straftaten möglich ist und vom BVerfG in seiner Entscheidung vom 2. März 2010 als zulässig zu Grunde gelegt wurde. In diesen Fällen sind den Strafverfolgungsbehörden bereits die Internetprotokoll-Adressen bekannt. Das vom BVerfG angesprochene diffus bedrohliche Gefühl des Beobachtetseins entsteht hier mangels unmittelbaren Zugriffs der Strafverfolgungsbehörden auf die Verkehrsdaten nicht. Ebenso wenig besteht aus diesem Grund die ebenfalls vom BVerfG angesprochene Ermöglichung der Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers. Ein Zugriff zur Verfolgung von Ordnungswidrigkeiten (vgl. Urteil des BVerfG vom 2. März 2010, Rz. 262) ist nicht erlaubt.

2. Die Regelung wird auf Internetzugangsdienste beschränkt.

3. Bei der näheren Ausgestaltung ist aus Verhältnismäßigkeitsgründen, insb. Vermeidung absehbarer Existenzgefährdungen, eine Marginalgrenze für

Kleinstunternehmen zu prüfen. Auch die geltende TKÜV sieht bezüglich der Verpflichtung von TK-Anlagenbetreibern zum Treffen von TKÜ-Vorkehrungen eine Marginalgrenze vor (§ 3 Abs. 2 Nr. 5 TKÜV).

4. Die Speicherungsdauer muss strikt auf das notwendige Maß beschränkt bleiben und soll sieben Tage betragen.

5. Der Umfang der Speicherungspflicht sollte auf die in der EU-Richtlinie vorgegebenen Daten für Internetzugangsdienste (vgl. §113a Abs. 4 TKG a. F.) beschränkt sein.

6. Auch wenn kein Zugriff der Strafverfolgungsbehörden auf die Verkehrsdaten selbst zulässig ist, müssen die Vorgaben des BVerfG insbesondere zur Gewährleistung der Datensicherheit beachtet werden. Das BVerfG hat einen besonders hohen Sicherheitsstandard vorgegeben, der über das allgemein verfassungsrechtlich gebotene Maß für die Aufbewahrung von Daten der Telekommunikation hinausgeht. Sicherzustellen sind demnach jedenfalls
   - die getrennte Speicherung der anlasslos zu speichernden Daten,
   - eine anspruchsvolle Verschlüsselung der Daten,
   - ein gesichertes Zugriffsregime unter Nutzung etwa des Vier-Augen-Prinzips
   - eine revisionssichere Protokollierung.

7. Erforderlich ist ergänzend eine Benachrichtigung des Anschlussinhabers nach Maßgabe der Regelungen in § 101 Absatz 4 bis 8 StPO, um den Vorgaben des BVerfG im Urteil vom 2. März 2010 Rechnung zu tragen.