quintessenz
Verein zur Wiederherstellung der Bürgerrechte im Informationszeitalter
MQ Wien / Quartier 21
Museumsplatz 1
1070 Wien

Wien, 21.Mai 2007

Bundesministerium für Verkehr,
Innovation und Technologie
Sektion III, Abteilung PT 2
Ghegastraße 1
1030 Wien

Stellungnahme zum Begutachtungsverfahren zur Novelle des TKG - Geschäftszahl BMVIT-630.333/0001-III/PT2/2007 „Vorratsdatenspeicherung“

Einleitung

Die durch die EU beschlossene Richtlinie zur Vorratsdatenspeicherung (engl. "Data Retention") entstand unter dem Eindruck der Anschläge des September 2001 und den nachfolgenden Bombenattentaten in Spanien und England.

Diese Gefahrenlage bedarf einer grundsätzlichen Neubewertung, da über Muster und Ziele der Terroristen weit mehr Informationen vorliegen, als davor. In allen betroffenen Staaten wurden von Polizei und Geheimdiensten zielgerichtete Maßnahmen ergriffen.

Die pauschale und verdachtsunabhängige Speicherung der Kommunikationsspuren aller Bürger ist hingegen kein zielgerichtetes Instrument.

Das im österreichischen Entwurf eingeführte Strafmaß erlaubt die ausufernde Verwendung dieses besonderen Instrumentariums weit über die ursprüngliche Zielsetzung hinaus.

1. Die Maßnahme ist grob unverhältnismäßig

Das Kommunikationsgeheimnis umfasst nicht nur den Inhalt, sondern auch die Verkehrsdaten: Wer mit wem, wo und wann kommuniziert hat. Die verpflichtende Speicherung reduziert nun das Kommunikationsgeheimnis allein auf den Inhalt der Kommunikation. Der Staat greift damit tief in die Privatsphäre seiner Bürger ein, und erklärt sein grundlegendes Misstrauen gegenüber seinem Souverän und dessen Recht auf freie, unkontrollierte Kommunikation.

2. Die Speicherung trifft die Falschen

Anonyme und nicht rückverfolgbare Kommunikation kann mit keiner Maßnahme vollständig unterbunden werden. Nur der Aufwand, und damit die Kosten, steigen

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

disproportional zu den Ergebnissen. Dem internationalen Terrorismus - primäres Motiv für die Einführung der Vorratsdatenspeicherung - aber auch dem organisierten Verbrechen wird es weiterhin möglich sein, das Radar der totalen Kommunikationsprotokollierung zu unterfliegen. Schnelle Wechsel von einem Kommunikationsmedium zum anderen, die Aufteilung von Kommunikationsvorgängen auf mehrere Kanäle läßt Vorratsdatenspeicherung ins Leere laufen. Im Netz der Vorratsdatenspeicherung werden nur Gelgenheits- und Kleinkriminelle, unbedarfte Amateure und der ganz normale Bürger hängen bleiben.

3. Die Novelle setzt Vorgaben der EU um Jahre vorauseilend um

Die in §92 Abs 4a einbezogene Protokollierung von Internet e-Mail und Internet-Telefonie wird für die Umsetzung bis September 2007 von der EU gar nicht verlangt. Die Umsetzungsfrist zur Speicherung der Internet-Daten endet erst im März 2009. Sie ist in dieser Novelle daher ersatzlos zu streichen.

4. Die Maßnahme verlangt die Speicherung von Daten, die vielen Providern nicht bekannt sind

Manche Daten (zb Erfolglose Anrufe) wurden bisher gar nicht gespeichert, andere (Standort-Daten) wurden routinemäßig bei manchen Mobilfunkbetreibern nicht zentral gesammelt. Andere Daten wiederum (Bonität, etc) sind einigen Providern gar nicht bekannt. Das Vorblatt zur Novelle schränkt zwar ein, dass die „Speicherverpflichtung ausschließlich Daten betrifft, die bereits derzeit für Verrechnungszwecke gespeichert werden“, die Novelle des TKG trifft aber keine dementsprechenden Vorkehrungen für den Fall, dass der Netzbetreiber diese Daten bisher nicht gespeichert oder verarbeitet haben, oder gar nicht im Besitz der geforderten Informationen sind.

5. Die Novelle enthält keinen adäquaten Schutz der extra für die Vorratsdatenspeicherung zusammengetragenen Daten.

Im Zuge der Implementierung dieser Novelle werden die Netzbetreiber Daten aus Ihren Netzen speichern müssen, die sie bisher nicht erhoben haben. Das Gesetz stellt nicht sicher, dass diese Daten keiner Drittnutzung zugeführt werden. Die Verkehrsdatensätze, da sie nun einmal gesammelt im System vorhanden sind, können ebenso gut zu Marketingzwecken benutzt werden: Kunde reist viel, telefoniert auf Großveranstaltungen, hält sich regelmäßig in Funkzellen auf, die einen Golfplatz mitversorgen. Diese Verkehrsdaten sind, wie die Überwachungsskandale in Griechenland (2004/5) und Italien gezeigt haben, ein prioritäres Angriffsziel aus- und inländischer Geheimdienste. In beiden Fällen bezahlten der Netzwerksicherheitschef von Vodafone Hellas sowie jener der Telecom Italia mit ihrem Leben. In Italien wurden ein Dutzend Telekom-Techniker verhaftet und ebnsoviel ranghohe Polizisten sowie der stellvertretende Chef des Militärgeheimdienstes SISMI. Die Verkehrsdatensätze der italienischen Bürger/innen wurden über eine private Agentur auf dem freien Markt verkauft.

6. Die Novelle enthält keine Sicherung gegen Umgehung von Redaktionsgeheimnissen oder besonders schützenswerten Berufsgruppen.

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

Rechtsanwälte, Notare, Ärzte, Seelsorge, Drogenberatungen, Krankheitsberatungen (zb AIDS), Journalisten, Kirchen, Flüchtlingseinrichtungen, Abgeordnete, Militär, aber auch Nachrichtendiensten und Sicherheitsbehörden werden besondere schützenswerte Interessen zugestanden, oder sie leben von dem besonderen Vertrauensverhältnis zu den Menschen. All diesen Berufsgruppen wird die Basis der Vertraulichkeit entzogen. Potenzielle Informanten werden Skandale nicht mehr so einfach auffliegen lassen, wenn sie sicher sein können, dass jeder ihrer Telefonkontakte mit Journalisten von Dritten protokolliert wird. Beratungssuchende etwa mit psychischen Problemen, die sie z.B. dem Arbeitgeber gegenüber geheim halten wollen.

7. Die Verkehrsdaten verleiten per se zu falschen Schlüssen und Beschuldigungen.

Verkehrsdaten von Telefonanschlüssen, Mobilfunkverträgen oder Internetprovidern lassen so gut wie nie einen eindeutigen Schluss auf den tatsächlich Kommunizierenden zu. Die Stammdatensätze weisen nur den Inhaber des Anschlusses aus.

8. Die Novelle setzt ein viel zu niedriges Strafmaß als Zugriffsbeschränkung auf die auf Vorrat gespeicherten Daten. §102a Abs. 1:

Das Strafmaß schießt weit über die des internationalen Terrorismus und der organisierten Kriminalität hinaus. Das Strafmaß muss deutlich angehoben werden, und die Verwendung der Daten für einen genau definierten Bereich (am besten taxaktiv) eingeschränkt werden.

9. Die Novelle enthält keine Evaluierung der Erfolgs und des Verhältnisses der Eingriffe

Das Recht des Bundesministers oder der Europäischen Kommission auf die Kontrolle der Protokolle (§102b) beinhaltet keine Evaluierungsverpflichtung. Der Erfolg der Maßnahme sollte mit gleichen oder strengeren Maßstäben wie die der besonderen Ermittlungsmethoden (Lauschangriff und Rasterfahndung) erfolgen, und zusammen mit diesen auf nationaler Ebene veröffentlicht werden.

10. Die Novelle enthält keine Sicherungen gegen Netzwerkanalysen und Rasterfahndung in den Kommunikationsdaten

Der Entwurf lässt völlig offen, wie und in welcher Form auf die Daten aus der Vorratsdatenspeicherung zugegriffen werden darf. Dies ermöglicht komplexe Netzwerkanalysen von Kommunikationsverhalten bestimmter Gruppen – s.g. „rekursive Abfragen“ ohne explizite Tiefenbeschränkung: jede Person die mit jeder Person die mit (...) einer ganz bestimmten Person kommuniziert hat.
Zugriffe könnten auch aufgrund von Orts- und Zeitangaben, dem Wohnort oder Gerätehersteller/Marke (Herstellerkennung in der IMEI) erfolgen.
Durch relativ simple Abfragen lassen sich auch besonders Schützenswerte Daten wie die politische Ausrichtung, die Religionszugehörigkeit, Gesundheitsinformationen etc mit relativ geringer Fehlerrate ermitteln, ohne den Inhalt der Nachricht analysiert zu müssen.

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

11. Gespeicherte Daten wecken neue Begierlichkeiten

Datensammlungen sind ein magischer Magnet für neue Begierlichkeiten aus allen möglichen Richtungen. Sind Daten einmal vorhanden und gespeichert fällt die Argumentatin warum diese für einen ganz besonderen Zweck benutzt werden dürfen, aber für einen vermeintlich genauso legitimen anderen Zweck nicht verwendet werden dürfen, schwer.
Interessensverbände, Opfer aber auch die Medien werden Ihres Beitragen, die Grenze bei besonders aufsehnerregenden Fällen oder durch besonders hartnäckiges Intervenieren weiter hinabzusetzen. Ein einfaches Verbot der Verwendung ist unzureichend – am Besten lässt man die Datensammlungen erst gar nicht entstehen.

12. Den Providern wird kein Ersatz für Ihren Aufwand geleistet

Eine Vergebührung der Zugriffe (zb nach Datensatz, Suchtiefe und Dauer der Speicherung) scheint nicht nur fair, sie schützt auch jeden einzelnen Bürger auch vor allzu großen und unverhältnismäßigen Eingriffen in sein Kommunikationsgeheimnis.

13. Die Maßnahme ändert grundsätzlich das Verständnis zwischen Staat und seinen Bürgern

Der Staat dokumentiert damit das grundsätzliche Misstrauen gegenüber allen seinen Bürgern. Freie Kommunikation ist nur noch erlaubt, wenn die Sicherheitsbehörden auch nachträglich darüber verfügen dürfen. Es erhebt den staatlichen Anspruch, große Teile des privaten und beruflichen Lebens jedes Einzelnen im Vorhinein zu protokollieren und im Nachhinein kontrollieren zu können. Mit dem Effekt, das die Unschuldsvermutung ad absurdum geführt wird.

14. Selbst die lückenloseste Kommunikationsprotokollierung konnte noch in keinem Staat der Welt Kriminalität gänzlich verhindern

Historische Beispiele aus der zweiten Hälfte des 20. Jahrhundert in Europa, oder aktuelle Beispiele aus anderen Teilen der Welt zeigen, dass selbst die strengste staatliche Kontrolle von Kommunikationsmitteln und deren Verwendung weder Kriminalität noch gewaltsame Anschläge verhindern konnten.

Mit freundlichen Grüßen

Adrian Dabrowski,
Obmann

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.