An die
Parlamentsdirektion
Begutachtungsverfahren

1010 Wien

Wien, 12. Februar 2012

Betreff: Zeichen: GZ S91000/5-ELeg/2012
Stellungnahme der ARGE DATEN zum
Entwurf eines Bundesgesetzes, mit dem das Wehrgesetz 2001, das Heeresdisziplinargesetz 2002, das Heeresgebührengesetz 2001, das Auslandseinsatzgesetz 2001, das Militärbefugnisgesetz, das Sperrgebietsgesetz 2002, das Munitionslagergesetz 2003, das Militärauszeichnungsgesetz 2002, das Betriebliche Mitarbeiter- und Selbständigenvorsorgegesetz sowie das Truppenaufenthaltsgesetz geändert werden.

In der Anlage finden Sie die Stellungnahme der
ARGE DATEN – Österreichische Gesellschaft für Datenschutz
mit dem dringenden Ersuchen um Kenntnisnahme und Berücksichtigung.

Für allfällige Fragen stehen wir gerne zur Verfügung.

Mit vorzüglicher Hochachtung

elektronisch erstellt
Dr. Hans G. Zeger (Obmann)

Anlage:
Stellungnahme elektronisch übermittelt (begutachtungsverfahren@parlinkom.gv.at)

Alle Stellungnahmen werden unter ftp://ftp.freenet.at/privacy/gesetze veröffentlicht.

Stellungnahme der ARGE DATEN zum Entwurf Verwaltungsgerichtsbarkeits-Begleitgesetz-Wehrrecht

Entwurf eines Bundesgesetzes, mit dem das Wehrgesetz 2001, das Heeresdisziplinargesetz 2002, das Heeresgebührengesetz 2001, das Auslandseinsatzgesetz 2001, das Militärbefugnisgesetz, das Sperrgebietsgesetz 2002, das Munitionslagergesetz 2003, das Militärauszeichnungsgesetz 2002, das Betriebliche Mitarbeiter- und Selbständigenvorsorgegesetz sowie das Truppenaufenthaltsgesetz geändert werden.

1. EINLEITUNG

Ziel des vorliegenden Entwurfs ist die Anpassung sämtlicher wehrrechtlicher Verfahrensbestimmungen an die ab 1. Jänner 2014 in Kraft tretende Verwaltungsgerichtsbarkeits-Novelle 2012. Gleichzeitig sollen im Rahmen der notwendigen Anpassungen legistische Verbesserungen vorgenommen werden.

1.1 Verwendung von Vorratsdaten

Eine der geplanten Änderungen ist die Ausweitung der Befugnisse des militärischen Nachrichtendienstes. Dieser soll zukünftig nicht nur von einem weit umfangreicheren Personenkreis als bisher Auskünfte über die Identität eines Telefonanschlussinhabers verlangen dürfen, sondern auch Identitätsangaben über Inhaber einer IP-Adresse fordern können.

Zur Feststellung, welcher Person eine IP-Adresse in der Vergangenheit zugeordnet war, sollen Internetprovider verpflichtet werden Vorratsdaten auszuwerten.

Wie die ARGE DATEN in ihrer Stellungnahme zur - Änderung des Telekommunikationsgesetzes 2003 (TKG 2003) mit der die EU-Richtlinie 2006/24/EG über die Vorratsdatenspeicherung umgesetzt wurde[1] - ausführlich dargelegt hat, steht die verdachtslose Speicherung von Kommunikationsdaten in keiner Relation zu dem Angestrebten Zweck - der Terrorbekämpfung - ist somit grob unverhältnismäßig und damit grundrechtswidrig.

Der geplante, intransparente Zugriff auf Vorratsdaten durch den militärischen Nachrichtendienst, geht weit über den derzeitigen gesetzlichen Rahmen hinaus und würde einen Grundrechtseingriff in ungeahntem Ausmaß darstellen.

Um dem Nachrichtendienst die Erfüllung seiner Aufgaben zu ermöglichen, sollen Internetprovider beliebig und ohne Protokollierung auf Daten zuzugreifen, die ausschließlich zur Verbrechenbekämpfung gespeichert werden. Die geplante Änderung ist dabei nicht nur aufgrund der Unvereinbarkeit mit dem Grundrecht auf Privatsphäre abzulehnen, sondern aufgrund der geltenden gesetzlichen Bestimmungen unzulässig.

[1] Stellungnahme der ARGE DATEN zur Umsetzung der Vorratsdatenspeicherung – abrufbar online unter: http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00117_03/imfname_177168.pdf

Wie die geplante Gesetzesänderung überdeutlich zeigt, wecken vorhandene Daten Begehrlichkeiten verschiedenster Natur. Die einzige Möglichkeit diese Begehrlichkeiten zu verhindern ist, Daten nicht zu sammeln. Aus diesem Grund sei erneut auf Alternativen zur Vorratsdatenspeicherung hingewiesen die weniger intensiv in die Grundrechte der Betroffenen eingreifen. Als ein Beispiel sei das sogenannte *quick freeze*- Verfahren genannt, bei dem Kommunikationsdaten nur im Verdachtsfall und nur von den Verdächtigen gespeichert werden.

Der geplante Zugriff des militärischen Nachrichtendienstes auf Vorratsdaten ist gesetzes- und grundrechtswidrig und daher klar abzulehnen.

1.2 Videoüberwachung im Wachdienst

Geplant ist, dass der Wachdienst zukünftig zum militärischen Eigenschutz Videoüberwachung einsetzen kann. Zum militärischen Eigenschutz gehört ebenfalls der Schutz vor Verwaltungsübertretungen.

Das Datenschutzgesetz 2000 (DSG 2000) nennt ausschließlich den Schutz überwachter Objekte bzw. Personen sowie die Erfüllung rechtlicher Sorgfaltspflichten als rechtmäßige Zwecke von Videoüberwachung. Videoüberwachung zum Schutz vor Verwaltungsübertretungen würde eine nicht ausreichend begründbare, willkürliche Ausdehnung der im DSG 2000 geregelten Zwecke darstellen.

Aufgrund der Bestimmungen des Datenschutzgesetzes 2000 ist eine Sonderregelung, für Videoüberwachung im Wachdienst, nicht notwendig sondern würde eine willkürliche Zweckerweiterung darstellen. Von der geplanten Änderung ist daher abzusehen.

2. VERWALTUNGSGERICHTSBARKEITS-BEGLEITGESETZ-WEHRRECHT. IM DETAIL

2.1 § 55a WG 2001 – Schutz sensibler Daten

Die geplante Änderung des § 55a Wehrgesetz 2001 (WG 2001), dass Untersuchungsdaten zur Eignung zum Wehrdienst ausschließlich aufgrund von Gesetzen, die ein wichtiges öffentliches Interesse wahren, weitergegeben werden dürfen, ist zu begrüßen.

2.2 § 15 Abs 2 MBG – Videoüberwachung

Gemäß dieser Bestimmung soll die Ermittlung von personenbezogenen Daten per Bildübertragungs- und Bildaufzeichnungsgeräten (Videoüberwachung) im Wachdienst zulässig sein, sofern dies für Zwecke des militärischen Eigenschutzes erforderlich ist.

In § 2 Militärbefugnisgesetz (MBG) werden die Aufgaben des Wachdienstes, im Rahmen des militärischen Eigenschutzes, als Schutz vor drohenden und zur Abwehr von gegenwärtigen Angriffen gegen militärische Rechtsgüter oder zum Schutz oder zur Abwehr betreffend vergleichbare Tatbestände von Verwaltungsübertretungen, die gegen militärische Rechtsgüter gerichtet sind, festgehalten. Zu diesem Zweck soll der Wachdienst zukünftig auch Videoüberwachung einsetzen dürfen.

Videoüberwachung greift besonders stark in die Rechte der Überwachten ein, da diese für einen permanenten Überwachungsdruck sorgt. Gleichzeitig werden von Videoüberwachungen vornehmlich Daten von Personen erfasst, die nicht dem Zweck der Videoüberwachung entsprechen.

Das DSG 2000 nennt in § 50a Abs 2 DSG 2000 zulässige Zwecke von Videoüberwachung. Dies sind der Schutz eines überwachten Objekts bzw. einer überwachten Person oder die Erfüllung rechtlicher Sorgfaltspflichten. Gesetzliche Bestimmungen können weitere zulässige Zwecke für Videoüberwachung vorsehen.

Durch den geplanten § 15 Abs 2 MBG wäre es dem Wachdienst zukünftig möglich Videoüberwachungen einzusetzen, um Verwaltungsübertretungen abzuwehren bzw. zu verhindern.

> **Die Verhinderung von Verwaltungsübertretungen steht in keinem Verhältnis zu dem tiefen Eingriff in die Persönlichkeitsrechte die Videoüberwachung verursacht. Aus diesem Grund ist von der geplanten Änderung abzusehen.**

Der Schutz von Objekten bzw. Personen, sowie die Erfüllung rechtlicher Sorgfaltspflichten werden ohnehin in § 50a Abs 2 DSG 2000 als zulässige Zwecke von Videoüberwachung genannt. Aus diesem Grund ist eine Sonderbestimmung zum Einsatz von Videoüberwachung für den Wachdienst im MBG nicht notwendig, da diese bereits aufgrund der allgemeinen gesetzlichen Regelungen des DSG 2000 zulässig ist.

2.3 § 22 Abs 2a MBG – Vorratsdaten

Zur nachrichtendienstlichen Aufklärung, der Beschaffung, Bearbeitung, Auswertung und Darstellung von Informationen über das Ausland oder über internationale Organisationen oder sonstige zwischenstaatliche Einrichtungen betreffend militärische und damit im Zusammenhang stehende sonstige Tatsachen, Vorgänge und Vorhaben (§ 20 Abs 1 MBG) oder zur nachrichtendienstlichen Abwehr, dem militärischen Eigenschutz durch die Beschaffung, Bearbeitung, Auswertung und Darstellung von Informationen über Bestrebungen und Tätigkeiten, die vorsätzliche Angriffe gegen militärische Rechtsgüter zur Beeinträchtigung der militärischen Sicherheit erwarten lassen (§ 20 Abs 2 MBG), sollen militärische Organe zukünftig auch Auskünfte aus Vorratsdaten verlangen können.

Im Detail sollen militärische Organe von Betreibern öffentlicher Telekommunikationsdienste und sonstigen Diensteanbietern, neben Auskünften über die Identität eines Telefonanschlussinhabers, ebenfalls Informationen über den Inhaber einer IP-Adresse einholen können. Sofern dies notwendig ist, soll dabei auch die Verwendung von Vorratsdaten zulässig sein.

Vorratsdaten iSd. TKG 2003 dürfen ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a Strafprozeßordnung 1975 (StPO) rechtfertigt, gespeichert werden – nicht aber zur nachrichtendienstlichen Aufklärung oder zur nachrichtendienstlichen Abwehr.

> **Vorratsdaten dürfen nicht für Zwecke der nachrichtendienstlichen Aufklärung oder zur nachrichtendienstlichen Abwehr gespeichert werden. Die Verwendung von Vorratsdaten für diese Zwecke ist somit unzulässig.**

Die Fälle, in denen Sicherheitsbehörden auf Vorratsdaten zugreifen dürfen, sind gesetzlich klar und abschließend geregelt. Militärische Organe hingegen sollen allgemein, zur Erfüllung der nachrichtendienstlichen Aufklärung oder Abwehr, Vorratsdaten verwenden dürfen. Dies stellt einen Freibrief zur schrankenlosen Verwendung von Vorratsdaten durch militärische Organe dar.

Gleichzeitig wäre aufgrund der geltenden gesetzlichen Bestimmungen unklar wie Auskünfte, denen die Verwendung von Vorratsdaten zugrundeliegt, an militärische Organe übermittelt werden müssen. § 94 Abs 4 TKG 2003 regelt schließlich ausschließlich die Übermittlung von Vorratsdaten aufgrund der Bestimmungen der StPO bzw. des SPG.

Die Übermittlung von Vorratsdaten an militärische Organe könnte somit ohne Verwendung der Durchlaufstelle (§ 8 Datensicherheitsverordnung TKG-DSVO) und somit ohne jegliche Transparenz erfolgen.

Die in § 22 Abs 2a Z 3 MBG vorgesehene Verwendung von Vorratsdaten ist daher ersatzlos zu streichen.

2.4 § 22 Abs 2a MBG – Sonstige Diensteanbieter

Weiters ist in § 22 Abs 2a MBG geplant, die Auskunftspflicht über einen Telefonanschluss- bzw. IP-Adresseninhabers auch auf sonstige Diensteanbieter auszudehnen.

Obwohl weder im MBG noch in den Erläuterungen konkretisiert, ist davon auszugehen, dass es sich dabei um Diensteanbieter iSd. § 3 Z 2 E-Commerce-Gesetz (ECG) handelt. Dies sind natürliche oder juristische Personen oder sonstige rechtsfähige Einrichtungen, die einen Dienst der Informationsgesellschaft, ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst, anbieten.

Hierbei ist darauf hinzuweisen, dass Diensteanbieter, die von Nutzern eingegebene Informationen speichern (Hosting-Anbieter), bereits aufgrund des § 18 Abs 3 ECG verpflichtet sind, Behörden, Name und Adresse von Nutzern bekannt zu geben, sofern dies eine wesentliche Voraussetzung zur Wahrnehmung ihrer Aufgaben darstellt. Bezüglich dieser Diensteanbieter wäre die geplante Gesetzesänderung bei Auftreten militärischer Organe als Behörde überflüssig.

Neben Hosting-Anbietern, nennt das ECG den Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangebote, die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern als Dienste der Informationsgesellschaft. Eine Ausweitung der Auskunftspflicht auf diese Diensteanbieter wäre überschießend und würde nicht mit den Bestimmungen des TKG 2003 in Einklang stehen.

Gleichzeitig sei darauf hingewiesen, dass die überwiegende Mehrzahl von sonstigen Diensteanbietern (z.B. Anbieter von Suchmaschinen, Link-Anbieter, Anbieter die Informationen zwischenspeichern (Caching), Anbieter die Informationen durchleiten) nicht über die in § 22 Abs 2a MBG aufgezählten Informationen über ihre Nutzer verfügen und somit nicht in der Lage wären Auskunftsbegehren nachzukommen.

Von der in § 22a MBG vorgesehenen Ausweitung der Auskunftspflicht auf sonstige Diensteanbieter ist daher abzusehen.