

Nachdem § 53 Abs. 4 GOG
an die Abgeordneten verteilt

ENTSCHLIESSUNGSANTRAG

der Abgeordneten Peter Pilz, Albert Steinhauser, Freundinnen und Freunde

betreffend Umfassender Stopp dem Überwachungsstaat

eingebraucht im Zuge der Debatte über den Dringlichen Antrag „Stopp dem Überwachungsstaat: Gläserner Staat statt gläserne Bürgerinnen und Bürger“ (1193/A(E))

BEGRÜNDUNG

Im heutigen Dringlichen Antrag von Team Stronach und Neos verbergen sich gefährliche Hintertüren:

Team Stronach und Neos fordern: "Keine Einführung einer systematischen, anlasslosen, personenbezogenen Datenspeicherung ohne parlamentarische Kontrolle".

Die Vorratsdatenspeicherung ist eine dieser „systematischen, anlasslosen, personenbezogenen Datenspeicherungen“. Auch mit parlamentarischer Kontrolle wäre eine solche Vorgehensweise aber klar verfassungswidrig, wie sich unter anderem aus den entsprechenden Entscheidungen des Verfassungsgerichtshofes und des Europäischen Gerichtshofes ergibt.

Team Stronach und Neos fordern: "Keine überbordende Ermächtigung zur Sammlung von Fingerabdrücken und IP-Adressen im Finanzstrafgesetz".

Jede – auch eine nicht „überbordende“ - Ermächtigung zur Sammlung von Fingerabdrücken und IP-Adressen im Finanzstrafverfahren ist für uns inakzeptabel.

Darüber hinaus fehlen trotz des Titels „Stopp dem Überwachungsstaat“ viele der wichtigsten Forderungen zum Schutz der Bürgerinnen und Bürger.

Die unterfertigenden Abgeordneten stellen daher folgenden

ENTSCHLIESSUNGSANTRAG

Der Nationalrat wolle beschließen:

„Die Bundesregierung wird aufgefordert, gegen die ständig zunehmende nationale und internationale Aushöhlung der Privatsphäre von Bürgerinnen und Bürgern

einzuschreiten, und zu diesem Zweck insbesondere zu den im folgenden beschriebenen Problemlagen die kursiv geschriebenen Maßnahmen zu ergreifen:

AUFKLÄRUNG VON ÜBERWACHUNGS-ANGRIFFEN AUF ÖSTERREICH

1. Die Behörden in Belgien, den Niederlanden und der Schweiz ermitteln in der NSA-Affäre bereits auf Hochtouren. Bis heute haben StA Wien und BVT keine vergleichbaren Ermittlungsschritte gesetzt. ***Daher: sofortige Untersuchung der Transitleitungen der Telekom Austria AG, die zwischen 2005 und 2008 von BND und NSA angegriffen worden sind; Feststellung, ob diese Leitungen von Regierung, internationalen Organisationen und Unternehmen genützt worden sind.***
2. Die Telekom Austria AG hat bis heute nichts zur Aufklärung beigetragen und öffentlich nichts zum Schutz ihrer Kundinnen und Kunden beigetragen. ***Daher: Auftrag des Eigentümers an die Telekom Austria, die NSA-Angriffe aufzuklären, rechtliche Schritte gegen BND und Deutsche Telekom AG einzuleiten und wirkungsvolle Maßnahmen zum Schutz der Kundinnen und Kunden zu setzen.***
3. UNO und OSZE werden durch den in Wien stationierten Special Collection Service von NSA und CIA und durch die Abschöpfung von Leitungen durch die NSA überwacht. Daher: ***Schutzprogramm gegen die Ausspähung internationaler Organisationen in Wien.***

SCHUTZ VOR ÜBERWACHUNGSSTAAT IN ÖSTERREICH

4. Die Vorratsdatenspeicherung ist eine systematische, anlasslose, personenbezogene Datenspeicherung. Daten von allen NutzerInnen moderner Kommunikationsmittel werden gespeichert, ohne dass sie sich etwas zu Schulden kommen lassen haben. Die vermeintlichen Adressaten der Vorratsdatenspeicherung, „die Kriminellen“, werden sich hingegen schützen. Was bleibt ist die Missbrauchsgefahr für die BürgerInnen. ***Daher: Keine Wiedereinführung der Vorratsdatenspeicherung.***
5. Seit Jahren werden Stück für Stück BürgerInnenrechte beschnitten und neue Überwachungsformen gesetzlich verankert. Eine umfassende Evaluierung der Überwachungsgesetze auf Notwendigkeit, Verhältnismäßigkeit und das Funktionieren des Rechtsschutzes ist überfällig. ***Daher: Evaluierung sämtlicher Überwachungsgesetze.***
6. Das BMI hat einen Entwurf für ein Staatsschutzgesetz, das dem BVT eine Generalvollmacht zur Überwachung und zur Übermittlung der Daten an ausländische Geheimdienste ausstellt, vorgelegt. Damit soll Österreich Überwachungs-Spitzenreiter in der EU werden. ***Daher: Zurücknahme des Entwurfs für ein Staatsschutzgesetz und neue Erarbeitung im Rahmen parlamentarischer Verhandlungen.***
7. Im BVT sind derzeit die Kompetenzen des Nachrichtendienstes, der Kriminalpolizei für politische Delikte und der Spionageabwehr unter einem Dach vereint. Die Erfahrung zeigt, dass hier Unvereinbarkeiten das BVT am

Schutz österreichischer Personen und Unternehmen hindern. **Daher: Trennung von Nachrichtendienst und Kriminalpolizei; Schaffung einer eigenen, von CIA, GCHQ, MI5 und BND völlig unabhängigen Spionageabwehr.**

8. Nach wie vor missbrauchen ausländische Geheimdienste den diplomatischen Schutz ihrer spionierenden Mitarbeiter in Österreich. Für die gesetzwidrigen Tätigkeiten von NSA und CIA liegen Beweise vor. **Daher: Prüfung der Ausweisung des CIA-Residenten an der US-Botschaft und Überprüfung der Tätigkeiten russischer, chinesischer, britischer und anderer fremder Dienste in Österreich.**
9. SPÖ und ÖVP planen die Öffnung von Konten ohne richterlichen Befehl. **Daher: keine Kontenöffnung ohne richterlichen Beschluss.**
10. Da Datenströme grenzübergreifend fließen, sind verbindliche Datenschutzregelungen in der gesamten Europäischen Union notwendig, um einen höheren Schutz und die Durchsetzung der Rechte sicherstellen. Das Recht auf Privatsphäre und insbesondere auf den Schutz personenbezogener Daten zählen für uns zu den Grundrechten aller in der EU lebenden BürgerInnen. Das Recht auf Vergessen, explizite Zustimmungspflicht zur Datenspeicherung auch im Internet, Privacy by default oder Privacy by design müssen als Schutzstandards verankert werden. **Daher: Österreichische Initiative für eine starke neue EU-Datenschutzverordnung und neue Regeln für Daten im Internet.**
11. USA, Russland und andere respektieren unseren Datenschutz nicht. Das muss Konsequenzen haben. Bankdatenabkommen, Passagierdatenabkommen, Safe Harbour-Abkommen (über die erleichterte Datenübermittlung in die USA), Polizeidatenabkommen usw. müssen neu mit strengen Datenschutzstandards verhandelt werden. **Daher: Reform der Datenüberlassung an Drittstaaten und Kündigung von Abkommen wie Safe Harbour bei Verweigerung der Reform durch Partner wie die USA.**
12. Das beste Mittel gegen Korruption und Überwachungsstaat ist Transparenz. Informationen, die in öffentlichen Stellen vorhanden sind, gehören der Allgemeinheit, nicht der Behörde. Sie sollten deshalb auch öffentlich zugänglich sein. **Daher: Abschaffung des Amtsgeheimnisses und Informationsfreiheitsgesetz für umfassendes Recht der Bürgerinnen und Bürger auf Information.**

PARLAMETARISCHE KONTROLLE

13. Die parlamentarische Kontrolle funktioniert mangels klarer und durchsetzbarer Kompetenzen nicht. **Daher: Kontrolle der Nachrichtendienste nach dem Prinzip „kein Geheimnis vor dem Parlament“.**

