Bayerischer Landtag

18. Wahlperiode 04.07.2019 **Drucksache 18/2881**

Dringlichkeitsantrag

der Abgeordneten **Florian Streibl, Dr. Fabian Mehring, Wolfgang Hauber, Gerald Pittner, Manfred Eibl, Prof. (Univ. Lima) Dr. Peter Bauer, Susann Enders, Dr. Hubert Faltermeier, Hans Friedl, Tobias Gotthardt, Eva Gottstein, Joachim Hanisch, Johann Häusler, Dr. Leopold Herz, Alexander Hold, Nikolaus Kraus, Rainer Ludwig, Bernhard Pohl, Kerstin Radler, Gabi Schmidt, Jutta Widmann, Benno Zierer** und **Fraktion (FREIE WÄHLER)**,

Thomas Kreuzer, Prof. Dr. Winfried Bausback, Alexander König, Tobias Reiß, Tanja Schorer-Dremel, Petra Guttenberger, Manfred Ländner, Holger Dremel, Norbert Dünkel, Matthias Enghuber, Max Gibis, Alfred Grob, Otto Lederer, Dr. Franz Rieger, Josef Schmid, Karl Straub, Walter Taubeneder, Peter Tomaschko und **Fraktion (CSU)**

Standortfaktor „Sichere digitale Kommunikation“: Schutz von Geschäftsgeheimnissen und Kundendaten stärken

Der Landtag wolle beschließen:

Der Landtag begrüßt, dass die Bundesregierung am Prinzip “Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung” festhalten möchte.

Unternehmen, Verbraucher und Verwaltung müssen sich bei digitalen Produkten und Dienstleistungen darauf verlassen können, dass ihre Daten technisch so gut wie möglich geschützt und die genutzten Systeme vertrauenswürdig sind.

Gerade für Unternehmen spielt es heute eine zentrale Rolle bei der Wahl ihres Standortes, dass Geschäftsgeheimnisse und Kundendaten nicht nur regulatorisch, sondern auch technisch hochgradig geschützt sind.

Die Staatsregierung wird daher aufgefordert, sich auf Bundesebene dafür einzusetzen, dass

– die technischen Möglichkeiten der IT-Sicherheit für Bürger, Unternehmen und Behörden in Deutschland ausgeschöpft und zugleich die unabweisbaren Bedürfnisse der Sicherheitsbehörden berücksichtigt werden,

– das internationale Ansehen Deutschlands als führender Standort für eine sichere und datenschutzorientierte Digitalwirtschaft weiter gefördert wird und

– Unternehmen und Verbrauchern weiterhin für die Gefahren durch digitale Sabotage, Wirtschaftsspionage und Datendiebstahl sensibilisiert werden.

Der Landtag stellt zugleich fest, dass das Prinzip “Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung” das Problem beschreibt, dass es heutzutage unbestreitbar einen Bedarf an breit verfügbaren digitalen Verschlüsselungstechnologien gibt, die aber zu keiner unverhältnismäßigen Beeinträchtigung der Handlungsfähigkeit des Staates führen dürfen. Ermittlungsbehörden und Nachrichtendienste müssen entsprechend ausgestattet werden, um dem kriminellen Missbrauch von Verschlüsselungstechnologien entgegentreten zu können.

Begründung:

Presseberichte von Ende Mai haben suggeriert, auf Bundesebene würde geplant werden, verschlüsselte Kommunikation von Messenger-Diensten überwachbar zu machen. Mitte Juni hat ein Sprecher des Bundesministeriums des Innern, für Bau und Heimat gegenüber der dpa jedoch klargestellt, dass die Bundesregierung am Prinzip „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ fest halte und keine Hintertüren oder Verschlüsselungsverbote einführen wolle.

Das Prinzip von „Sicherheit durch und trotz Verschlüsselung“ greift das Problem auf, dass der unbestreitbare Bedarf an Verschlüsselung im Zeitalter von Cyber-Kriminalität zu keiner unverhältnismäßigen Beeinträchtigung der Handlungsfähigkeit des Staates führen darf.

Laut Branchenverband Bitkom sind in den Jahren 2016/2017 durch digitale Sabotage, Wirtschaftsspionage und Datendiebstahl alleine im Industriesektor Schäden in Höhe von mindestens 43 Mrd. Euro entstanden. Als innovationsfreundlicher und wettbewerbsfähiger Wirtschaftsstandort benötigt Deutschland die besten Schutzmöglichkeiten. Verschlüsselungstechnologien spielen hierbei eine zentrale Rolle.

Deutschland und vor allem auch Bayern sind zudem Standort für IT-Sicherheitsunternehmen u. a. mit Fokus auf Verschlüsselungstechnologien. Ein Verbot der Ende-zu-Ende-Verschlüsselung würde diese Unternehmen im internationalen Wettbewerb massiv benachteiligen. Dabei ist zu berücksichtigen, dass eine Schwachstelle von Kriminellen, aber auch von Mitarbeitern der Betreiber ausgenutzt werden könnte, um an sensible Informationen von Bürgerinnen und Bürgern, Firmen und Behörden zu gelangen.

Aus der technischen Perspektive ist Folgendes festzustellen:

Erstens es wäre schwierig, eine geheime Hintertüre in quelloffene Messenger, wie beispielsweise Signal, einzubauen, da der Programmcode öffentlich ist.

Zweitens, würde man einzelne Messenger sperren wollen, müsste man eine umfangreiche IT-Infrastruktur aufbauen. Der Aufwand wäre sehr hoch, weil vor allem Kriminelle zu den Ersten gehören würden, die mittels Virtueller Privater Netzwerke (VPN) oder dem sogenannten TOR-Netzwerk diese Sperren umgehen.

Die Verschlüsselung birgt allerdings auch erhebliche Missbrauchsrisiken durch Kriminelle (z.B. im Bereich des Terrorismus, des illegalen Waffenhandels und der Kinderpornographie). So hat eine Untersuchung des Bundeskriminalamts (BKA) bereits für den Zeitraum der Jahre 2012 bis 2013 in 72 Prozent der Verfahren den Einsatz von Verschlüsselungsdiensten aufgezeigt (vgl. die Antwort der Bundesregierung auf eine Kleine Anfrage von Abgeordneten und der Fraktion BÜNDNIS 90/Die Grünen, BT-Drs. 19/1434, S. 14 – Frage 38).

Auf der anderen Seite liefern die neuen digitalen Entwicklungen in der Kommunikationstechnologie mehr Daten, als jemals früher zur Verfügung standen. Zahlreiche aktuelle Fälle dokumentieren, dass auch im sogenannten Darknet – das technisch als extrem abhörsicher gilt – mit klassischen Ermittlungsmethoden beeindruckende Erfolge zu erzielen sind, teils auch in Kombination mit aufwändiger technischer Überwachung (z. B. „Black Hand“ in Frankreich oder „Elysium“ in Deutschland).

Bei der grenzüberschreitenden Zusammenarbeit zwischen den USA und Deutschland im Fall „Wall Street Market“ haben die Ermittler auf eindrucksvolle Weise klassische Ermittlungsmethoden in Verbindung mit hochkomplexen Blockchain-Technologien genutzt, um die Täter zu überführen. Das zeigt, dass Nachrichtendienste und Strafverfolgungsbehörden entsprechend gut ausgestattet werden müssen, um dem kriminellen Missbrauch entsprechend entgegentreten zu können, wenn Verschlüsselungstechnologien breit verfügbar sind,

Vor diesem Hintergrund ist es nötig, die hohe Bedeutung der Verschlüsselung für den Wirtschaftsstandort Deutschland und Bayern mit den unabweisbaren Bedürfnissen der Sicherheitsbehörden in technikneutraler Weise in Einklang zu bringen.