RN/58

13.10

Bundesrat Werner Gradwohl (FPÖ, Steiermark): Danke, Herr Präsident! Sehr geehrter Herr Bundesminister! Herr Staatssekretär! Werte Kollegen im Bundesrat! Sehr geehrte Damen und Herren im Saal und vor den Bildschirmen via Livestream! Ich begrüße die jungen Zuhörer *(Bundesrat **Reisinger** [SPÖ/OÖ]: ... ausschließlich Zuhörer!)* im Hintergrund recht herzlich! – Danke, dass Sie so ein Interesse für den Bundesrat haben.

Wir beraten heute das Netz- und Informationssystemsicherheitsgesetz 2026 – ein Gesetz, das laut Regierung die Cybersicherheit in Österreich stärken soll. Ich sage gleich zu Beginn ganz klar: Niemand in diesem Haus stellt die Bedeutung von Cybersicherheit infrage. Cyberangriffe sind real, sie betreffen Staaten, Unternehmen und Bürger gleichermaßen. Gerade deshalb braucht es Gesetze, die wirksam, verhältnismäßig und klar sind. *(Beifall bei der FPÖ.)*

Was wir heute vorliegen haben, ist jedoch ein Entwurf, der nicht aus Überzeugung entsteht, sondern aus Druck. Die NIS2-Richtlinie ist seit Anfang 2023 in Kraft. Die Umsetzungsfrist ist im Oktober 2024 abgelaufen. Österreich ist säumig und jetzt – Jahre später – wird uns gesagt, wir müssen das beschließen, sonst droht ein Vertragsverletzungsverfahren. Zeitdruck ersetzt keine Qualität. Ein schlechtes Gesetz wird nicht besser, nur weil man es zu spät beschließt.

Die Regierung spricht von rund 4 000 betroffenen Einrichtungen. Das ist keine Randnotiz, das ist ein massiver Eingriff in unsere Wirtschafts- und Verwaltungsstruktur. Doch niemand kann heute seriös beantworten, wie viele Betriebe konkret pro Sektor, pro Bundesland und entlang der Lieferketten betroffen sein werden, denn dieses Gesetz endet nicht bei den unmittelbar erfassten Einrichtungen. Durch die Verpflichtung zur Absicherung der

Lieferkette werden auch zahlreiche kleine und mittlere Unternehmen erfasst – Betriebe, die weder vorbereitet noch informiert wurden. Das ist keine Transparenz, das ist Unsicherheit per Gesetz.

Besonders gravierend ist die Kostenfrage. Die Regierung legt keine nachvollziehbare Gesamtkostenabschätzung vor – weder für die Unternehmen noch für die öffentliche Hand. Internationale Vergleiche zeigen: Die einmaligen Implementierungskosten reichen von 10 000 Euro bis weit über 1 Million Euro. Dazu kommen laufende Kosten von 100 000 Euro pro Jahr – für zusätzliches Personal, externe Prüfungen, technische Sicherheitsmaßnahmen und umfassende Dokumentationspflichten. Diese Kosten verschwinden nicht, sie werden weitergegeben: an Konsumentinnen und Konsumenten, an Patientinnen und Patienten, an die gesamte Bevölkerung.

Kommen wir zu den Sanktionen: Geldstrafen von bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes. Das ist kein pädagogischer Zeigefinger, das ist eine existenzielle Bedrohung. *(Beifall bei der FPÖ.)*

Gleichzeitig bleiben die gesetzlichen Pflichten erstaunlich unklar. Es ist die Rede von geeigneten Maßnahmen, von Verhältnismäßigkeit, von gebührender Berücksichtigung von Risiken. Was das konkret bedeutet, soll eine Behörde per Verordnung festlegen können. Das Parlament gibt Kompetenzen ab und das Risiko bleibt bei den Unternehmern.

Besonders problematisch ist auch die institutionelle Konstruktion: Die neue Cybersicherheitsbehörde wird direkt dem Innenminister unterstellt. Gleichzeitig ist dieses Ressort für Überwachungsinstrumente zuständig, die strukturell davon leben, dass Sicherheitslücken existieren. Wer Sicherheitslücken schließen soll, darf kein Interesse daran haben, sie offenzuhalten.

Mit diesem Gesetz schaffen wir einen großen neuen Apparat: ein Bundesamt, mehrere Computer-Notfallteams, Sondergremien, Koordinationsstellen im Gesundheitsbereich. Die Kosten für die öffentliche Hand werden sich in den nächsten fünf Jahren auf geschätzte 150 bis 200 Millionen Euro belaufen. Mehr Behörden bedeuten aber nicht automatisch mehr Sicherheit.

Der Bundesrat ist nicht dazu da, Gesetze einfach durchzuwinken. Er ist dazu da, dort Nein zu sagen, wo ein Gesetz aus dem Gleichgewicht gerät. *(Beifall bei der FPÖ.)*

Cybersicherheit darf kein Vorwand für Bürokratie, unklare Pflichten und Millionenstrafen sein. Sicherheit entsteht durch klare Regeln, nicht durch Angst.

Ein Gesetz, das Kosten verschweigt, Verantwortung abschiebt und Existenzen gefährdet, ist kein gutes Gesetz. Ein schlechtes Gesetz wird nicht richtig, nur weil die EU Druck macht. Ein teures Gesetz wird nicht gerecht, nur weil man es Sicherheit nennt. Deshalb sage ich klar und verantwortungsvoll: Aus diesen Gründen können wir diesem Gesetz nicht zustimmen. *(Beifall bei der FPÖ.)*

13.16

Vizepräsident Michael Wanner: Als Nächster zu Wort gemeldet ist Bundesrat Klubvorsitzender Mag. Harald Himmer.