Sächsischer Landtag
6. Wahlperiode

DRUCKSACHE 6/12999

Antrag

der **Fraktion DIE LINKE.**

Thema: Erhebliche Subsidiaritätsbedenken bezüglich des Vorschlages für eine „Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (Grenzen und Visa) und zur Änderung der Entscheidung 2004/512/EG des Rates, der Verordnung (EG) Nr. 767/2008, des Beschlusses 2008/633/JI des Rates, der Verordnung (EU) 2016/399 und der Verordnung (EU) 2017/2226, COM(2017) 793 final“(*Bundesrat-Drucksache: 45/18*) und des Vorschlages für eine „Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration), COM(2017) 794 final“(*Bundesrat-Drucksache: 46/18*)

Der Landtag möge beschließen:

I.

Der Landtag stellt unter Anerkennung der Bemühungen für eine effektive Nutzung von auf gesetzlicher Grundlage und bei Einhaltung höchster Datensicherheits- und Datenschutzstandards erhobener elektronischer Daten durch Polizei- und Justiz im Rahmen ihrer Aufgabenerfüllung mit dem Ziel der Erhöhung öffentlicher Sicherheit und einer effektiven rechtsstaatlichen Justiz zu den o. g. Bundesrat-Drucksachen: 45/18 sowie 46/18 folgende erheblichen Bedenken fest:

1. die Anlage und Nutzung digitaler Massendaten, wie sie von den oben näher bezeichneten Rechtssetzungsvorschlägen der Europäischen Union mit strategischer Absicht im Bereich der Entwicklung von IT-Großsystemen bis 2023 in einem interoperablen Gesamtverbund in die Alltagspraxis insbesondere von Polizei und Grenzschutz umgesetzt werden sollen, müssen in rechtlich gesicherter Weise zwingend einer strikten und wirksamen politischen Steuerung sowie ebenso wirksamen parlamentarischen und Datenschutzkontrolle unterworfen sein;

Dresden, 06.04.2018 - b.w. -

Rico Gebhardt
Fraktionsvorsitzender

Eingegangen am: 06.04.2018 Ausgegeben am: 06.04.2018

2. Wirtschafts- und Marktinteressen, technische Möglichkeiten oder alles technisch Machbare bei der Digitalisierung im Bereich Sicherheit und Justiz dürfen nicht die Zwecke und Maßnahmen der Digitalisierungspolitik bestimmen, vielmehr muss demokratische Politikgestaltung die Zwecke und Funktionen der Digitalisierung setzen, diese überwachen und deren Umsetzung garantieren;

3. gleichwohl die neuen Strukturen der digitalen Governance, die in den letzten Jahren auch im „Raum der Freiheit, der Sicherheit und des Rechts“ rasant entstanden bzw. zu neuer Qualität ausgebaut worden sind (exemplarisch seien hier für den Sicherheits- und Justizbereich euLISA, ENISA, meCodex, EGVP, GKDZ und LIT genannt), treffen die o. g. Verordnungsvorschläge keine dringend erforderlichen Regelungen zur ausnahmslosen Gewährleistung der demokratischen und rechtsstaatlichen Grundverfasstheit der Europäischen Union und ihrer Mitgliedsstaaten sowie der daraus resultierenden Rechte oder des Rechtsschutzes für die betroffenen Bürgerinnen und Bürger;

4. mit den o. g. Verordnungsvorschlägen wird eine schon bestehende Substruktur von Institutionen, die in Distanz zur Steuerung und Kontrolle durch demokratische Institutionen auf allen Ebenen des EU-Multi-Level-Governance-Systems bis auf die regionale Ebene weitgehend eigenständig und mit geringen oder fehlenden Möglichkeiten demokratische Teilhabe über Grundfragen der Entwicklung der Digitalisierung und daraus folgende tiefgreifende gesellschaftliche Transformationen entscheiden und vollendete Tatsachen schaffen („Smarte Diktatur“ nach Harald Welzer), weiter verfestigt, ohne dass dies in den Vorschlägen berücksichtigt worden ist;

5. die o. g. Rechtssetzungsvorhaben der Europäischen Union berühren sowohl Bundesrecht wie auch jene Teile des Landesrechtes (angefangen beim Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 33 der Verfassung des Freistaates Sachsen, über die Bestimmungen des Sächsischen Datenschutzgesetzes bis hin zum Sächsischen E-Government-Gesetz), welche die Ausgestaltung der Digitalisierung im Bereich Sicherheit und Justiz regeln und daher zwangsläufig deren Anpassung – insbesondere im Bereich der Schutzes personenbezogener Daten – zur Folge haben werden;

6. die mit den Verordnungsvorschlägen angestrebte Öffnung des europaweiten Zugangs zu zentralen EU-Datenbanken für Polizei- und Grenzschutzbeamte über das „Europäische Suchportal“ (ESP) im operativen Dienst, welche überwiegend Personendaten enthalten, die auch aus Vorgängen im Rahmen der Gefahrenabwehr oder der Strafverfolgung in Deutschland und auch Sachsen stammen können, schafft grundlegend neue Herausforderungen für die Gewährleistung der Datensicherheit und des Datenschutzes, die bisher nur unzureichende Berücksichtigung in den Verordnungsvorschlägen gefunden haben;

7. angesichts der mit den o. g. Verordnungsentwürfen angestrebten ausgeweiteten massenhaften Datennutzung muss eine wirksame Kontrolle der Wahrung von Verhältnismäßigkeit und Zweckbindung bei der Datenerhebung und -verarbeitung durch bislang fehlende klare und eindeutige Regelungen zur Gewährleistung einer unabhängigen, vollständigen und vor allem ungehinderten Kontrolle der Einhaltung von Datensicherheit und Datenschutz und der Aufdeckung möglichen Datenmissbrauchs besonders durch die Datenschutzbeauftragten sichergestellt sein.

II.

Der Landtag fordert die Staatsregierung auf der Grundlage der vorangegangenen Feststellungen auf,

1. die im Antragspunkt I. dargestellten (und ihre ggf. eigenen weiteren) Bedenken bei der Behandlung der EU-Rechtssetzungsvorschläge im Rahmen der Subsidiaritätskontrolle vor Ablauf der Frühwarnfrist am 16. April 2018 bei der Europäischen Kommission für den Freistaat Sachsen förmlich einzuwenden sowie auf entsprechende Korrekturen und Anpassungen hinzuwirken;
2. die ihr zur Verfügung stehenden Mittel und Möglichkeiten auf Bundes- und EU-Ebene zu nutzen, um die nach dem Antragspunkt I dargestellten Bedenken auch nach Ablauf der Frühwarnfrist einzubringen und auf eine dementsprechende Änderung der betreffenden EU-Rechtssetzungsvorhabens zu drängen.

Begründung:

Die oben näher bezeichneten Rechtssetzungsvorschläge der Europäischen Union zur Herstellung voller Interoperabilität zwischen EU-Informationssystemen (Grenzen und Visa; polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) entsprechen den Erfordernissen von euLISA, wie sie in der VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, zur Änderung der Verordnung (EG) Nr. 1987/2006 und des Ratsbeschlusses 2007/533/JI sowie zur Aufhebung der Verordnung (EU) Nr. 1077/2011, COM(2017) 352 final, festgelegt wurden. Sie liefern die rechtliche Grundlage für die Vernetzung relevanter Datenbanken, die als IT-Großsysteme von euLISA betreut und entwickelt werden und verpflichten gleichzeitig die EU-Mitgliedsstaaten (Schengen-Raum) zur Umsetzung.

Gleichwohl Interoperabilität von IT-Großsystemen im „Raum der Freiheit, der Sicherheit und des Rechts“ bei Einhaltung höchster Standards für Datensicherheit und Datenschutz zur Erhöhung öffentlicher Sicherheit und effektiver Strafverfolgung als eine Folge der beabsichtigten Digitalisierung nicht grundsätzlich abzulehnen sein mag, ist jedoch zu beobachten, dass der Trend und die offensichtliche Absicht zu einer vollen Ausschöpfung der mit der Digitalisierung im Bereich Inneres und Justiz gegebenen technischen Möglichkeiten weder demokratisch hinsichtlich ihrer tiefgreifenden Wirkungen debattiert, noch umfassend politisch gesteuert und kontrolliert wird.

Mögliche Risiken für die Grundrechte der Bürgerinnen und Bürger werden zwar benannt, aber – jenseits einer wirksamen Kontrolle oder dar eines wirkungsvollen Rechtsschutzes – nur rudimentär eingegrenzt und überwacht.

Dieses sich **abzeichnende starke Ungleichgewicht** zwischen den technischen Möglichkeiten durch Digitalisierung bei Gefahrenabwehr und Strafverfolgung, Grenzschutz und Migrationskontrolle zum einen, dem fehlenden Primat der Politik (unter Einschluss echter parlamentarischer Kontrolle) gegenüber der technologie-getriebenen Digitalisierung zum anderen sowie einer wirklichen Balance der mit der Digitalisierung entstandenen technischen Möglichkeiten der Datenverarbeitung mit dem Schutz von Grundrechten und

ihrer effektiven Durchsetzung zum dritten, droht mit den beiden Verordnungsvorschlägen zur Herstellung voller Interoperabilität zwischen EU-Informationssystemen weiter zu verstärken.

Der Sächsische Landtag ist gefordert, mit allen ihm zur Verfügung stehenden Mitteln, auf diese Entwicklungen aufmerksam zu machen und auf die Politik der Digitalisierung Einfluss zu nehmen, um eine demokratische Gestaltung derselben im Bereich Sicherheit, Justiz und Migrationskontrolle zu erreichen.

Werden die auch mit den oben näher bezeichneten Rechtssetzungsvorschlägen der Europäischen Union angestrebten Strukturveränderungen nicht hinreichend demokratisch eingebunden, droht die von Harald Welzer antizipierte „Smarte Diktatur". Insbesondere im Bereich der Migrationskontrolle werden die dunklen Visionen des interoperablen IKT-Sicherheits- und Justizsystems deutlich: Bürgerinnen und Bürger werden zunehmend und am Ende allumfassend digital erfasst und einem Ranking als Sicherheitsrisiko unterzogen. Es gehört schon heute nicht mehr ins Reich der Fantasie, dass dieses Monitoring und Ranking maschinengestützt vollzogen wird und Entscheidungen entweder auf dieser Basis durch Menschen oder aber durch die datenverarbeitenden Maschinen selbst getroffen werden.

Ein besonderes Problem ergibt sich aus dem in Umsetzung der Verordnungsvorschläge zu erwartenden täglichen europaweiten und massenhaften Zugriff über das „Europäische Suchportal" (ESP) durch Polizei- und Grenzbeamte im Schengen-Raum aber auch darüber hinaus in der EU bzw. über Interpol.

Wie der Europäische Datenschutzbeauftragte in seinem „Reflexionspapier zur Interoperabilität von Informationssystemen im Raum der Freiheit, der Sicherheit und des Rechts" vom 17. November 2017 feststellt, beobachtet seine Behörde „immer wieder, dass technische Machbarkeit eines Datenaustauschs zwangsläufig dazu führt, dass diese Daten tatsächlich ausgetauscht werden. … Es besteht die Gefahr, dass in einem solchen Fall die Mittel das Ziel heiligen." (S. 6)

Diese aus der unmittelbaren praktischen Erfahrung des Europäischen Datenschutzbeauftragten stammenden Warnungen stehen in direktem Zusammenhang mit den Feststellungen unter Punkt 1 bis Punkt 5, nämlich damit, dass die mit der Datenverarbeitung und Bereitstellung beauftragten Institutionen Eigeninteressen (ver)folgen, die aus den Möglichkeiten des „Mittels" erwachsen und das (ursprüngliche) politische Ziel überlagern.

Der Bundesrat hat die Entstehung und Nutzung der IT-Großsysteme im Sicherheits- und Justizbereich von Beginn an kritisch begleitet. Bereits die Verordnung zur Errichtung der Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts[1] war vom Bundesrat mit einem Beschluss[2] ganz grundsätzlich mit Blick auf Subsidiarität und Verhältnismäßigkeit in Frage gestellt worden.

[1] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung einer Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht KOM(2009) 293 endg.; Ratsdok. 11722/09.
[2] Drucksache 648/09 (Beschluss) vom 18.09.09.

Insbesondere wurden in dem Bundesratsbeschluss die mangelnde Begründung der zwingenden Notwendigkeit der Einrichtung einer solchen Agentur, die Kosten-Nutzen-Relation (Verhältnismäßigkeit) und die unzureichende Beachtung des Schutzes von Grund- und Menschenrechten sowie des Datenschutzes hervorgehoben.

Die bereits in der Begründung der **Subsidiaritätsbedenken bezüglich des Vorschlages für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, zur Änderung der Verordnung (EG) Nr. 1987/2006 und des Ratsbeschlusses 2007/533/JI sowie zur Aufhebung der Verordnung (EU) Nr. 1077/2011, COM(2017) 352 final (Drs. 6/10629)** vorgetragene Kritik, insbesondere aber, dass „(dem) gigantischen Netzwerk von EU-weiten Datenverarbeitungssystemen im Bereich von Sicherheit und Justiz … derzeit kein auch nur annähernd gleichwertig effektiv funktionierendes System demokratischer, parlamentarisch-öffentlicher Kontrolle entgegen (steht)“, muss mit Blick auf die diesem Antrag zugrundeliegenden Verordnungsvorschläge nicht nur wiederholt, sondern verstärkt werden.

Eine ernstgemeinte, effektive und vor allem unabhängige Kontrolle des Funktionierens (bzw. Nicht-Funktionierens) der IT-Großsysteme gerade im „Raum der Freiheit, der Sicherheit und des Rechts“ und ihrer Nutzung setzt unter anderem voraus, dass klare Regeln zu einer permanenten internen Untersuchung durch unabhängige externe Sachverständige, die mit ausreichender Ausstattung bei den Datenschutzbeauftragten angesiedelt sein könnten, dass Beschwerde- und Auskunftsrechte für potenziell Betroffene klar ausgestaltet werden und ebenso zwingende Auskunftspflichten für die datenverarbeitenden Institutionen für den gesamten Anwendungsbereich der Verordnungsvorschläge existieren.

Die auf den Seiten 20 ff. der beiden Verordnungsvorschläge gegebenen Erklärungen zu „Grundrechten“, „Schutz personenbezogener Daten“ oder zum „Monitoring“ bzw. die entsprechenden Regelungen in den Verordnungen sind eher allgemeiner und rechtlich unverbindlicher Natur. Derartige faktische Versprechen wie

> „Die Kommission wird dafür sorgen, dass Verfahren zur Überwachung der Entwicklung und Funktionsweise der vier Komponenten (Europäisches Suchportal, gemeinsamer Dienst für den Abgleich biometrischer Daten, gemeinsamer Speicher für Identitätsdaten, Detektor für Mehrfachidentitäten) und des zentralen Speichers für Berichte und Statistiken eingeführt werden, und sie nach Maßgabe der wichtigsten politischen Ziele bewerten…Darüber hinaus hat die Kommission fünf Jahre nach Einführung und Inbetriebnahme der Funktionen und danach alle vier Jahre eine Gesamtbewertung der Komponenten zu erstellen, die auch die direkten oder indirekten Auswirkungen der Komponenten und ihrer praktischen Umsetzung auf die Grundrechte beinhaltet.“ (S. 25f.)

sind abstrakt, unverbindlich und gewähren keinerlei wirksame Kontrolle, geschweige denn Rechtsschutz. Hier besteht deutlich Verbesserungsbedarf.

Nach der Datenschutz-Grundverordnung besteht – auch – für EU-Institutionen die gesetzliche Verpflichtung, Datenschutz by Design zu gewährleisten. In den am 23. März 2018 erschienen „Guidelines on the protection of personal data in IT governance and IT management of EU Institutions” des Europäischen Datenschutzbeauftragten heißt es dazu:

> “This will mean that data protection and privacy must be built in to the design specifications and architecture of information and communication systems and technologies. Similar obligations will apply to EU Institutions and Bodies.”

Zwar sind Ansätze des Datenschutzes by Design in den Verordnungsvorschlägen enthalten, wie im Zusammenhang mit Artikel 36 das „Führen von Protokollen“ zu allen Datenverarbeitungsvorgängen. Fraglich ist hier aber schon, ob die vorgesehene Aufbewahrungsfrist von einem Jahr ausreicht, um längerfristige Muster von Missbrauch festzustellen.

Hinzu kommt: Die volle Umsetzung der Guidelines des EU-Datenschutzbeauftragten vom 23. März 2018, die sich speziell an EU-Institutionen wenden, ist in den Verordnungsvorschlägen nicht zu erkennen, insbesondere, soweit es um die Begrenzung, Verhältnismäßigkeit und Zweckbindung der Datennutzung im Rahmen der interoperablen IT-Großsysteme in Verantwortung von euLISA geht.

Im Rahmen der Subsidiaritätskontrolle ist nach Art. 5 Abs. 4 EUV gerade auch die Verhältnismäßigkeit von Maßnahmen der EU zu prüfen und ggf. einzufordern. Die Beachtung und rechtliche Umsetzung der Guidelines des EU-Datenschutzbeauftragten vom 23. März 2018 sollte in Umsetzung der mit diesem Antrag formulierten Subsidiaritätsbedenken in der Perspektive von Verhältnismäßigkeit und des effektiven Schutzes der Rechte der Betroffenen befördert werden.