Bundesrat **Drucksache** **340/21**

30.04.21

Antrag
des Landes Hessen

Entschließung des Bundesrates - Europäische Datensouveränität schützen

Der Hessische Ministerpräsident Wiesbaden, 29. April 2021

An den
Präsidenten des Bundesrates
Herrn Ministerpräsidenten
Dr. Reiner Haseloff

Sehr geehrter Herr Präsident,

die Hessische Landesregierung hat beschlossen, die anliegende

Entschließung des Bundesrates - Europäische Datensouveränität schützen

mit dem Antrag zuzuleiten, die Entschließung zu fassen.

Ich bitte Sie, die Vorlage gemäß § 36 Absatz 2 der Geschäftsordnung des Bundesrates in die Tagesordnung der 1004. Plenarsitzung am 07. Mai 2021 aufzunehmen und sie anschließend den Ausschüssen zur Beratung zuzuweisen.

Mit freundlichen Grüßen
Volker Bouffier

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

Entschließung des Bundesrates - Europäische Datensouveränität schützen

Der Bundesrat möge beschließen:

1. Der Bundesrat sieht die Digitalisierung als große Zukunftschance. Nahezu alle Bereiche des menschlichen Daseins sind bereits von digitalen Leistungen durchdrungen. Die Anwendungsbreite der Digitalisierung scheint dabei schier unendlich. Angefangen von Dienstleistungen in sozialen Medien bis hin zur Wirtschaft 4.0 hat die Digitalisierung in den letzten Jahren Einzug in den Alltag der allermeisten Menschen gefunden und führt zu einem umfassenden Wandel der Wirtschaft. Dabei erreichen die erfassten personenbezogenen und sonstigen Daten sowohl in der Bandbreite als auch in der Menge immer neue Dimensionen.

2. Die Europäische Kommission hat die Bedeutung von Daten erkannt. In ihrer Datenstrategie vom 19.02.2020 erläuterte sie ihre Vorstellung eines gemeinsamen europäischen Datenraums, d. h. eines Binnenmarkts für Daten, in dem Daten unabhängig vom physischen Ort ihrer Speicherung in der Union unter Einhaltung des geltenden Rechts verwendet werden können. Zur Umsetzung der Datenstrategie hat sie am 25.11.2020 einen Entwurf für eine Daten-Governance-Initiative vorgestellt. Ein weiterer Legislativvorschlag, der sogenannte Data Act, wird im Laufe des Jahres folgen. Ebenfalls von Bedeutung für den europäischen Datenraum ist der Digital Markets Act vom 15.12.2020. Mit diesen Initiativen hat die EU-Kommission nicht nur den Regulierungsbedarf erkannt, sie eröffnet auch die Diskussion zur Erneuerung unseres Verständnisses von Daten. Begriffe wie Datentreuhänder, Datenuntreue oder Datenspende werden unser Verständnis von Daten, deren Dimension und Wert neu definieren.

3. Der Bundesrat begrüßt, dass die EU-Kommission sich des Themas angenommen hat und auch, dass sie in den Vorhaben einen ausgewogenen Weg zwischen der Nutzung wertvoller Daten für die Gesellschaft, der Schaffung europäischer Datenräume zur Sicherung der Wettbewerbsfähigkeit der europäischen Wirtschaft und der Regulierung der Nutzung von großen Datenmengen durch private und staatliche Stellen sucht.

4. Die Entwicklungen der letzten Jahre haben gezeigt, dass einstige Start-up-Unternehmen wie Google, Facebook, Alibaba oder Amazon mit ihren Geschäftsmodellen zu großen BigTech Datenkonzernen herangewachsen und viele neue Akteure, wie zum Beispiel Content Delivery Networks (CDN), entstanden sind. Ein wichtiger Bestandteil ihrer Tätigkeit besteht darin, personenbezogene Daten einer Vielzahl von Nutzerinnen und Nutzern mit Algorithmen zu verarbeiten und kommerziell nutzbar zu machen. Neben der Auswertung von Bewegungsprofilen, Medienkonsumverhalten, Kaufpräferenzen und Kommunikationsvorlieben mit dem Ziel der Bildung individueller oder gruppenbasierter Persönlichkeitsprofile, werden Nutzerdaten auch gesammelt, strukturiert und ausgewertet, um diese zur Weiterentwicklung der eigenen Dienste, zur Vermarktung an Dritte oder Entwicklung neuer Geschäftsfelder und -modelle zu verwerten. Zugleich haben sich Strukturen mit großer Marktmacht bis hin zu Monopolstrukturen entwickelt und verfestigt, die Marktbarrieren schaffen und einen fairen Wettbewerb verhindern.

5. Der Bundesrat stellt in diesem Zusammenhang fest, dass einige Maßnahmen zur Verbesserung des Datenschutzes und des Verbraucherschutzes erreicht wurden. Ein in Europa großer Schritt war zuletzt die Datenschutzgrundverordnung und die damit korrespondierenden Datenschutzgesetze des Bundes und der Länder. Es ist aber auch festzustellen, dass diese Maßnahmen die Datenerfassung und -verarbeitung durch private Unternehmen nur in begrenztem Umfang einschränken konnten. Im Tausch gegen die Nutzung von Angeboten vollen Umfangs stimmen viele Nutzerinnen und Nutzer einer Erhebung ihrer personenbezogenen Daten zu, auch in Ermangelung einer konsequenten Umsetzung eines stringenten Kopplungsverbots. Dabei ist der bzw. dem Einzelnen die volle Tragweite seiner Zustimmung oftmals gar nicht bewusst. Dies gilt insbesondere für die stetig wachsenden komplexen Verwertungsstrukturen und zukünftigen Verwertungsmöglichkeiten erhobener Daten bzw. erzeugter Metadaten.

6. Die nachträgliche Kontrolle der Nutzung einmal zur Verfügung gestellter bzw. erhobener Daten durch die Technologiekonzerne bzw. Dritte ist kaum möglich. Angesichts der technischen und strukturellen Komplexität, der im Regelfall Undurchsichtigkeit der komplexen informationstechnischen Aus- und Verwertung der Daten sowie oftmals intransparenten und schnell wechselnden Unternehmensstrukturen, Geschäftsmodelle und Verbindungen der Technologiekonzerne

fällt es Nutzerinnen und Nutzern sowie Datenschützerinnen und Datenschützern schwer, eine missbräuchliche Nutzung von Nutzerdaten zu erkennen oder nachzuweisen. Gleiches gilt in Bezug auf etwaige wettbewerbsrechtlich oder kartellrechtlich problematische Verhaltensweisen der Technologiekonzerne oder Dritter, die auf einer entsprechenden Datenerhebung bzw. Nutzung beruhen. Oftmals sind die unterschiedlichen Datensätze weltweit dezentral gespeichert und verwaltet.

7. Gemäß Art. 5 Buchst. a) des Verordnungsvorschlages der Europäischen Kommission für ein Gesetz über digitale Märkte („Digital Markets Act“) soll z.B. den Gatekeepern verboten werden, personenbezogene Daten aus ihren zentralen Plattformdiensten mit personenbezogenen Daten aus anderen von ihnen oder Dritten angebotenen Diensten zusammenzuführen oder die Nutzerin bzw. den Nutzer automatisch bei mehreren Diensten anzumelden, außer wenn der Endnutzerin bzw. dem Endnutzer diesbezüglich gemäß der Verordnung (EU) 2016/679 eine Wahl gegeben wurde und sie bzw. er eingewilligt hat. Der Bundesrat sieht darin einen richtigen Ausgangspunkt dafür, die Datensouveränität besser zu schützen. Es ist gängige Praxis, nicht nur unter Gatekeepern, manipulative Auswahlmenüs oder Entscheidungsarchitekturen zu nutzen, um solche Nutzereinwilligungen zu erhalten. Der Bundesrat bittet deshalb darum, dass der Gedanke des Art. 5 Buchst. a) des Digital Markets Act-Entwurfs auch bei weiteren Regulierungsvorhaben Eingang findet. Der Gesetzgeber muss sicherstellen, dass Gatekeeper die Beschränkung der Zusammenführung von Nutzerdaten oder der automatischen Anmeldung bei mehreren Diensten nicht umgehen. Um dies zu gewährleisten, muss nach Auffassung des Bundesrates das Umgehungsverbot in Art. 11 um Bestimmungen ergänzt werden, die verhindern, dass Gatekeeper die Zustimmung der Endnutzerinnen und Endnutzer durch Ausnutzung manipulativer Entscheidungsarchitekturen – Stichwort „Dark Patterns“ – und sogenannter „Biases“ erlangen, zum Beispiel durch eine irreführende Optik oder Menüführung der Webseite.

8. Der Bundesrat stellt fest, dass große Technologieunternehmen zunehmend weitere Wirtschaftsbereiche in den Blick nehmen und ihre bisherigen Möglichkeiten und Fähigkeiten dazu nutzen, neue Geschäftsmodelle zu entwickeln. Neben dem Bereich der Finanz- und Lieferdienstleistungen sowie des Medien- und Entertainmentsektors ist zunehmend die Gesundheitswirtschaft im Fokus. Ein Beispiel

dafür ist der Kauf von Fitbit durch Google. Dabei nutzen die Unternehmen ihre aus anderen Bereichen gewonnenen Erkenntnisse (die ggf. auf Nutzerdaten beruhen), um sich Wettbewerbsvorteile zu sichern.

9. Der Bundesrat verweist in diesem Zusammenhang auf die ähnlich gelagerte, aber deutlich vorangeschrittene Debatte um die technologische Souveränität in der EU. Hierbei geht es regelmäßig darum, wichtige technologische Schlüsselbereiche zum Beispiel im Mobilfunksektor (5G) oder der Batterie- und Wasserstofftechnologie durch umfangreiche Strategien besser zu schützen. Der Debatte um eine technologische Souveränität muss auch eine intensive Diskussion um eine europäische Datensouveränität folgen, wie sie bereits im Rahmen der europäischen Cloud-Initiative GAIA-X angelegt ist. Dabei geht es nicht darum, im globalen Kontext einen europäischen Sonderweg zu gehen. Vielmehr ist eine bestmögliche Balance zwischen den Vorteilen und den Risiken der Digitalisierung für die Nutzerinnen und Nutzer zu erreichen. Dies ist nur dann zu gewährleisten, wenn der Gesetzgeber einen festen Rahmen, insbesondere im Hinblick auf Datenschutz und Wettbewerb setzt, diesen bei neuen Entwicklungen zur Sicherung von Datenschutz und Wettbewerb angemessen überprüft und gegebenenfalls anpasst und wenn dessen Einhaltung sichergestellt ist. Nur so können europäische Werte, wie das Recht auf informationelle Selbstbestimmung, einen wirksamen Schutzraum darstellen. Der EU-Rechtsrahmen könnte damit auch insoweit Leitbild für Reformbemühungen in Drittstaaten werden und global Standards setzen.

10. Angesichts der Möglichkeiten von Gatekeeper-Plattformen zur Profilbildung sowie zur Deanonymisierung und Depseudonymisierung von Daten bittet der Bundesrat die Bundesregierung zudem, auf die besondere Sensibilität von sehr persönlichen Daten, wie Gesundheitsdaten, zu achten. Insbesondere Daten aus dem Bereich medizinischer Anwendungen oder softwaregestützten Operationsanwendungen müssen einem besonderen Schutz unterliegen. Eine Verknüpfung von sensiblen Gesundheitsdaten mit personenbezogenen Informationen aus der Nutzung digitaler Dienstleistungen aus anderen Geschäftsfeldern (beispielsweise Suchmaschinenabfragen, Positionsdaten und Sprachdaten), die zu umfassenden Persönlichkeitsprofilen verknüpft werden könnten, sollte beschränkt werden. Zum Schutz der digitalen Souveränität von Patientinnen und Patienten ist die Verarbeitung hochsensibler Gesundheitsdaten und weiterer personenbezogener Da-

ten, die nicht zur Bereitstellung von Gesundheitsdiensten benötigt werden, gesetzlich zu regulieren. Dies gilt insbesondere für Anbieter, die in anderen Geschäftsfeldern als dem Gesundheitsmarkt digitale Dienstleistungen erbringen und auf diese Weise personenbezogene Daten für die kommerzielle Nutzung generieren.

11. Weiterhin bittet der Bundesrat Entflechtungstatbestände zu schaffen, die private Unternehmen, die Gesundheitsdaten verarbeiten und gleichzeitig andere, nicht gesundheitsspezifische Dienstleistungen, etwa Kranken- und Lebensversicherungen anbieten, erfassen. In diesem Zusammenhang erinnert der Bundesrat an seinen Beschluss vom 29.11.2019 (BR-Drs. 539/19), mit dem festgestellt worden ist, dass im Krankenversicherungswesen das Grundprinzip der Solidarversicherung zu schützen sei. Diesem Grundprinzip liefe eine laufende automatisierte Übertragung hochsensibler Gesundheitsdaten an die Krankenversicherer oder deren Partnerunternehmen zur Tarifgestaltung zuwider, die beispielsweise durch Fitness-Tracker und die dazugehörigen Apps unproblematisch technisch möglich ist. Insbesondere gelte es zu verhindern, dass Self-Tracking-Tarife den Krankenversicherungsmarkt durchdringen und sich Versicherungsnehmerinnen und Versicherungsnehmer aus ökonomischem Druck zur Preisgabe ihrer höchstpersönlichen Gesundheitsdaten veranlasst sehen. In diesem Sinne sollte es künftig auch mit der Zustimmung der Patientinnen und Patienten nicht möglich sein, Gesundheitsdaten in anderen Geschäftsfeldern anzubieten oder mit anderen personenbezogenen Daten zusammenzuführen, um diese kommerziell zu verwenden. Kranken- und Lebensversicherungen, die auf Basis solcher Daten angeboten werden, riskieren das Prinzip der Solidargemeinschaft in der Krankenversorgung.