

Inhaltsprotokoll

Öffentliche Sitzung

Ausschuss für Digitalisierung und Datenschutz

72. Sitzung
18. Mai 2026

Beginn: 14.00 Uhr
Schluss: 15.53 Uhr
Vorsitz: Johannes Kraft (CDU)

Vor Eintritt in die Tagesordnung

Siehe Beschlussprotokoll.

Punkt 1 der Tagesordnung

Aktuelle Viertelstunde

Vorsitzender Johannes Kraft hält fest, dass im Vorfeld der Sitzung keine schriftlichen Fragen eingereicht worden seien.

Stefan Ziller (GRÜNE) fragt vor dem Hintergrund der aktuellen Presseberichterstattung zum ITDZ, ob auf der letzten Verwaltungsratssitzung der Wirtschaftsplan beschlossen worden sei und auf welcher Grundlage das ITDZ derzeit arbeite.

Staatssekretär Matthias Hundt (Skzl) erklärt, dass in der Sitzung ein Nachtragshaushalt ohne Bezug zum eigentlichen Haushalt vorgelegt, jedoch nicht beschlossen worden sei. Der Vorgang werde derzeit geprüft. Die nächste Verwaltungsratssitzung finde am 11. Juni statt und werde sich neben den Themen Liquidität und Finanzen auch damit befassen.

Stefan Ziller (GRÜNE) fragt nach, ob auch die Vertreterin der Finanzverwaltung an der Sitzung teilgenommen habe und wie der aktuelle Arbeitsstand zwischen Senatskanzlei und Finanzverwaltung zum ITDZ sei.

Vorsitzender Johannes Kraft macht darauf aufmerksam, dass Einzelpersonalangelegenheiten nicht in öffentlicher Sitzung behandelt würden.

Staatssekretär Matthias Hundt (Skzl) unterstreicht, dass Senatskanzlei und Finanzverwaltung beim Thema ITDZ eng zusammenarbeiteten. Die Finanzverwaltung sei in der Verwaltungsratssitzung vertreten gewesen.

Der **Ausschuss** schließt den Tagesordnungspunkt ab.

Punkt 2 der Tagesordnung

Bericht aus der Senatskanzlei

Staatssekretär Matthias Hundt (Skzl) berichtet, dass die Digitalministerkonferenz in Hamburg stattgefunden habe. Im Mittelpunkt hätten die Fortsetzung und Weiterentwicklung der Föderalen Modernisierungsagenda sowie deren Ökosystem und Arbeitsweise gestanden. Zudem sei der gemeinsame Antrag von Baden-Württemberg, Bayern, Hessen, Sachsen und Schleswig-Holstein „Gründen in 24 Stunden“ beschlossen worden. Darüber hinaus sei eine Erklärung zum Umgang mit Datenschutz verabschiedet worden. Insbesondere der Schutz von Kindern in den sozialen Medien, unter anderem im Zusammenhang mit einer Klarnamen- und Identifikationspflicht sei dabei kontrovers diskutiert worden. Hierzu sei kein Beschluss gefasst, sondern eine Arbeitsgruppe zur Erarbeitung einer gemeinsamen Position der Länder eingesetzt worden. Ein weiteres Thema sei die Zusammenarbeit der Länder mit dem Bund gewesen. Zur Bündelung von Ressourcen und der gemeinsamen Nutzung von Plattformen solle im IT-Planungsrat eine entsprechende Initiative mit einem Beschluss auf den Weg gebracht werden.

Vom 18. bis 20. Mai finde die re:publica statt. Berlin werde dort mit einem eigenen Stand und dem mobilen Bürgerservice vertreten sein. Geplant sei zudem eine Paneldiskussion sowie ein Interview mit dem rbb zum Thema BärGPT und dem Einsatz von KI.

Am 21. Mai finde das Bund-Länder-Treffen zum Digitalcheck statt. Dabei solle auch der Austausch mit dem Zentrum für Logistik fortgesetzt werden.

Außerdem werde am 28. Mai der Open Data Day im Festsaal des Roten Rathauses veranstaltet.

Dr. Matthias Kollatz (SPD) fragt in Bezug auf den Bericht zur Digitalministerkonferenz, welche Position Berlin in der Arbeitsgruppe zum Umgang mit Datenschutz vertrete und wie die Chancen für deren Durchsetzung eingeschätzt würden.

Staatssekretär Matthias Hundt (Skzl) hebt hervor, der Schutz von Minderjährigen im Internet sei vielschichtig und könne nicht durch eine einzelne Maßnahmen gesichert werden. Berlin vertrete die Einführung einer Identifikationspflicht. Während drei Bundesländer eine Klarnamenpflicht favorisierten, wobei zugleich unterschiedliche Auffassungen zu deren Vereinbarkeit mit dem Grundgesetz bestünden, verträten andere Bundesländer die Auffassung, dass

jegliche Veränderung des Datenschutzes verfassungswidrig sei. Dies verdeutliche die Bandbreite der Diskussion.

Eine besondere Herausforderung seien die Algorithmen, die Jugendliche im Internet beeinflussten und zugleich schwer zu steuern seien. Fragen zur Unterscheidung von Realität und Fiktion, zum konsumierten Content und zu möglichen Kontrollmechanismen bei einer Regulierung seien auf der Digitalministerkonferenz ausführlich diskutiert, bislang jedoch nicht abschließend geklärt worden.

Gollaleh Ahmadi (GRÜNE) weist darauf hin, dass die Diskussion um eine Klarnamen- und Identifikationspflicht neben der Vereinbarkeit mit dem Grundgesetz auch weitere Vor- und Nachteile umfasse. Einerseits könne dadurch die Nachverfolgung von Tätern digitaler Gewalt erleichtert werden, andererseits seien Frauen bei häuslicher Gewalt ohne eine solche Pflicht besser geschützt. Welche weiteren Maßnahmen zum Schutz im digitalen Raum seien auf der Digitalministerkonferenz diskutiert worden?

Staatssekretär Matthias Hundt (Skzl) informiert, dass derzeit die Vorschläge der Bundesländer gesammelt würden, die von einzelnen Maßnahmen bis hin zu gesetzlichen Regelungen reichten. In einem gemeinsamen Positionspapier sollten anschließend die als sinnvoll und umsetzbar erachteten Maßnahmen gebündelt werden. Da mit den Ländern vereinbart worden sei, die Vorschläge vertraulich zu behandeln, könne er hierzu keine weiteren Angaben machen.

Gollaleh Ahmadi (GRÜNE) fragt, ob Berlin neben der Identifikationspflicht weitere Maßnahmen vorgeschlagen werde.

Staatssekretär Matthias Hundt (Skzl) bestätigt, dass Berlin weitere Maßnahmen erarbeitet habe. Diese würden derzeit auf ihre Rechtskonformität und Umsetzbarkeit geprüft. Er stehe hierzu mit mehreren Behörden im Austausch. Er sage zu, die Vorschläge nach Abschluss der Prüfungen vorzustellen.

Meike Kamp (Berliner Beauftragte für Datenschutz und Informationsfreiheit) stellt dem Ausschuss Cay Cornelius vor, der die Leitung der Abteilung III – Recht –, insbesondere für den nicht öffentlichen Bereich, übernommen habe.

Der **Ausschuss** schließt den Tagesordnungspunkt ab.

Punkt 3 der Tagesordnung

Besprechung gemäß § 21 Abs. 3 GO Abghs
**Verantwortung der Plattformen: Daten- und
Jugendschutz in sozialen Medien**
(auf Antrag der Fraktion der CDU und der Fraktion der
SPD)

[0160](#)
DiDat

Hierzu: Anhörung

Vorsitzender Johannes Kraft begrüßt die Anzuhörenden in alphabetischer Reihenfolge und hält deren Einvernehmen, dass die Sitzung live übertragen und später im Internet bereitgestellt werde, fest.

Der **Ausschuss** beschließt, dass auf die Anfertigung eines Wortprotokolls verzichtet werde.

Christopher Förster (CDU) erklärt, die Risiken der Social-Media-Nutzung für Kinder und Jugendliche würden derzeit international, auf europäischer und auf Bundesebene intensiv diskutiert. Wie könne das Alter der Nutzerinnen und Nutzer sichergestellt werden? Wie werde mit Fake News umgegangen, und wie werde Grooming bekämpft? Könne ein Rückzug Jugendlicher infolge von Mobbing oder Suizidgefährdung rechtzeitig erkannt werden? Das Ende 2025 in Australien eingeführte Social-Media-Verbot für unter 16-Jährige habe dazu geführt, dass sich inzwischen mehrere Millionen Nutzerinnen und Nutzern nicht mehr auf den Plattformen bewegten.

Jan Lehmann (SPD) bemerkt eingangs, dass der hohe Frauenanteil unter den Anzuhörenden zu begrüßen sei. – Welchen Einfluss hätten Social-Media-Verbote auf die Werbung? Könne staatliche Regulierung dazu führen, dass sich Social-Media-Plattformen nicht mehr finanzieren könnten? Wie könne eine Altersverifikation für Jugendliche umgesetzt werden? Sollten sich nur Jugendliche oder alle Nutzerinnen und Nutzer verifizieren?

Vorsitzender Johannes Kraft weist die Anzuhörenden drauf hin, dass ihnen für ihre einleitenden Stellungnahmen jeweils etwa fünf Minuten zur Verfügung stünden.

Elina Eickstädt (Chaos Computer Club – CCC – e.V.) erklärt, der Chaos Computer Club sei eine Vereinigung von Hackerinnen und Hackern, die sich seit über 42 Jahren mit den gesellschaftlichen Auswirkungen von Technologie befasse. Im CCC gebe es Expertinnen und Experten zu nahezu allen Bereichen der Digitalisierung. Der CCC habe frühzeitig auf die Bedeutung von Daten und Information hingewiesen. Insbesondere für Kinder und Jugendliche bedeute das Leben in einer digitalisierten Welt häufig der Verlust der Kontrolle über die eigenen Daten. Plattformen seien zu zentralen Informationssammlern und -überwachern geworden und trügen daher eine besondere Verantwortung für Datenschutz sowie Jugend- und Medienschutz. Der CCC warne bereits seit Langem vor Geschäftsmodellen, die auf umfangreicher Sammlung, Auswertung und Weitergabe von Daten basierten. Recherchen wie die Databroker Files hätten gezeigt, in welchem Ausmaß persönliche Daten inzwischen verfügbar seien. Das führe zu einem Gefühl der Machtlosigkeit – bei Eltern, die ihren Kindern einen verantwortungsvollen Umgang mit digitalen Medien vermitteln wollten, bei Kindern und Jugendlichen, für die soziale Plattformen zugleich wichtige Kommunikations- und Beteiligungsräume sowie

potenzielle Suchtmittel seien, und bei allen Bürgerinnen und Bürgern, die die Kontrolle über ihr digitales Leben und ihre Daten zurückgewinnen wollten.

Notwendig seien daher ein gesellschaftlicher Aushandlungsprozess und eine gemeinsame Vision für eine bessere digitale Zukunft. Datenschutzfreundliche Lösungen müssten stärker in den Mittelpunkt rücken und die positiven Aspekte sozialer Netzwerke gefördert werden. Das Internet sei nicht mit den Plattformen gleichzusetzen. Statt den Schwerpunkt auf Altersverifikationen und Verbote zu legen, müsse stärker über Datenschutz und die konsequente Durchsetzung bestehender Regulierung gesprochen werden. Dafür brauche es ausreichende Kapazitäten und klarere Konsequenzen. Eine wirksame Durchsetzung von Datenschutz und Plattformregulierung könne langfristig stärker zum Jugendschutz beitragen als reine Altersverifikationslösungen.

Dr. Laura Hirvi (Meta; Public Policy Manager) erklärt, es bestehe ein gemeinsames Grundverständnis darüber, dass junge Menschen sich sicher online bewegen und zugleich die Chancen der digitalen Angebote nutzen können sollten, etwa zur Entfaltung der eigenen Identität, zum Entdecken neuer Interessen und zum Erwerb neuer Fähigkeiten.

[Es wird eine Folie gezeigt.]

Um dies sicherzustellen, habe Meta die sogenannten Teen-Konten entwickelt, die bislang noch wenig bekannt seien. Die Konten richteten sich an 13- bis 17-Jährige und berücksichtigten sowohl die Bedürfnisse der Eltern als auch von Kindern und Jugendlichen. Die integrierten Schutzmaßnahmen seien standardmäßig aktiviert und auf ein hohes Schutzniveau eingestellt.

[Es wird eine Folie gezeigt.]

Die Schutzmaßnahmen zielten insbesondere auf die zentralen Sorgen von Eltern und beträfen Kontakte, Inhalte und Nutzungsdauer.

[Es wird eine Folie gezeigt.]

Standardmäßig seien die Konten privat und die Interaktionsmöglichkeiten eingeschränkt. Nur Personen auf der Freundesliste könnten Markierungen vornehmen und Nachrichten senden.

[Es wird eine Folie gezeigt.]

Jugendliche erhielten zudem nur altersgerechte Inhalte. In Europa werde keine Werbung angezeigt und unerwünschte Begriffe würden herausgefiltert. Eltern könnten eigene Begriffe ergänzen und die Einstellungen anpassen.

[Es wird eine Folie gezeigt.]

Standardmäßig sei ein tägliches Zeitlimit von 60 Minuten eingerichtet. Anschließend erhielten die Jugendlichen eine Erinnerung. Zudem sei zwischen 22 Uhr und 7 Uhr ein Schlafmodus aktiviert. Eltern könnten diese Einstellungen über den Parent Account anpassen.

[Es wird eine Folie gezeigt.]

Im Rahmen der Elternaufsicht könnten Eltern die digitale Medienbildung ihrer Kinder begleiten und Einblicke in deren Aktivitäten und Kontaktaufnahmen erhalten, ohne die konkreten Inhalte einsehen zu können. Außerdem würden sie informiert, wenn ihre Kinder häufig nach bestimmten Signalwörtern suchten.

[Es wird eine Folie gezeigt.]

Inzwischen verfügten 100 Millionen Nutzerinnen und Nutzer über einen Teen-Account. 97 Prozent der 13- bis 15-Jährigen nutzten behielten auch später voreingestellten Sicherheitseinstellungen.

[Es wird eine Folie gezeigt.]

Kinder nutzten durchschnittlich 40 Apps pro Woche. Um eine wirksame Regulierung zu erreichen, müssten die Beschränkungen für sämtliche Online-Dienste gelten.

[Es wird eine Folie gezeigt.]

Zur Altersregistrierung setze Meta auf KI. Bestehe der Verdacht, dass Nutzerinnen und Nutzer jünger als angegeben seien, könnten diese Konten gemeldet werden.

[Es wird eine Folie gezeigt.]

Es müsse gemeinsam an einer nachhaltigen Lösung gearbeitet werden. Die derzeit von Meta und anderen Anbietern eingesetzten Instrumente reichten bislang nicht aus. Ein datenschutzfreundlicher und zugleich effektiver Ansatz könne darin bestehen, dass Eltern bereits bei der Einrichtung eines Handys das Alter des Kindes im App-Store oder auf Betriebssystemebene hinterlegen müssten. Beispielsweise könnten Meta-Apps für unter 13-Jährige nicht heruntergeladen werden; bei älteren Jugendlichen sei die Zustimmung eines Elternteils erforderlich.

[Es wird eine Folie gezeigt.]

Darüber hinaus habe Meta Elternguides und Social-Media-Karten entwickelt, die die Funktionen der Apps erläuterten und Eltern dabei unterstützten, mit ihren Kindern über deren Online-Erfahrungen zu sprechen.

Dr. Marco Holtz (Medienanstalt Berlin-Brandenburg – mabb –; stellvertretender Direktor und Justiziar sowie Leiter der Abteilung Zulassung und Aufsicht) teilt mit, dass die Landesmedienanstalten bereits seit vielen Jahrzehnten für den Jugendmedienschutz zuständig seien. Während sich dieser früher vor allem auf Radio und Fernsehen bezogen habe, stünden heute Telemedien und das Internet im Mittelpunkt.

Im vergangenen Jahr habe die mabb insgesamt 2 500 Inhalte gesichtet und bearbeitet. Bei 600 Inhalten seien Rechtsverstöße festgestellt worden, insbesondere in den Bereichen Volksverhetzung, Pornografie ohne ausreichenden Altersverifikationsschutz, Gewaltdarstellungen und Verstöße gegen die Menschenwürde. Zur Identifizierung von Rechtsverstößen verfüge die mabb über verschiedene Instrumente. Dazu gehöre das KI-basierte Recherchetool KIVI, das insbesondere zur Untersuchung von Internetplattformen, unter anderem bei Meta, eingesetzt werde. Die anschließende Bewertung erfolge durch Menschen. Zudem führe die mabb

gemeinsam mit anderen Medienanstalten Schwerpunktuntersuchungen, etwa zu Rechtsextremismus, durch. Bei möglichen Straftaten würden die Fälle an die Staatsanwaltschaft und die Strafverfolgungsbehörden übermittelt. Könnten die Anbieter ermittelt werden, könne die mabb als Aufsichtsbehörde eigene Verfahren einleiten und medienrechtliche Untersagungen oder Beanstandungen aussprechen. Bei Verstößen gegen den Jugendschutz seien auch Verbote von Angeboten und die Verhängung von Bußgeldern möglich. Seit Inkrafttreten des Digital Services Act – DSA – arbeite die mabb angesichts der großen Zahl von Fällen verstärkt mit den Plattformen zusammen. Sie übermittle beispielsweise Löschanregungen an Anbieter wie Meta, X und Google, den diese in der Regel nachkämen. Als letztes Mittel könne die mabb Sperrungen veranlassen. So sei beispielsweise gegen die Pornoplattformen HardPorn und YouPorn vorgegangen worden. Die betroffenen Angebote würden jedoch immer wieder auf Umgehungsmöglichkeiten wie sogenannte Mirror-Domains zurückgreifen. Aktuell liefen Gespräche mit der Rundfunkkommission darüber, wie die Regelungen verbessert werden könnten, damit bei Jugendschutzverstößen nicht jedes Mal wieder bei null angefangen werden müsse. Die mabb kooperiere zudem mit dem Bundeskriminalamt und erhalte vor dort unter anderem Löschanregungen. Diese würden an die Plattformen weitergeleitet oder zum Anlass für eigene Verfahren genommen.

Eine aktuelle Herausforderung seien KI-Chatbots. Hier sei bislang ungeklärt, wer für problematische KI-generierte Inhalte hafte, etwa wenn ein Jugendlicher von einem Chatbot eine Anleitung zum Suizid erhalte. Während im Urheberrecht bereits erste Gerichtsentscheidungen vorlägen, seien entsprechende Fragen im Medienrecht noch offen. Die Rundfunkkommission prüfe daher, ob im nächsten Medienstaatsvertrag ein eigenes Regelwerk für KI-Anwendungen geschaffen werden solle.

Einen weiteren Schwerpunkt setze die mabb auf Förderprogramme zur Information- und Nachrichtenkompetenz, um Menschen jeden Alters einen sicheren und kompetenten Umgang mit sozialen Medien zu vermitteln.

Marc Vallendar (AfD) bekräftigt, dass sich Kinder und Jugendliche viele Stunden auf Plattformen bewegten, deren Geschäftsmodelle auf eine möglichst lange Verweildauer ausgerichtet seien. Für die Plattformregulierung sei jedoch nicht das Land Berlin, sondern die EU zuständig; der Jugendmedienschutz werde dagegen über den Jugendmedienschutz-Staatsvertrag geregelt.

Pauschale Verbote für Minderjährige seien aus Sicht seiner Fraktion nicht zielführend, da sie technisch nicht umsetzbar seien, ein falsches Sicherheitsgefühl vermitteln und oftmals die Falschen trafen. Die EU Digital Identity Wallet – EUDI-Wallet – als Instrument zur Altersverifikation sei als Dammbuch zu bezeichnen. Eine zentrale staatliche Identitätsprüfung bei jedem Plattformzugang könne eine Infrastruktur für Internetabschaltungen und politischen Filterungen schaffen. Eine solche Entwicklung sei weder erforderlich noch gewünscht. Sinnvoller seien eine konsequente Anwendung des DSA, sichere Standardeinstellungen für Jugendkonten ohne manipulative Designmuster, mehr Algorithmentransparenz und praktikable Risikoanalysen. Zudem solle Medienkompetenz als Schulfach eingeführt werden.

An Elina Eickstädt richte er die Frage, weshalb Social-Media-Verbote für Minderjährige aus Sicht des Chaos Computer Clubs den Jugendschutz schwächten. – Da die EUDI-Wallet von Teilen der Koalition als mögliche Lösung zur Altersverifikation betrachtet werde: Welche

technischen und grundrechtlichen Risiken bestünden bei einer staatlich zentralisierten Identifikationsprüfung bei jedem Plattformzugang? – An welchen Stellen könne die Politik konkret nachsteuern, sodass Kinder und Jugendliche statt durch Verbote und Identifikationspflichten allein durch einen stärkeren Datenschutz vor toxischen Inhalten geschützt werden könnten?

An Dr. Marco Holtz richte er die Frage, wie häufig die mabb in den vergangenen zwölf Monaten ihre Befugnissen gegenüber Plattformen wie Instagram, X und TikTok genutzt habe und wie viele Bußgelder insgesamt sowie insbesondere gegen diese Plattformen verhängt worden seien. – Gebe es Lücken im Rechtsrahmen aus DSA, Jugendmedienschutz-Staatsvertrag und Jugendschutzgesetz, und, falls ja, welche dieser Lücken könnten mit den vorhandenen Instrumenten bereits geschlossen werden?

An Dr. Laura Hirvi richte er Fragen zu den Teen-Konten. Wie könnten jüngere Kinder unter 13 Jahren geschützt werden? Nutzten diese ebenfalls Teen-Konten? Seien Teen-Konten automatisch mit Elternaccounts verknüpft, oder funktionierten sie auch ohne elterliche Kontrolle? – Welche Haltung habe Meta zu staatlich verpflichtenden Altersverifikationssystemen wie der geplanten EUDI-Wallet als Voraussetzung für den Zugang zu Plattformen in Europa? Welche Risiken seien damit verbunden?

Gollaleh Ahmadi (GRÜNE) macht darauf aufmerksam, dass der Jugendmedienschutz nicht nur in diesem Ausschuss, sondern auch im Ausschuss für Bundes- und Europaangelegenheiten, Medien behandelt werde. Beide Aspekte müssten zusammen betrachtet werden.

Sie begrüße grundsätzlich die Einführung der Teen-Konten, jedoch hänge deren Wirksamkeit stark von der Medienkompetenz der Eltern ab. Die größten Defizite lägen nicht bei Kindern und Jugendlichen, sondern bei Erwachsenen. Während sogenannten Digital Natives mit Computern und sozialen Medien aufwüchsen, seien manche Erwachsene im selben Haushalt bereits mit der Installation von Apps oder der Kontrolle von Datenschutzeinstellungen überfordert.

Die mabb habe einen Jugendrat eingerichtet, der vom Medienausschuss zum Thema Jugendschutz eingeladen worden sei. Dieser habe vor etwa einem Jahr in einem Impulspapier gefordert, Medienkompetenz fächerübergreifend in der Schule zu vermitteln. Inwieweit habe sich der Senat mit diesen Forderungen auseinandergesetzt? Sei geplant, Medienkompetenzbildung – zunächst vor allem für Lehrkräfte – in den Schulen zu verankern?

An den Chaos Computer Club richtet sie die Frage, wie hoch das Sicherheitsrisiko einer Identifikationspflicht einzuschätzen sei, wenn Plattformen wie Meta große Mengen an Identifikationsdaten von Kindern und Jugendlichen erhielten und diese möglicherweise in die Hände Krimineller gelangen könnten.

Vor wenigen Wochen habe die Europäische Kommission einen Bericht veröffentlicht, wonach insbesondere Meta bei der Altersüberprüfung gegen Vorgaben des DSA verstoße. Im DSA seien alle notwendigen Maßnahmen bereits geregelt. Entscheidend sei deren Umsetzung sowie gegebenenfalls die Verhängung von Sanktionen. Beabsichtige Meta infolge des Berichts seine Maßnahmen anzupassen?

Wie werde sich der Senat auf Bundesebene für eine Verschärfung der Sanktionen bei Verstößen gegen den DSA einsetzen?

Jan Lehmann (SPD) fragt Frau Dr. Hirvi, wie Meta überprüfe, ob tatsächlich die richtigen Eltern angegeben würden. Wie werde mit den erhobenen Daten umgegangen? Erhielten die Eltern Werbung, und wie könne Meta mit den Teen-Konten ansonsten Geld verdienen?

An Frau Meike Kamp (BlnBDI) richte er die Frage, ob es aus datenschutzrechtlicher Sicht problematisch sei, dass Eltern auf Daten ihrer Kinder, insbesondere der über 14-Jährigen, zugreifen könnten.

Wie viele Kinder und Jugendliche mit Teen-Konten wechselten von Meta zu anderen Plattformen?

Allen Anzuhörenden stelle er die Frage, ob die vor einem Jahr in Australien eingeführten Regelungen zum Schutz Minderjähriger in sozialen Medien sachgerecht und ausreichend seien. Welches sei das größte Defizit heutiger Social-Media-Nutzerinnen und -Nutzer, das durch einen entsprechenden Bildungsauftrag aufgearbeitet werden müsse?

Elke Breitenbach (LINKE) zeigt sich erstaunt, dass die Themen Aufklärung, Information, Nutzungsverhalten und Ermächtigung nur kurz behandelt worden seien. Welchen Stellenwert hätten diese Aspekte? – Eltern trügen grundsätzlich eine Verantwortung und sollten über die Aktivitäten ihrer Kinder informiert sei. Die Ausgestaltung der Teen-Konten empfinde sie jedoch als übergriffig, denn auch Jugendliche hätten einen Anspruch auf Privatsphäre. Stattdessen sollten Kinder und Jugendliche über die Folgen ihres Handelns sowie über Datenschutzbestimmungen aufgeklärt werden.

Es stehe außer Frage, dass Lehrkörper über digitale Kompetenzen verfügen müssten. Anstatt neue Angebote aufzubauen, sei es jedoch sinnvoller, bestehende Kooperationen auszubauen. Gebe es in diesem Zusammenhang die Initiative „Chaos macht Schule“ noch, und falls ja, wie stark werde diese in Berlin genutzt? Auch die Behörde für Datenschutz und Informationsfreiheit biete entsprechende Seminare an.

Kinder und Jugendliche sollten frühzeitig so qualifiziert und befähigt werden, dass sie selbst über das notwendige Wissen und die Kontrolle über ihr digitales Leben verfügten. Die Einrichtung eines Elternaccount bei den Teen-Konten setze Zeit und Medienkompetenz voraus. Eltern müssten daher entsprechend qualifiziert werden, damit sie nicht nur eine Kontrollfunktion wahrnähmen, sondern ihre Kinder auch unterstützen und beraten könnten.

Über welche Kompetenzen verfüge das Land Berlin bei Datenschutzbestimmungen und deren Durchsetzung, um Kinder und Jugendlichen entsprechend zu schützen?

Dr. Matthias Kollatz (SPD) erklärt, dass die Ausrichtung der Plattformen auf eine möglichst lange Verweildauer zwei Seiten habe; einerseits diene sie dem Geschäftsinteresse der Anbieter, möglichst viel Werbung platzieren zu können, andererseits erhöhe sich dadurch die Gefahr eines suchtartigen Nutzungsverhaltens. Die Verbotsdebatte in Australien speise sich insbesondere aus der Diskussion über die Suchtgefahr. Zu diesem Aspekt hätten sich die Anzuhörenden bislang nur wenig geäußert. Auch in anderen Bereichen, in denen eine Suchtgefahr

vermutet werde, werde häufig mit Verboten reagiert. Beispielsweise würden Rauchverbote ebenfalls wesentlich mit dem Suchtpotenzial begründet. Wie schätzten die Anzuhörenden diese Argumentationsweise ein?

Christopher Förster (CDU) fragt, wie die Plattformbetreiber das Alter von Kindern und Jugendlichen überprüfen und sicherstellen würden. Beispielsweise würden Leihroller trotz entsprechender Altersbeschränkungen von Minderjährigen genutzt, und es sei zweifelhaft, dass die Altersvorgaben digitaler Plattformen zuverlässig eingehalten würden. Wie verhinderten die Plattformen Täuschungsversuche von Jugendlichen? Würden beispielsweise Eltern aufgefordert, Ausweisdokumente zur Altersverifikation hochzuladen?

Welche Möglichkeiten habe die Datenschutzbeauftragte – mit Blick auf mögliche Datenschutzvorfälle –, wenn beispielsweise das Handy eines Jugendlichen gehackt werde? Könnten in einem solchen Fall Datenlöschungen angeordnet oder Nutzerkonten gesperrt werden, oder liege die Verantwortung hierfür bei den Plattformbetreibern?

Befürworteten die Anzuhörenden den von Australien eingeschlagenen Weg? Sei dieser auch für Deutschland sinnvoll, oder sei das Verbot leicht zu umgehen und die Wirkung daher letztendlich nur kurzfristig?

Dr. Marco Holtz (mabb) erläutert, die Zahl der Rechtsverstöße habe er bereits genannt, die Zahl der Löschanregungen liege im mittleren dreistelligen Bereich. Bußgelder würden in der Regel nicht gegen die Plattformen selbst, sondern gegen die Anbieter verhängt, etwa bei wiederholten Verstößen gegen den Jugendschutz, gegen Kennzeichnungspflichten für Werbung oder bei Missachtung der Verpflichtung zur Bestellung eines Jugendschutzbeauftragten.

Der Jugendrat habe ein Impulspapier zum Thema Social-Media-Verbot erarbeitet, das voraussichtlich im Juni veröffentlicht werde. Der Jugendrat betrachte das Thema differenziert und vertrete die Auffassung, dass vor möglichen Verbote zunächst die bestehenden Regeln konsequent umgesetzt werden sollten. Diese Position werde von der mabb geteilt.

Auf europäischer und nationaler Ebene gebe es bereits zahlreiche Regelungen zum Jugendschutz. Deren Durchsetzung sei insbesondere gegenüber ausländischen Anbietern derzeit noch schwierig. Die Aussage, dass die Bundesländer für die Plattformregulierung nicht zuständig sei, treffe nicht zu. Der Medienstaatsvertrag enthalte Regelungen zur Plattformregulierung, die derzeit allerdings durch den Digital Services Act überlagert würden. Dadurch sei es schwierig, die genaue Abgrenzung zwischen DSA, nationalem Recht und Herkunftslandprinzip vorzunehmen. Das Verwaltungsgericht sowie Spotify und andere sprächen der mabb ihre Zuständigkeit ab und sähen diese auf europäischer Ebene. Die Richtigkeit dieser Einschätzung sei schwer zu überprüfen. Beispielsweise sei die Vielfaltssicherung ein nationales Thema und falle seit jeher in die Zuständigkeit der Bundesländer.

Zur Frage der Abgeordneten Breitenbach zur Förderung von Informations- und Nachrichtenkompetenz: Die mabb habe bereits 2019 das Medienbildungsprojekt „Journalismus macht Schule“ gestartet. Dabei gingen Journalistinnen und Journalisten in die Schulen und vermittelten dort, wie journalistisch-redaktionelle Inhalte erkannt und von Fake News unterschieden werden könnten. Zudem gebe es den Desinfopoint, der ebenfalls dazu beitrage, Falschinformationen zu erkennen. Dieses mobile, aufsuchende Angebot zur Förderung der Medienkom-

petenz biete die mabb in ganz Berlin und Brandenburg an. Zudem habe die mabb im März 2026 das Onlineportal „jewusst wie“ gestartet, um Workshops, Veranstaltungen und Informationen zum Thema Nachrichtenkompetenz zu bündeln und leichter auffindbar zu machen.

Dr. Laura Hirvi (Meta) erklärt, Meta setze bereits seit Beginn KI zur Überprüfung der Altersangaben ein und werde diese künftig weiter ausbauen. Mithilfe von KI werde auch der Content überprüft und gegebenenfalls bereits vor der Veröffentlichung gelöscht, um die Sicherheit von unter 13-Jährigen zu gewährleisten. Bestehe der Verdacht, dass Nutzerinnen oder Nutzer jünger als 13 Jahre seien, werde der Account zunächst blockiert und die betreffende Person benachrichtigt. Diese habe dann die Möglichkeit, ihr Alter nachzuweisen; andernfalls werde der Account automatisch gelöscht. Die KI könne inzwischen auch erkennen, ob das angegebene Alter mit dem hochgeladenen Foto übereinstimme. Meta arbeite zudem in verschiedenen Gremien mit Eltern zusammen, um die Teen-Accounts fortlaufend weiterzuentwickeln.

In den vergangenen Monaten seien zwei Gutachten zu den Fragen erstellt worden, wer für den Jugendschutz im Onlinebereich zuständig sei und welche gesetzliche Regelungen dort griffen. Die Gutachten seien zu sehr unterschiedlichen Ergebnissen gekommen. Gleichzeitig liefen auf EU-Ebene neue Gesetzgebungsvorhaben, insbesondere im Zusammenhang mit dem DSA, wodurch sich die Frage nach den jeweils geltenden regulatorischen Rahmenbedingungen stelle. Die entsprechenden Regelungen sollten auf europäischer Ebene beschlossen werden. Da die europäische Jugend miteinander vernetzt sei, sollten beispielsweise europaweit einheitliche Altersbestimmungen gelten. Zudem fordere der Elternrat, in die Gestaltung einbezogen zu werden. Meta verfolge auch eigene Ansätze zur technischen Umsetzung, diese müssten jedoch ebenfalls aus regulatorischer Sicht betrachtet werden.

Meta stehe der EUDI-Wallet grundsätzlich offen gegenüber, sofern diese für Eltern und Jugendliche eine einfache und effiziente Lösung darstelle. Es müsse jedoch verhindert werden, dass Eltern sich täglich mit dem Thema auseinandersetzen und ihre eigene Medienkompetenz fortlaufend erweitern müssten. Außerdem solle vermieden werden, dass für jede App ein anderes Tool zur Altersverifizierung erforderlich sei.

Instagram biete bereits zahlreiche Funktionen an, beispielsweise zum Blockieren von Personen und zur individuellen Gestaltung des Algorithmus. Dafür sei jedoch eine entsprechende Medienkompetenz erforderlich. Die Teen-Accounts verfügten deshalb bereits über zahlreiche Voreinstellungen für Jugendliche zwischen 13 und 16 Jahren. Ab 16 Jahren könnten Jugendliche die Einstellungen selbstständig ändern.

Die Nutzung von sozialen Medien könne nicht mit dem Konsum von Zigaretten oder Alkohol verglichen werden. Viele Plattformen böten auch Informationsmöglichkeiten; so könnten Jugendliche beispielsweise die Inhalte der Tagesschau auf Instagram abrufen. Die Debatte über Social Media beschränke sich häufig auf die Gefahren und verliere dabei die positiven Möglichkeiten aus dem Blick.

Die Altersverifizierung und die Identifizierung eines Elternteils ließen sich am einfachsten und effektivsten bei der erstmaligen Einrichtung des Handys eines Kindes sicherstellen. Das Elternteil, das einen Account einrichte, um die Schutzeinstellungen des Teen-Accounts zu überprüfen und festzulegen, müsse selbst nicht aktiv auf der entsprechenden Plattform sein.

Dass 97 Prozent der Nutzerinnen und Nutzer die Einstellungen auch als Erwachsene beibehielten, sehe Meta positiv. Wenn Meta-Plattformen von Jugendliche positiv wahrgenommen würden, blieben die Nutzerinnen und Nutzer dort. Ein Wechsel zu anderen Plattformen werde im Gegenzug in Kauf genommen.

In Australien gelte eine strenge Altersverifizierung bislang nur für einige Apps. Jugendliche seien daraufhin teilweise auf andere Apps ausgewichen. Um den Jugendschutz im Onlinebereich nachhaltig zu regulieren, sollten daher nicht nur einzelne große Betreiber, sondern der gesamte digitale Bereich, in dem sich Jugendliche bewegten, berücksichtigt werden, beispielsweise auch der Gaming-Bereich.

Jugendliche hätten ein Recht auf digitale Teilhabe. Um Eltern bei der Entwicklung ihre Medienkompetenz zu unterstützen, stelle Meta analoge und digitale Instrumente zur Verfügung. So würden beispielsweise häufige Frage in einem Onlineguide gebündelt und jeweils für Eltern und Jugendliche aufbereitet.

Auf einem Kongress von Jugendpsychologen in Würzburg vor zwei Wochen sei die Suchtgefahr durch soziale Medien diskutiert worden. Eine renommierte Wissenschaftlerin habe dort erklärt, dass die Studienlage bei Jugendlichen, die nicht bereits zuvor ein Suchtpotenzial aufgewiesen hätten, nicht eindeutig sei. Ob soziale Medien eher als Verstärker oder Auslöser wirkten, sei weiterhin offen. Bislang habe die Wissenschaft keine eindeutigen Belege für negative gesundheitliche Auswirkungen der Sozial-Media-Nutzung bei Jugendlichen aus einem unproblematischen Umfeld gefunden.

Elina Eickstädt (CCC) erklärt, Grundvoraussetzung für die Durchsetzung eines Social-Media-Verbots sei ein Altersnachweis für sämtliche Nutzerinnen und Nutzer. Zudem müssten die Plattformen anhand von IP-Adressen oder anderen Geolocation-Daten feststellen, welchem Rechtsrahmen die Nutzerinnen und Nutzer unterlägen, um die entsprechenden Regelungen anzuwenden.

Für den Altersnachweis stünden verschiedene Verfahren zur Verfügung, etwa über Ausweisdokumente mittels KYC-Verfahren wie POSTIDENT oder VideoIdent, durch das Hochladen einer Ausweiskopie oder künftig über die EUDI-Wallet beziehungsweise das Auslesen der maschinenlesbaren Zone des Personalausweises. Die Verfahren setzten vorhandene Ausweisdokumente voraus und seien hinsichtlich Datensparsamkeit unterschiedlich zu bewerten. Das Hochladen des Personalausweises berge Risiken hinsichtlich eines möglichen Identitätsdiebstahls. Die EUDI-Wallet setze ein geeignetes Handy sowie die entsprechende PIN voraus. Besondere Schwierigkeiten könnten in Haushalten entstehen, in denen dasselbe Handy von mehreren Personen genutzt werde. Eine Altersschätzung mittels KI sei nicht zuverlässig; auch das Einlesen biometrischer Daten sei aus Datenschutzsicht fragwürdig. In Australien werde von den Nutzerinnen und Nutzern ein Verhaltensprofil erstellt und ausgewertet. Das stehe im Widerspruch zu der Forderung, dass die Daten von Kindern und Jugendlichen besonders geschützt werden müssten.

Insgesamt sei festzustellen, dass die verschiedenen Verfahren zum Altersnachweis ohnehin benachteiligte Personen zusätzlich benachteiligten. Wer die Verfahren nicht nutzen könne oder wolle, sei faktisch vom digitalen Raum ausgeschlossen. Die EU-Kommission habe in den vergangenen Wochen eine entsprechende Lösung vorgestellt, die allerdings nur auf iOS-

und Android-Geräten funktioniere. Die Altersverifikation könne außerdem durch das Verschleiern der IP-Adresse und die Angabe eines anderen Rechtsraums umgangen werden. Studien in Australien hätten zudem gezeigt, dass etwa ein Drittel der Eltern die Social-Media-Nutzung befürworte und ihre Kinder bei der Umgehung der Altersverifizierung unterstütze.

Bei der EUDI-Wallet würden künftig sogenannte Zero-Knowledge-Proofs zum Einsatz kommen, die sich derzeit in der Standardisierung befänden. Bei den entsprechenden Standardisierungsvorschlägen sei Google federführend. Sollten sich diese Standards durchsetzen, könne daraus eine Abhängigkeit des Personalausweissystems von Google entstehen. Auch die EUDI-Wallet berge datenschutzrechtliche Risiken. Studien hätten ferner gezeigt, dass sich Desinformationen nicht nur über Bots, sondern auch über gehackte Accounts oder gekaufte Likes und Reposts verbreiteten. Eine Identifizierungspflicht werde daran nichts ändern und könne das Problem unter Umständen sogar verschärfen.

Eltern seien teilweise selbst von problematischer Social-Media-Nutzung betroffen und verfügten nicht immer über einen guten Umgang mit sozialen Medien. Die Teen-Accounts seien grundsätzlich zu begrüßen; gleichzeitig solle darüber nachgedacht werden, wie soziale Medien für alle Altersgruppen besser gestaltet und durch geeignete Voreinstellungen sicherer gemacht werden könnten.

Aktuell hätten die Verhandlungen zum Digital Fairness Act begonnen. Laut Corporate Europe Observatory entfielen 93 Prozent der Lobbygespräche auf die Digitalisierungsindustrie und weniger als 13 Prozent auf die Zivilgesellschaft. Letztere gerate im Zusammenhang mit Plattformregulierung – Stichwort HateAid – zunehmend unter Druck. Sie appelliere an die Bundesregierung, angesichts dieser Einschränkungen den Digital Services Act weiterhin nachdrücklich zu unterstützen.

Das Projekt „Chaos macht Schule“ sei ein Alleinstellungsmerkmal des Chaos Computer Clubs und werde sporadisch in einigen sogenannten Erfahrungsaustauschkreisen angeboten. Sie sei außerdem im Vorstand der Open Knowledge Foundation Deutschland, die das Förderprogramm „Jugend hackt“ ins Leben gerufen habe. Kinder und Jugendliche sollten nicht nur zu bewussten und handlungsfähigen Nutzerinnen und Nutzern befähigt werden, sondern auch Freiräume für neues Denken erhalten. So sei 2025 die Konferenz „Beyond Code“ veranstaltet worden, bei der digitalpolitische Themen diskutiert und positive Zukunftsvisionen für den digitalen Raum entwickelt worden seien.

Staatssekretär Matthias Hundt (Skzl) weist darauf hin, dass eine digitale Welt auch eine digitale Identität erfordere. Die EUDI-Wallet sei bei der Altersabfrage eine gute Alternative zum Hochladen von Ausweisdokumenten. Angesichts von inzwischen rund 180 Anbietern, die die EUDI-Wallet unterstützten, sei die digitale Brieftasche, die ab 1. Januar 2027 zur Verfügung stehen solle, aus Sicht des Senats sowohl für den öffentlichen als auch den privaten Bereich ein gutes Produkt.

Die Senatskanzlei stehe derzeit mit der SenBJF zum Thema Jugendschutz und Bildung im Austausch, um weitere Projekte für Schülerinnen und Schüler anbieten zu können.

Die Zuständigkeiten bei Verstößen im Internet seien teilweise nicht eindeutig geregelt. Die Senatskanzlei arbeite hierzu mit der mabb zusammen und stehe darüber hinaus mit den zu-

ständigen Landes-, Bundes- und europäischen Behörden im kontinuierlichen Austausch, um Maßnahmen besser zu koordinieren und Themen frühzeitig zu erkennen.

Meike Kamp (Berliner Beauftragte für Datenschutz und Informationsfreiheit) unterstreicht, dass Altersverifikationssysteme erhebliche Herausforderungen hinsichtlich Datenschutz, Umgehungsmöglichkeiten und Zuverlässigkeit der Verfahren mit sich brächten. Die EU-Kommission habe Leitlinien zu Artikel 28 des Digital Services Act zum Schutz Minderjähriger entwickelt, in denen typische Risiken für Kinder im Internet systematisiert würden. Diese beträfen jedoch grundsätzlich alle Nutzerinnen und Nutzer von Plattformen, insbesondere im Hinblick auf Wohlergehen, Gesundheitsschutz und Datenschutz. Risiken entstünden beispielsweise durch personalisierte Werbung und algorithmengesteuerte Empfehlungssysteme.

Im Mittelpunkt der Debatte stünden die von Drittnutzern veröffentlichten Inhalte und die Frage, mit welchen Inhalten Kinder und Jugendliche konfrontiert würden. Aus datenschutzrechtlicher Sicht müssten jedoch auch die Plattformen selbst als potenzielle Angreifer betrachtet werden. Offen sei insbesondere, was mit den Daten Minderjähriger geschehe. Selbst bei Einhaltung der Altersbeschränkungen erzeugten deren Aktivitäten auf den Plattformen weiterhin Daten. Zwar dürften Minderjährige gemäß Artikel 28 keine personalisierte Werbung erhalten, dennoch seien Profiling und das Zusammenführen von Informationen über verschiedene Dienste hinweg möglich. Zudem sei unklar, ob mit den Daten Minderjähriger grundsätzlich anders umgegangen werde.

Die französische Datenschutzbehörde habe mit „FantomApp“ eine Anwendung entwickelt, mit der Eltern und Kinder gezielt nach datenschutzfreundlichen Einstellungen für Plattformen suchen könnten. Die Berliner Datenschutzbehörde arbeite derzeit an einer deutschen Übersetzung. Die Plattformen hätten entsprechende Anwendungen bereits früher entwickeln und unterstützen sollen. Die heutigen Teen-Konten seien auch eine Folge hoher Bußgelder, die die irische Datenschutzbehörde 2020 gegen Meta verhängt habe. Hintergrund sei gewesen, dass Teen-Konten standardmäßig auf „public“ eingestellt und dadurch unter anderem Telefonnummern und E-Mail-Adressen einsehbar gewesen seien. Die Plattformen müssten somit auf die europäischen Regulierungen reagieren.

Belastbare Studien zum Social-Media-Nutzungsverhalten gebe es bislang nur in begrenztem Umfang, da der Zugang zu entsprechenden Daten bisher stark eingeschränkt gewesen sei. Auch dieser Bereich sei durch den Digital Services Act reguliert worden. Künftig seien Plattformen verpflichtet, Daten zu Forschungszwecken bereitzustellen.

Nach Artikel 8 der Datenschutzgrundverordnung liege das Alter für eine datenschutzrechtliche Einwilligung bei Diensten der Informationsgesellschaft grundsätzlich bei 16 Jahren. Bei unter 16-Jährigen sei daher in der Regel die Einwilligung der Eltern erforderlich. Voraussichtlich werde diese Altersgrenze auch für die entsprechenden Verfahren der Plattformen maßgeblich sein. Gleichzeitig berücksichtige die Datenschutzgrundverordnung das bilaterale Verhältnis zwischen Eltern und Kindern im Hinblick auf personenbezogene Daten und Datenschutz nicht ausdrücklich, da dieses als persönliche familiäre Angelegenheit gelte. Relevant werde dies insbesondere in Fällen, in denen das Verhältnis zwischen Kindern und Erwachsenen belastet sei. Eine rechtliche Unsicherheit bestehe zudem bei der Frage, bis zu welchem Alter Eltern im Rahmen einer von ihnen vorgenommenen Altersverifizierung auf die Daten ihrer Kinder zugreifen und diese kontrollieren sollten.

Hinsichtlich der Zuständigkeiten gelte in Europa nach der Datenschutzgrundverordnung grundsätzlich das sogenannte One-Stop-Shop-Verfahren. Da zahlreiche große Plattformen ihren europäischen Hauptsitz in Dublin hätten, sei die irische Datenschutzbehörde für deren datenschutzrechtliche Aufsicht und die Bearbeitung entsprechender Beschwerden zuständig. Gleichzeitig sei vereinbart worden, dass bestimmte Beschwerden auch von den jeweiligen nationalen oder lokalen Aufsichtsbehörden bearbeitet werden könnten. Berlin habe beispielsweise mit der hier ansässigen Plattform TikTok gute Erfahrungen bei der Umsetzung von Löschungsfordernungen in Vorverfahren gemacht. Größere datenschutzrechtliche Anliegen würden jedoch weiterhin von der irischen Datenschutzbehörde bearbeitet.

Für den Bereich Medienpädagogik liege die Regulierungszuständigkeit beim Land Berlin. Datenschutz und Medienkompetenz könnten beispielsweise verbindlicher und flächendeckender im Rahmenlehrplan oder im Berliner Schulgesetz verankert werden. Bislang würden entsprechende Medienkompetenzkurse von verschiedenen Institutionen angeboten, darunter auch von der Datenschutzbehörde.

Vorsitzender Johannes Kraft stellt fest, dass keine weiteren Wortmeldungen vorlägen und der Tagesordnungspunkt abgeschlossen sei.

Punkt 4 der Tagesordnung

Antrag der Fraktion Bündnis 90/Die Grünen
Drucksache 19/2963
Berliner Open-Source-Gesetz

[0154](#)
DiDat

Stefan Ziller (GRÜNE) weist darauf hin, dass der vorherige Tagesordnungspunkt gezeigt habe, was geschehe, wenn die Souveränität verloren gehe und der Einfluss auf bestimmte Entwicklungen schwinde. Digitale Souveränität und Open-Source seien wiederholt Gegenstand in diesem Ausschuss gewesen, zuletzt im Zusammenhang mit der Open-Source-Strategie des Landes Berlin. Der Einsatz von Open-Source-Software ermögliche es, die Kontrolle über die eigene IT zurückzugewinnen, Abhängigkeiten von einzelnen Anbietern zu verringern und durch transparente sowie gemeinschaftlich geprüfte Quellcodes die Sicherheit zu erhöhen. Dadurch könne Berlin stärker bestimmen, wie die eigene digitale Infrastruktur gestaltet werde. Zugleich passe Open-Source zu Berlin als Standort für digitale Innovation. Berlin verfüge über eine lebendige Open-Source-Community sowie ein breites Ökosystem aus Hochschulen, Forschungseinrichtungen und Start-ups. Eine konsequente Nutzung und Förderung von Open-Source könne diese Kompetenzen stärken, Arbeitsplätze schaffen und die Berliner Tech-Branche wettbewerbsfähiger machen. Allerdings fehlten bislang der politische Wille und verbindliche Ziele für einen umfassenderen Umstieg. Dies sei bereits im Rahmen der Open-Source-Strategie diskutiert worden.

Um digitalen Souveränität verbindlich zu stärken, solle dieser politische Wille durch eine Ergänzung des E-Government-Gesetz verankert werden. Bis 2035 solle dort, wo es möglich sei, auf Open-Source umgestellt werden; begründeten Ausnahmen sollten zulässig bleiben. Für die Umsetzung stehe damit ein realistischer Zeitrahmen von neun Jahren zur Verfügung. Gleichzeitig könne ein solches Ziel den Druck auf dem Markt erhöhen, entsprechende Produkte bereitzustellen. Wünschenswert sei, dass auch der Bund und andere Bundesländer dem

Beispiel Berlins folgten – nicht nur auf der Angebotsseite, etwa durch ZenDiS, sondern auch durch verbindliche gesetzliche Ziele für mehr digitale Souveränität.

Marc Vallendar (AfD) betont, dass das grundsätzliche Anliegen des Antrags, die Berliner Verwaltung zur Nutzung von Open-Source-Software zu verpflichten und damit die digitale Souveränität des Landes Berlin zu stärken, richtig sei. Eine entsprechende Position habe die AfD-Fraktion bereits 2024 auf Bundesebene in ihrem Antrag Drucksache 20/10393 vertreten. Unterstützt werde dieses Anliegen unter anderem vom Chaos Computer Club, vom Zentrum Digitale Souveränität – ZenDiS – und von der Open Source Business Alliance.

Mehrere Punkte des Antrags seien jedoch kritisch zu bewerten. Das Zieldatum 1. Januar 2035 liege zu weit in der Zukunft. Zudem sei der Anwendungsbereich auf verfahrensübergreifende IKT beschränkt, sodass insbesondere kostenintensive Verträge etwa mit Microsoft oder SAP unberührt blieben. Auch fehle eine Kostenfolgenabschätzung. Seine Fraktion würde dem Antrag zustimmen, wenn dieser ambitionierter ausgestaltet und das Zieldatum verändert werde. Andernfalls werde sich seine Fraktion enthalten.

Jan Lehmann (SPD) stimmt zu, dass der Antrag grundsätzlich zu begrüßen sei. Allerdings sei in der Open-Source-Strategie des Senats bereits festgelegt, dass der Einsatz nicht quell-offener Software ausdrücklich begründet werden müsse und bis 2032 ein Anteil von 50 Prozent Open-Source-Software angestrebt werde. Auch das ITDZ sei in diesen Prozess eingebunden. Der Antrag sei daher nicht grundsätzlich falsch, zunächst solle jedoch abgewartet werden, welche Ergebnisse mit der Open-Source-Strategie bis 2032 erreicht würden.

Staatssekretär Matthias Hundt (Skzl) betont ebenfalls, dass die Umstellung auf Open-Source grundsätzlich unterstützt werde. Das derzeit erarbeitete Digitalgesetz sehe vor, dass vor der Anschaffung oder Einführung einer Software stets geprüft werden müsse, ob bereits eine geeignete Open-Source-Lösung vorhanden sei. Eine verbindliche Verpflichtung schränke hingegen die digitale Souveränität eher ein.

Stefan Ziller (GRÜNE) erwidert, seine Fraktion sei nicht davon überzeugt, dass der Senat ohne gesetzlich verankerte Ziele die notwendige Entwicklung vorantreiben werde. Die bisherigen Maßnahmen seien zudem nicht ausreichend unterlegt, um das Ziel eines 50-prozentigen Open-Source-Anteils bis 2032 zu erreichen. Deshalb sei im Antrag ein Zeitraum von neun Jahre vorgesehen. Ohne zusätzliche Maßnahmen werde Berlin das angestrebte Ziel bis 2035 nicht erreichen.

Wie sei der Zeitplan für das Digitalgesetz? Sei dessen Umsetzung für die laufende Legislaturperiode tatsächlich gestoppt worden, oder werde das Gesetz noch vor deren Ende eingebracht?

Vorsitzender Johannes Kraft hält fest, dass der Senat diese Frage unbeantwortet lasse.

Der **Ausschuss** beschließt, dem Plenum die Ablehnung des Antrags Drucksache 19/2963 zu empfehlen.

Punkt 5 der Tagesordnung

Verschiedenes

Siehe Beschlussprotokoll.