**** Disclaimer: Dieses Transkript ist ki-generiert und kann Fehler aufweisen****

Ich bin Anke Domscheit-Berg, digitalpolitische Sprecherin der Linken im Bundestag und wie immer berichte ich euch aus dem digitalen Maschinenraum des Bundestages, also aus dem Digitalausschuss. Wir haben heute vier verschiedene Themen. Wir hatten nämlich zum einen am 16. Mai 2024 fand das alles statt, eine Anhörung zu den nationalen Spielräumen bei der Umsetzung der KI-Verordnung der EU und wir hatten drei Themen im Digitalausschuss, nämlich einmal der super alte, nicht totzukriegende Zombie-Chatkontrolle und zusätzlich zur Chatkontrolle auch noch eine andere EU-Richtlinie zum Kinderschutz vor sexualisierter Gewalt online. Dann hatten wir das Thema Cyberangriffe auf Parteien, Regierungen, diverse Unternehmen, Verbände und Stiftungen. Vor allem ging es aber um einen Cyberangriff auf die SPD. Und ganz kurz am Ende geht es nochmal um die allererste Digitalminister-Fachkonferenz. Und damit geht es nochmal um die allererste Digitalminister-Fachkonferenz. Und damit geht es los. Die Chatkontrolle. Der drölfzigste neue Versuch, diesmal von der belgischen Ratspräsidentschaft, hier was Schreckliches durchzusetzen und die schon erwähnte niegelnagelneue Richtlinie zum Kinderschutz. Vielleicht nochmal ein kleiner Recap so am Anfang. Ganz wichtig für euch, es sind zwei völlig verschiedene europäische Gesetzesinitiativen. Das wurde von etlichen Abgeordneten im Digitalausschuss auch durcheinandergebracht. Zuerst will ich euch nochmal diese europäische Verordnung Chatkontrolle kurz erklären. Die wird in Europa ja nicht Chatkontrolle genannt, sondern CISA am Richtlinie. Und das kommt von CSA, Child Sexual Abuse. Das sagt schon, worum es geht. Das Ziel ist ja ein Heeresziel. Es geht also darum, sexualisierte Gewalt gegen Kinder zu bekämpfen.

und Kommunikationsdienste massenhaft Kommunikation zu scannen, also auch private Kommunikation, was alles, ihr so elektronisch von WhatsApp bis sonst wohin hin und her kommuniziert, das alles sollte von den jeweiligen Unternehmen durchgescannt werden und zwar selbst Ende-zu-Ende verschlüsselte Kommunikation. Das geht übrigens wenn nur, man Sicherheitslücken einbaut. Das ist also wirklich gruselig. Aber das war noch gar nicht alles. Damit verbunden waren auch Alterverifizierungspflichten, dass man also alle Nasen und überall nachweist, wie alt man ist. Netzsperren waren drin und noch ganz vieles andere. Aber ich habe hier schon öfter drüber geredet. Wer es also noch genauer wissen will, die Podcast Folgen 10 und 18 von der ADB Podcast, die ich euch unten verlinken die will, Podcastfolgen 10 und 18 von der ADB-Podcast, die ich euch unten verlinken werde, die sind da ein bisschen ausführlicher. Die Folge davon wäre, dass wir ein Briefgeheimnis in der elektronischen Kommunikation faktisch nicht mehr hätten. Gleichzeitig hätten wir aber auch Kinder gar nicht besser geschützt. Also es ist ein Lose-Lose, wenn man so will. Das hat auch ein Gutachten des Wissenschaftlichen Dienstes vom Bundestag ergeben. Das habe ich 2022 beauftragt und das war ganz glasklar. Das hat also gesagt, diese Chatkontrolle nach dem vorliegenden Entwurf der EU ist weder verhältnismäßig, ist auch nicht angemessen und komplett ungeeignet und

im Übrigen auch ein Verstoß gegen die Charta der Grundrechte der Europäischen Union. Natürlich verlinke ich euch auch dieses wissenschaftliche Dienstgutachten. Da ist völlig klar, als Linke können wir sowas nur ablehnen und zwar von Anfang bis Ende. Auch das gibt es inausführlich, nämlich am Positionspapier der Bundesarbeitsgemeinschaft Netzpolitik der Linken. Das ist ganz nagelneu vom März 2024 und gibt euch einen guten Überblick über das ganze Thema, aber auch, was wir als Linke da parlamentarisch schon so getrieben haben. Wir haben eigene Anträge gestellt. Wir haben uns in Anhörungen und Debatten geäußert. Also alles das kriegt ihr da geballt. Die Position der Bundesregierung war in diesem ganzen Thema ewig unklar. Die sind sich also mal wieder in der Ampel nicht einig geworden. Was bei den EU-Verhandlungen natürlich echt nicht gut rüberkam. Andere Länder wie Österreich haben sich da von Anfang an sehr klar und zwar dagegen positioniert. Eine gemeinsame Position hat die Ampel erst im April 2023 gefunden und hat sinngemäß erklärt, ja, also die Verordnung, die ist schon nicht so schlecht. Man will die ja eigentlich haben, aber es gäbe da so K.O.-Kriterien, die Deutschland hat für eine Zustimmung, nämlich einmal muss Ende-zu-Ende verschlüsselte Kommunikation geschützt sein und es darf kein Client-Side-Scanning geben.

dass man es da schon mal mitliest. Auch dazu muss man Sicherheitslücken einbauen, und zwar auf jedem Handy oder auf jedem anderen Endgerät. Und das will natürlich keiner, das wäre auch ein absolutes Desaster. Im Klartext heißt aber auch, diese beiden K.O.-Kriterien als einzige zu nennen, dass die Bundesregierung völlig fein damit ist, massenhafte private Kommunikation zu scannen, zum Beispiel auf den Servern oder in irgendwelchen Clouds, also wenn sie zum Beispiel nicht verschlüsselt sind, was immer noch bei ganz vielen Kommunikationen der Fall ist. Für meine Interpretation wäre das ein Bruch des Koalitionsvertrags, aber naja, wäre nicht der erste und auch nicht der einzige. Aber Stand heute sind die Mitgliedstaaten der EU immer noch uneinig. Netzpolitik.org hat mal so eine kleine Übersichtslandkarte erstellt, wie sich die jeweiligen Länder da positionieren. Das ist noch nicht so alt, hat den Stand Dezember 23 verlinkt in den Shownotes. gab es plötzlich neue Dynamiken. Es gab die neue belgische Ratspräsidentschaft, die hat noch ein paar neue Kompromissvorschläge sich ausgedacht. Aber ehrlich alles sind weiter gerottig, gesagt, alle sind schlimm und wahrscheinlich deshalb gibt es immer noch keine Einigung in der Europäischen Union. Die Bundesregierung, die hat aber auch laut einem Netzpolitikbericht vom März 2024 intern in der EU erklärt, dass sie ihre eigene Position zur Chatkontrolle updatet. Und da fragt man sich ja als aufmerksame Bürgerin schon, was zum Kuckuck wollen die da updaten? Mein persönliches Bauchgefühl sagt, es wird nicht zum Besseren. Also wer weiß, wir warten darauf. Das ist also so grob gefasst die Ausgangslage für unsere Ausschussbefassung. Dann hatten wir aber noch diese zweite Richtlinie, komplett unabhängig von der Chatkontrolle, eine nagelneue Richtlinie zum Schutz von Kindern vor sexualisierter Gewalt. Da gab es den erstmaligen Gesetzentwurf der Europäischen Kommission erst gerade im März, verlinke ich euch auch unten, aber es ist schon eine Novellierung einer sehr viel älteren Richtlinie, es ist nicht so, als hätte die gar keine Vorgeschichte gehabt und sie kurz ist, gesagt, sehr einer sehr viel älteren Richtlinie. Es ist nicht als hätte so, die gar keine

Vorgeschichte gehabt. Und sie ist kurz gesagt sehr, sehr viel sinnvoller als die Chatkontrolle-Verordnung. Die hat also mit Massenüberwachung erstmal nix am Hut. Da geht's um folgende Inhalte. Einmal sollen KI-generierte Darstellungen und Deepfakes explizit als Missbrauch benannt werden. Das ist in Deutschland auch noch eine rechtliche Grauzone. Da fehlt also eine eindeutige Rechtsprechung. Und wenn das von Europa eindeutig benannt werden würde, würde das natürlich eine eindeutige Rechtsprechung erleichtern. Dann soll es gezieltere Maßnahmen geben gegen sogenannte Livestream-Exploitation. Das ist eine wirklich widerliche Geschichte. Also viele Täter, ja meistens sind es Männer, die in westlichen Ländern sitzen, die bezahlen dann so einen Livestream. Die schicken dann so 100 Euro per PayPal irgendwo hin und in armen Ländern, wo man auf solche Einnahmen existenziell angewiesen ist, wird dann halt eine Tochter oder ein Sohn quasi geopfert, um das zu tun, was die westlichen Typen da so gerne sehen wollen online. Viele dieser gequälten Kinder befinden sich zum Beispiel in den Philippinen und da wird echt viel zu wenig dagegen gemacht. Da haben wir als westliche Länder eine Verantwortung gegenüber denen, die da ausgebeutet werden und das soll auch diese Richtlinie ermöglichen. Zum Beispiel gibt es da den Vorschlag, den ich persönlich befürworte, mit den Finanzdienstleistern besser zusammenzuarbeiten. Die Bezahlmuster für solche ausbeuterischen Verhältnisse und Gewaltverhältnisse, die sind nämlich sehr typisch. Das sind meistens kleine Zahlungen, die immer an die gleichen Adressaten gehen und da kann man schon Verdachtsfälle bekommen, die man dann sich genauer angucken kann. Verdachtsfälle

Ist nicht viel anders als was Finanzdienstleister das, heute schon bei Geldwäscheverdacht oder Terrorverdacht überprüfen müssen. Die hätten dann halt einen vor allem besonders sinnvollen Zweck mehr. Außerdem soll es mehr verdeckte Ermittlungsmöglichkeiten der Polizei im Netz geben. Für diesen Zweck finde ich das auch in Ordnung. Da werden ausdrücklich Honeypots erlaubt. Also Fallen auslegen sozusagen, die dann andere reintappen. Das ist schon sinnvoll. Also gerade wenn man gezielt und im Darknet ermitteln möchte, dann ist das in Ordnung. Ich persönlich gehe davon aus, dass man Deepfake-Material dafür für zulässig erklärt. Und natürlich kein echtes Material. Das fände ich völlig inakzeptabel. Denn ganz oft muss man in solchen Honeypots irgendwelches Material bereitstellen. Und solange das Dieb gefakt ist, könnte ich damit noch leben, falls man auf diese Weise echten Tätern auf die Spur kommt. Ganz wichtige Änderung wäre auch noch, was in dieser Richtlinie drinsteht, also es ist ja nur ein Entwurf im Moment, eine kindergerechtere Justiz zu ermöglichen. Das betrifft also kindgerechte Meldewege, aber auch Strafverfahren, die auf Kinder und ihre Belange viel mehr Rücksicht nehmen und zum Beispiel auch eine soziale Betreuung von Opfern während solcher Verfahren. Die sollen ja nicht ein zweites und ein drittes Mal gequält werden, sondern man soll das angemessen machen. Und auch überfällig, man könnte sagen, ist ja nur ein Wort, aber Wörter mettern. Insofern für mich ist es nicht nur ein Wort. Diese Richtlinie sagt auch, den Begriff Kinderpornografie benutzen wir nicht mehr. Er soll ersetzt werden durch den Begriff Darstellung sexuellen Missbrauchs von Kindern. Ich persönlich denke, man hätte noch einen Schritt weiter gehen können. Denn Missbrauch, mindestens im

Deutschen, funktioniert halt auch nicht. Bei Abuse ist es genau das Gleiche, da ist Use drin. Man kann Kinder nicht rechtmäßig gebrauchen. Insofern finde ich, die einzig wirklich korrekte Bezeichnung ist Darstellung von sexualisierter Gewalt gegen Kinder. Das ist es jetzt nicht geworden, aber immerhin werden wir diesen leidigen Begriff Kinderpornografie damit los. Es gibt noch ein paar mehr Änderungen, die sinnvoll sind in dieser Richtlinie, nämlich die ausdrückliche Erlaubnis, einvernehmliche sexuelle Handlungen von Minderjährigen, also untereinander, ohne dass Erwachsene daran beteiligt sind, nicht als Straftat einzustufen. Das ist nämlich logischerweise keine sexualisierte Gewalt, wenn, weiß ich, zwei 16-Jährige miteinander Dinge tun. Und das korrigiert bisher eine in diversen Ländern, übrigens auch bei uns, viel zu weitgehende Auslegung und führt im Prinzip zu einer massenhaften Kriminalisierung von ziemlich alterstypischer Sexualentwicklung. von ziemlich alterstypischer sexuelle Entwicklung. Dafür sollen aber Strafmaß- und Verjährungsfristen für echte Täter bei sexuellen Handlungen an Kindern erhöht werden. Und die Mindestfrist bei Verjährung ist künftig 30 Jahre. Das macht Sinn, weil es sind ja oft auch sehr kleine Kinder betroffen. Dann ist man traumatisiert. Man ist nicht gleich mit Erreichen des 18. Lebensjahres plötzlich in der Lage, soas anzuzeigen. Sowas dauert eine Weile. Insofern macht eine lange Verjährungsfrist da total viel Sinn. Bei der Chatkontrolle, hier gibt es einen kleinen Link zur Chatkontrolle, da ist auch die Einrichtung eines sogenannten EU-Zentrums erwähnt. Hier taucht dieses EU-Zentrum auf, aber mit einer sinnvollen Anwendung, nämlich um Analysen und Statistiken über Opfer und TäterInnen als EU-weite Wissensplattform bereitzustellen. Das erscheint mir schon sinnvoll. In der Chatkontrolle, da stehen da ganz andere Uses drin, da soll nämlich dieses EU-Zentrum vor allem ein Datensilo sein für Darstellung sexualisierter Gewalt an Kindern. Das finde ich immer gefährlich. Vor allem bei dieser Art von Darstellung will man die nicht auf einem Haufen haben. Aber es soll vor allem auch KI-Tools bereitstellen, um private Kommunikation zu scannen und dafür IT-Unterstützung leisten. Und Prävention kommt da im Prinzip gar nicht vor.

Aber selbst diese sinnvollen Maßnahmen legen vor allem den Fokus auf die Strafverfolgung und so gut wie gar nicht auf Prävention. Das finde ich aber ist die allerwichtigste Aufgabe. Opferwerdung verhindern. Und dafür reicht es ehrlich gesagt nicht, nur darauf zu setzen, dass man WiederholungstäterInnen schneller ergreift. Damit kommen wir jetzt aber zum Ausschuss. Das war ja nur die Intro. Und im Ausschuss, da hat die Bundesregierung aus zwei verschiedenen Richtungen Sachen vorgestellt. Erstmal selber. Das war also einmal ein Staatssekretär aus dem Innenministerium, der sprach zur Chatkontrolle und dann eine Kollegin aus dem Justizministerium zu dieser neuen Kinderschutzrichtlinie. Bei der Chatkontrolle, da wurde einfach nur noch mal vom Staatssekretär betont, ja, immer noch umstritten, keine Einigung in der EU absehbar. Aber die belgische Präsidentschaft sei da total optimistisch, dass man da schneller vorankommt. Und ansonsten würden das Ungarn und Polen als Nachfolge Präsidentschaften übernehmen. Man sei sich einig mit der EU und auch mit den anderen Mitgliedstaaten, dass man eine sogenannte allgemeine Ausrichtung möglichst schnell im Konsens haben will und allerspätestens 2026, wenn nämlich diese

Ausnahmegenehmigung für große Plattformen wie Facebook und Google usw. ausläuft, dass dann eine Ersatzverordnung da sein muss. Oder mit den Worten des Staatssekretärs, sonst sieht es hier ganz dunkel aus, falls ihr das nicht wisst, diese Sonderausnahme für diese ganz großen Dienste, die gilt dafür, weil die auf freiwilliger Basis schon seit etlichen Jahren private Kommunikation scannen, also auch eure, falls ihr diese Dienste benutzt. Und damit wird im Prinzip die E-Privacy-Richtlinie ausgehebelt. Also es braucht diese Ausnahmeverordnung, weil es sonst eine Verletzung der E-Privacy-Richtlinie wäre. Und das finde ich nach wie vor total bedenklich. Wir wissen nicht, was die Bundesregierung jetzt explizit zum aktuell vorgelegten Kompromiss der belgischen Ratspräsidentschaft denkt, weil sie prüft und prüft und prüft. Und offenbar ist sie damit noch nicht fertig. Sie hat das Gleiche erklärt wie immer. Also Kleinzeitscanning ist nicht. Verschlüsselte Kommunikation kaputt machen ist auch nicht. Und mehr wissen sie aber nicht. Sie wissen eigentlich gar nicht genau, was da drin steht, weil sie prüfen und sie prüfen ja noch. Aber der Staatssekretär hat betont, diese neue Verordnung muss auf jeden Fall sicherstellen, dass das Dunkelfeld nicht vergrößert wird, wenn die neue Verordnung diese Ausnahmeverordnung für die großen Plattformen ersetzt.

Also zum Beispiel die Spezialstaatsanwaltschaft in Nordrhein-Westfalen, die macht das ja schon.

Die haben einfach mehr Ressourcen in die haben mehr die sich darum kümmern können, NRW, Leute, die Beweise auswerten und schwupps kannst du das Dunkelfeld verkleinern. Also dazu muss man nicht Massenüberwachung einführen.

wiederum vom BMJ, die sprach zur neuen Kinderschutzrichtlinie, hat die toll gefunden, kann ich auch nachvollziehen. Aber auch da zieht sich die genaue Bewertung noch. Da sind also verschiedene Ministerien beteiligt und die sind damit ordentlich fertig. Und auch da wird eine sehr schnelle Einigung angestrebt. Wahrscheinlich aber erst dann im Laufe der polnischen Präsidentschaft. Und die tritt ihr Amt an Anfang 2026.

ehrlich gesagt schlecht vorbereitet waren. Die haben das also nicht gerafft, dass es um zwei verschiedene Rechtsakte ging und haben also ständig Kinderschutzrichtlinie und Chatkontrolle in einen Top geworfen. Finde ich ein bisschen peinlich. Ich bin ja ganz alleine im Digitalausschuss. Andere Fraktionen wie die SPD haben dann neuen Mitglieder und haben es trotzdem nicht geschafft, sich ordentlich vorzubereiten. Mann, Mann, Mann. Also da wird dann zum Beispiel gefragt, ob in der Kinderschutzrichtlinie wieder Kleinstheitsscanning drin sei und der BMJ-Vertreterin mit Unverständnis begegnet, als sie das verneint und gar nicht versteht, warum da ein Kleinzeitscanning drin sein soll. Ja, weil das ja auch nicht da drin war, sondern in der Chatkontrolle. Aber nun ja. Ich fasse mal die Erkenntnisse aus den Antworten der Bundesregierung zum Thema Chatkontrolle zusammen. Worten der Bundesregierung zum Thema Chat-Kontrolle zusammen. Also ohne jetzt auf alle Fragen und Antworten so genau einzugehen. Also es gibt keine finale Position der Ampel zum neuen weil Entwurf,

Prüfung, Prüfung. Prüfung, Der frühere Vorschlag Deutschlands, die umstrittensten Teile abzuspalten und separat zu regeln, wurde von keinem anderen Mitgliedstaat aufgegriffen. Und die Position zu kleinen Sidescanning ist also weiterhin ein No-Go für die Bundesregierung, aber die Position zu Server-Side-Scanning, also was Facebook und Konsorten seit Jahren schon machen, die sei noch offen.

der ist entweder von Ende April oder Anfang das klingt für uns ein bisschen Mai, wie einfach ein neues Wort.

Aber das weiß keiner. Also auch die Bundesregierung hat keine was damit gemeint ist und hat gesagt, Ahnung, das muss nochmal technisch erklärt was werden, das so sein soll. Deswegen, also wissen wir es nicht. Nicht so fein war die Antwort, als ein Abgeordneter fragte, ja, was tut denn die Bundesregierung genau bei diesem Thema sonst noch so? Da wurde einfach nur darauf verwiesen, dass man die Daten der US-NecMec-Datenbank benutzt. Ja, wissen wir, das ist nicht alles, was man dazu machen kann. Und auch zur Quote falsch positiver Ergebnisse aus KI-Tools, die ja für sowas eingesetzt werden sollen, gab es keine Antwort. Verwiesen wurde auf Technologieneutralität, was ein bisschen bogus ist, weil es ist völlig klar, dass nur KI-Tools dafür zum Einsatz kommen und dass es natürlich eine Rolle spielt, wie groß der Anteil falsch positiver Ergebnisse ist. dass es natürlich eine Rolle spielt, wie groß der Anteil falsch positiver Ergebnisse ist. was war mein Ja, Beitrag in dieser Debatte? Ich hatte spektakuläre zwei das sind 120 Sekunden. Minuten, Da kann man natürlich nicht zu zwei verschiedenen und noch so komplexen EU-Rechtsakten vernünftige Fragen stellen und Antworten bekommen. Also quasi pro Richtlinie eine Minute für Frage und Antwort. Deswegen habe ich das diesmal mal anders gemacht. Ich habe meine Zeit einfach für ein Statement genutzt. Zur Chatkontrolle habe ich darauf hingewiesen, dass es also einfach nur ein erneuter Versuch ist, das gleiche Schlechte durchzusetzen. Ich habe auf die vernichtende Kritik bei der Anhörung zur Chatkontrolle im Digitalausschuss nachgewiesen und dass man ein soziales Problem schlicht mit Technik nicht lösen kann. Ist eine einfache Aussage, aber bei der Bundesregierung auch noch nicht angekommen. Eine Massenüberwachung von Millionen Unbescholtenen ist schlicht verfassungswidrig, weil immer noch nicht verhältnismäßig, nicht geeignet und auch nicht angemessen, siehe wissenschaftlicher Dienstgutachten. Was es stattdessen mehr braucht, sind endlich mehr Präventionen, weil wir wollen doch eigentlich alle nicht, dass es überhaupt zu Opfern kommt. Dass die die ganze Zeit nur davon reden, wie man besser Strafverfolgung zeigt, dass es nicht vor allem um die Kinder geht, dann würde man nämlich zuerst an Prävention denken, damit Kinder niemals überhaupt zu Opfern werden. Wenn man aber schon von Strafverfolgung redet, da braucht es mehr Ressourcen für die Ermittlung, um vorhandenen Hinweisen nachzugehen. Da haben wir in der Anhörung, ich kann mich da noch wie gestern daran erinnern, hat dieser eine Staatsanwalt aus NRW gesagt, dass sie manchmal für die Beweissichtung mehrere Jahre brauchen, schlicht weil sie nicht genug Leute haben. Mehrere Jahre. Wir reden wirklich fast immer von WiederholungstäterInnen. Das heißt, mehrere Jahre lang könnte man eventuell nach Analyse

von Beweisen eine Person ergreifen und stattdessen kann die weiter ein Kind nach dem anderen quälen. Also das finde ich ist komplett inakzeptabel.

Und ich ich habe es irgendwann schon mal ich mache es glaube, immer noch weil ich es immer noch komplett erwähnt, fucking fassbar mal, das Hilfetelefon des sogenannten unfassbar, Missbrauchsbeauftragten finde, des geht also um einen Beauftragten des Bundes für Missbrauchsfälle Bundes, gegen da sind Kinder in der da können die nicht anrufen. Kinder, das, Schule, Also das ist komplett Und natürlich verbietet sich auch eine Überwachungsmaßnahme, unzureichend. solange diese versprochene Überwachungsgesamtrechnung überhaupt fehlt. In meinem Statement zu dieser neuen Kinderschutzrichtlinie, da habe ich gesagt, ja klar, viele sinnvolle Maßnahmen drin, kann man machen, reicht aber nicht aus. Und Deutschland muss auch als Bund aktiver werden. Da kann man also einen Haufen Sachen tun, zum Beispiel ganz niedrigschwellig die erwähnte Hotline zu kinderüblichen Zeiten viel besser erreichbar machen, viel mehr für Prävention tun, sich vor allem gezielter kümmern um Grooming in Online-Games, das ist nämlich ein Ding und irgendwie passiert da fast gar nichts auf dem Feld. Und ein ganz konkreter, kleiner, einfacher Tipp wäre, so gute und wichtige Aufklärungsfilme wie der nach wie vor beste in diesem Feld, der heißt Gefangen im Netz, den freikaufen und in Bildung integrieren, also zum Beispiel den Bundesländern einfach anbieten. Das kostet wahrscheinlich nicht mehr als 50.000 Euro. Lass es 100.000 Euro kosten. Das sind also das Leben und die Unversehrtheit von Kindern ja wohl locker wert. Und dann könnten Eltern, Lehrkräfte, Minderjährige viel besser aufgeklärt werden. So ein Film alleine kann schon einen ganz wichtigen Beitrag leisten bei Prävention und bei Gefahrenfrüherkennung. Ich habe dann auch erklärt im Ausschuss, dass in meinem brandenburgischen Heimatort haben wir diesen Film mal von der 6. Klasse gezeigt. 100% der SchülerInnen in dieser Klasse, Jungs wie Mädels, haben eigene Erfahrungen mit Cyber-Grooming bestätigt. 100%. Kein einziges dieser Kinder hatte je mit seinen Eltern darüber geredet. Ich meine, stellt euch das mal vor. Das Ausmaß ist so riesig, es braucht da wirklich viel, viel mehr Handlung. Und dieser Film, der ist super. Den gibt es in zwei Versionen. Für ab 12 kann man also direkt auch schon Sechsklässler zeigen. Und es gibt den ab 16, dann auch für Erwachsene geeignet. Und den sollten wirklich alle Kinder, Eltern, Lehrkräfte, Menschen, die irgendwie Umgang mit Minderjährigen haben, die sollten sich den mal reinziehen. Und aktuell muss eine Schule, die diesen Film zeigen will, 50 Euro dafür bezahlen. Das muss doch echt keine Hürde mehr sein. Deswegen, lieber Bund, kauft es frei. Habe ich Sie darum gebeten. ihr schon dabei seid, Dinge zu tun. Mehr Forschung zu Tätermotiven braucht es auch und es braucht mehr vertrauliche Hilfsangebote für potenzielle TäterInnen. Das kann nämlich auch TäterInnen daran hindern, Taten auszuüben und damit verhindern, dass Kinder zu Opfern werden. Von all diesen Dingen hätte ich auch ganz gerne die Bundesregierung gefragt, was sie denn da schon macht. Aber ihr könnt es euch denken, 120 Sekunden waren da schon um. Ja, mein Fazit zu diesem Tagesordnungspunkt im Ausschuss. Die Chatkontrolle ist immer noch nicht vom Tisch. Der Zombie kommt einfach immer wieder. Die Bundesregierung ist immer noch nicht konsequent genug. Da wird viel rumgeeiert. Und vom

BMI klang es eher so, als würde man sich eine zeitnahe Einigung in der EU auch noch ausdrücklich wünschen. Und das, nach meinem Verständnis, wäre ein Bruch des Koalitionsvertrags, wenn es nicht von Deutschland eine Ablehnung gibt, massenhaft privater Kommunikation zu scannen. Die Kinderschutzrichtlinie dagegen, die ist sinnvoll, aber reicht nicht aus. Der Bund muss selber einfach noch viel mehr tun. Also Chatkontrolle in die Tonne und Kinderschutz verbessern, vor allem im Bereich Prävention. Übrigens, falls ihr das noch nicht auf dem Schirm hattet, diese Chatkontrolle, die wurde wahnsinnig gepusht in Brüssel von einer sehr finanzstarken Lobby, die privatwirtschaftliche Eigeninteresse hatte. Also so viel zu Kinderschutz. Wer dazu mehr lesen möchte, da verlinke ich euch auch noch was in den Show Notes. Damit kommen wir zu unserem nächsten Thema, nämlich Cyberangriffe mal wieder auf Parteien, auf Unternehmen etc. Das Thema ist ja nicht neu. Also hier hört ihr das öfter, in Nachrichten hört ihr das öfter. Da werden also immer wieder Sicherheitslücken ausgenutzt. Und zwar in der Regel in Systemen, die möglichst viele Menschen nutzen. Also gängige Programme, wie zum Beispiel irgendein Programm von Microsoft. Es gibt viele verschiedene Gründe, warum sowas stattfindet, also Kriminelle, die nutzen zum Beispiel Ransomware, um Kohle zu erpressen, mit und ohne Datenleak. Da hat der Bitkom übrigens für 2023 ausgerechnet, dass bei deutschen Unternehmen durch Ransomware ein Schaden von 206 Milliarden Euro entstanden ist. 206 Milliarden Euro, also ein Haufen Holz ist dahinter, aber neben den Kriminellen, die einfach Geld erpressen, gibt es auch noch andere Schäden, zum Beispiel Industrie-Spionage oder Sabotage, das ist dann mehr wirtschaftlich hinterlegt und es gibt das ganze Feld der politischen Einflussnahme, Desinformation, Manipulation gehört auch alles da rein und wir haben klassische Spionage durch andere Staaten. Um so einen Fall scheint es hier zu gehen.

geredet. Diesmal geht es aber um einen anderen Fall. Eigentlich einen älteren Fall, der aber neu bewertet worden ist. Wieder geht es um eine Sicherheitslücke bei Microsoft, diesmal bei Outlook und die ist unter anderem ausgenutzt worden, um SPD-Parteispitze zu beschnüffeln. Also die Medien konnte man entnehmen, dass da zum Beispiel Kevin Kühners Mailbox angezapft worden ist. Nochmal ein bisschen zum Hintergrund. Stattgefunden oder mitbekommen hat man das erstmalig so Ende 2022, Anfang 2023. Da gab es also Berichte über Angriffe auf E-Mail-Konten der SPD. Da gab es aber wenig interessante Infos. Man hörte immer nur so Ermittlungen laufen. Fast forward, ein Jahr, mehr als ein Jahr geht vorbei. Wir haben den Mai 2024, also quasi jetzt. Und dann hat die Bundesregierung öffentlich erklärt, dass dafür der russische Militärgeheimdienst, also so eine Untergruppe, die da cybertechnisch aktiv ist, APT 28 heißt die, meistens, hat noch ein paar andere Namen, dass die dafür verantwortlich ist. Diesen Prozess nennt man übrigens Attribution. Wenn man also einer Cyberattacke einem bestimmten Urheber zuschreibt, dann nennt sich das Attribution und das ist super selten. Der Nachweis von Tätern ist nämlich wahnsinnig kompliziert und in fast allen Fällen überhaupt nicht möglich. Da werden jede Menge falsche Fährten gelegt und dann verschwindet irgendwo die Spur im Cyberraum. Man kann nicht eindeutig sagen, von wo die herkommt. Diesmal hat man es aber getan. Also Annalena Baerbock hat sich da hingestellt,

Klartext gesprochen, hat gesagt, staatliche russische Hacker haben Deutschland im Cyberraum angegriffen und hat Konsequenzen angekündigt. Die ersten gab es auch schon, der russische Botschafter wurde einbestellt und kriegte eins auf die Mütze. Der deutsche Botschafter in Russland wurde zur Beratung nach Deutschland gerufen und es gab eine große Erklärung von der NATO. Da war die Rede von feindlichen Aktivitäten gerichtet gegen Deutschland. Solidaritätserklärungen aus baltischen Ländern, von Polen, von Tschechien, von Großbritannien. Tschechien übrigens war auch selber betroffen von diesem Hack. Abgelaufen ist dieser Angriff seinerzeit so, die Sicherheitslücke in Outlook wurde natürlich nach Entdecken von Microsoft sofort geschlossen, ist klar, aber vorher war die halt da. Und das war eine besonders gemeine Sicherheitslücke. Die erlaubte nämlich ohne Nutzerinteraktion, dass man Windows-Zugangsdaten der Nutzer abgegriffen hat, also die gehashten Zugangsdaten, ohne Nutzerinteraktion. Zugangsdaten ohne Nutzerinteraktion. Das heißt, die haben keinen Anhang geöffnet oder auf irgendeinen Link geklickt. Die haben also nichts von den Dingen getan, von denen man immer gewarnt wird. Das ist einfach quasi völlig ohne Zutun der Betroffenen ausgenutzt worden, die Sicherheitslücke. Und diese abgegriffenen, gehashten Windows-Zugangsdaten, die konnte man, je nachdem, wie das angegriffene Netzwerk konfiguriert war, schon benutzen, um böswillige, unerlaubte Zugriffe auf die E-Mail-Konten zu erhalten. Und ganz oft gab es leider auch schlechte Passwörter und dann konnte man auch noch die richtigen Passwörter erraten.

Da war die Bundesregierung recht umfangreich vertreten im Ausschuss, mit dem Innenministerium, mit dem Verfassungsschutz, mit dem Auswärtigen Amt. Also da gibt es eine Beauftragte für Cyber-Außen- und Cybersicherheitspolitik, die war da. In der Intro der Bundesregierung ging es eigentlich wie immer darum, dass sie Bedrohungen zugenommen haben, vor allem seit dem russischen Angriffskrieg gegen die Ukraine. Aber nicht nur digitale, sondern auch analoge. Aber auch das habt ihr mitbekommen. aber nicht nur digitale, sondern auch analoge, aber auch das habt ihr mitbekommen, Stichwort Spionagefälle Rüstungsdinge und so weiter. Also das war schon sehr heikel, das ist auch explizit betont worden, gerade weil die Führung einer Regierungspartei mit betroffen war und von Auswärtigen Amt wurde ganz klar gesagt, das war ein Angriff auf demokratische Institutionen und Deutschland lässt sich das nicht bieten. war ein Angriff auf demokratische Institutionen und Deutschland lässt sich das nicht bieten. In der Debatte wurde dann noch ausführlich wie denn der Weg zur Attribuierung, erklärt, also zur Zuschreibung

Da gibt es übrigens tägliche da steht dann sowas Könnt ihr euch für so eine Art Newsletter auch wenn ihr und danach hat dann BSI-Cyberlagen, eine umfangreiche technische Analyse drin. Da waren also ganz viele Ministerien registrieren, Auswärtiges wollt. Naja, das das das stattgefunden. Ich nehme mal inklusive derer nachgeordneten beteiligt, also da waren dann Amt, die Verteidigungsministerium, ganzen Geheimdienste von denen BMI, BMJ, von Verfassungsschutz Kanzleramt. bis BND, an, Behörden, dabei,

aber sicherlich auch das also das wird das schon auch BSI, mitgemischt haben. Und dann hat man natürlich das Ganze auch noch politisch eingeordnet. Und dann gab es am Mai 3. 2024 eine gemeinsame öffentliche Bekanntmachung von der Innenministerin Faeser und von Außenministerin Baerbock mit der Zuschreibung zur russischen Hackergruppe ATP28. Die haben schon ganz viel Dreck am Stecken gehabt und alle möglichen Sachen verbrochen und spielten auch im letzten Podcast eine Rolle, also die gleiche Gruppe, von der wir da reden. Was ist seitdem passiert? Also neben dieser konzertierten öffentlichen Verurteilung erfolgte auch ein expliziter Hinweis darauf, dass internationale Cybernormen gebrochen worden sind. nämlich dass man damit diese erfüllt, internationale also dieses Regelwerk Cybernorm, stärkt, weil wenn man jetzt nicht mal offiziell den Bruch dieser Cybernorm anprangert, dann wäre es komplett sinnlos. Aber natürlich kann es dabei nicht bleiben. Deswegen wird jetzt gerade abgewogen, ob es auch weitere Maßnahmen geben soll. Diese Abwägung, die erfolgt europaweit. Da gibt es eine sogenannte Cyber Diplomacy Toolbox, die gibt es schon seit 2018, um schwerwiegende Cyberangriffe abwehren zu können. Und die enthält auch ein eigenes Sanktionsregime. Also da kann man dann Sanktionen gegen solche oder aufgrund solcher Cybervorfälle verhängen. Und das macht dann die EU als gemeinsame Reaktion. Das zielt nicht auf Staaten ab. also man kann da keine Sanktionen gegen Russland verhängen, sondern da geht es immer um Individuen oder Gruppen. Aber so einfach ist es nicht, weil wie gesagt Attribution ja total schwierig ist. Das heißt, man braucht sehr belastbare und zwar öffentlich verwendbare Informationen mit sehr hohen Hürden. Und da ist man jetzt sozusagen dran. Ich habe dann in der Debatte mal nachgefragt, in diesen öffentlichen Erklärungen hat nämlich Innenministerin Faeser auch was erzählt von hochgefahrene Cybersicherheitsmaßnahmen. Das hat mich dann schon interessiert. Was ist denn das? BSI mehr Geld bekommt, zum Beispiel die 37 Millionen Euro, die denen fehlen, um ihre Arbeit richtig zu machen, nach Aussage der Präsidentin. Aber die Antwort war mir so ein echter Witz. Mir wurde nämlich gesagt, ja, hochgefahrene Maßnahmen, das heißt, aktuell hätten wir ja eine hohe Alarmbereitschaft und jetzt hätte man eine noch höhere Alarmbereitschaft. Ihr wisst jetzt auch Bescheid, oder? Also ich jedenfalls nicht. Ich habe nur so gedacht, WTF? Noch höhere Alarmbereitschaft? Also ich wir haben ja wahrscheinlich meine, schon eine sehr hohe. sehr, Was soll das jetzt geändert haben? und was den Haushalt für das BSI angeht, Naja, da wurde nur darauf verwiesen, dass wir ja gerade Haushaltsverhandlungen haben. Regierungsintern würde man über sowas reden. Deswegen könnte man da keine Aussagen machen. Und da geht es aber um den Haushalt 2025. Und ich finde, das BSI braucht jetzt Geld, weil wir haben jetzt eine Bedrohungslage und es ist erst Mai. Ich wollte noch mehr wissen zu dem, was die Bundesregierung so macht für mehr Cybersicherheit. Ich habe nämlich vor fast einem Jahr, im Juli 2023, meine schriftliche Frage gestellt. Es hat nämlich die Bundesregierung eine sogenannte Cybersicherheitsagenda beschlossen und veröffentlicht. Und da gibt es 47 Maßnahmen. Und ich habe vor einem Jahr mal gefragt, was ist denn mit diesen 47 Maßnahmen? Was ist der Stand? Die Antwort vor einem Jahr war, die eine Hälfte ist geplant, die andere ist in Umsetzung. Und eine der Maßnahmen, die in Planung war vor einem Jahr, das war eine Maßnahme des Verfassungsschutzes. Und die hieß Verbesserte Befugnisse zur

Aufklärung technischer Sachverhalte bei Cyberangriffen fremder Mächte. Was auch immer das sein möchte. Ich wollte jedenfalls wissen, wurde diese Maßnahme denn umgesetzt? Hat der Verfassungsschutz jetzt verbesserte Befugnisse zur Aufklärung technischer Sachverhalte bei Cyberangriffen fremder Mächte? Und wenn ja, was heißt das genau? Und wenn nein, wann kommt denn das? Und ich habe darum gebeten, weil wenig Fragezeit und so, mir ein Update schriftlich nachzureichen zu sämtlichen anderen 46 Maßnahmen. Also was davon ist jetzt schon wie umgesetzt? Die Antwort war zum einen, ja, diesen Nachbericht kann ich bekommen zu den 47 Maßnahmen, in welchem Zustand die gerade haben. Habe also eine schriftliche Frage gespart, das ist sehr gut. Und der Bundesverfassungsschutzvertreter hat mir geantwortet, dass es in der Tat eine Verfassungsschutznovelle gegeben hätte, also eine Gesetznovelle. Da wäre aber keine Ausweitung der Befugnisse drin gewesen, aber bis Ende der Legislatur sei eine weitere Novelle geplant. Und da geht es um mehr Befugnisse, vor allem im Cyberbereich. Also wenn da mal kein Hackback um die Ecke kommt oder vielleicht gar keine Gesetzesnovelle, weil man sich dann doch nicht einigen kann und zum Beispiel die FDP gegen Hackbacks ist. Das werden wir dann mal sehen. Dann hat es noch einen Moment schwarzen Humors gegeben. Da habe ich ein bisschen dumm geguckt. Da hat nämlich jemand den Vertreter des Verfassungsschutzes gefragt, wie wird denn so ein Cyberangriff abgewehrt so in der Praxis? Hätte man jetzt ganz viele verschiedene Dinge antworten können, aber die Antwort war echt lustig. Das nächste, was jetzt kommt, ist speziell für Honkhase. Bitte setz dich hin, halt dich irgendwo fest, lege die Streichhölzer ganz weit weg, weil du willst danach wieder alles anzünden. Die Antwort war, wie wehrt man also Cyberangriffe ab? Diese Angriffe, die sind ja oft wegen schlechter Passwörter und ein System würde man säubern, indem man die Passwörter wechselt von schlechten Passwörtern in bessere Passwörter.

Malwehr infiltriertes System wird natürlich nullkommagar nicht gesäubert durch eine Änderung von Passwörtern. Und wer das nicht weiß, der ist vielleicht in seinem Job falsch. Honkhase, ich hoffe, du bist sitzen geblieben und hast keine Streichhölzer genommen. Weil es wieder um eine Microsoft-Sicherheitslücke ging, haben wir natürlich auch ganz obligatorisch danach gefragt, was sich daraus denn für Konsequenzen ergeben für den Einsatz von Microsoft im Bund. Die Antwort war ehrlich gesagt die totale Verarsche. Von Seiten BMI hieß es, ja, das würde wieder mal zeigen, wie wichtig digitale Souveränität ist. Ja, hm, Worthülse. Ihr alle, wenn ihr regelmäßig zuhört, erinnert euch natürlich, wie das Budget für Zendes gekürzt worden ist. Die Stelle, die zuständig dafür ist, den Open-Source-Arbeitsplatz für die Verwaltung weiterzuentwickeln und wie viele Milliarden ausgegeben werden für Lizenzen an Microsoft. Aber ganz genau erfahren wir letzteres Jahr gar nicht, denn wir kriegen nicht mal als Abgeordnete den Grad der Abhängigkeit genau heraus. Ganz nagelneues Beispiel. Mein Abgeordnetenkollege Viktor Perli aus der Gruppe der Linken im Bundestag, der ist Haushaltsberichterstatter. Und der hat erfragt, welche Lizenzkosten 2023 für sämtliche Ministerien angefallen sind. Diese Abfrage macht er seit Jahren. Jährlich kommt ein steigendes Volumen für diese Lizenzen raus, zum Beispiel im Jahre seit 2015 in den sechs Jahren danach sich die Microsoft-Lizenzkosten verfünffacht haben. Und jetzt kriegt er wieder

eine Antwort auf seine jedes Jahr gleiche Frage, aber auf einmal ist sie eingestuft. Mit anderen Worten, er darf sie nicht öffentlich verwenden. Auch ich darf euch nicht sagen, wie viel Geld Microsoft jetzt für diese Lizenzen bekommt. Ich verlinke euch mal den Twitter-Thread zu diesem Thema. Er hat natürlich Widerspruch eingelegt, völlig zu Recht. Zusammengefasst, die Angriffslage, ja, Überraschung, steigt weiter. Inzwischen werden auch politische Parteien an der Spitze getroffen, bisschen wie beim Präsidentschaftswahlkampf damals mit Hillary Clinton. Nur, dass weniger öffentlich geworden ist zu den Inhalten. Und es ist eine ganz seltene öffentliche Attribution von Angreifern erfolgt. Aber sonst sind Konsequenzen kaum erkennbar. Kein Umdenken zum Einsatz von Microsoft und den Abhängigkeiten von diesen Systemen. Keine konkreten Maßnahmen außer noch höhere Alarmbereitschaft. Das BSI hat immer noch zu wenig Geld und es gab Bogus-Aussagen wie mit einem Passwortwechsel säubert man ein angegriffenes System. WTF. Also ich sag euch, die Bundesregierung muss das Thema IT-Sicherheit endlich wirklich ernster nehmen. Viel zu spät ist immer noch die Umsetzung der NIST-2-Richtlinie der Europäischen Union. Da läuft gerade erst die Verbändeanhörung. Es fehlt immer noch das Kretes-Dach-Gesetz. Und es fehlt ein konsequentes Verbot der Ausnutzung von Sicherheitslücken. Auch das Schwachstellenmanagement immer noch keine Spur, hatte die Bundesregierung auch versprochen. Was aber so gar nicht hilfreich ist, dass es auch aus diesem Anlass wieder mal die Forderung diesmal von der Union gab, Hackback zu haben. Und dass da auch pensionierte Behördenchefs, Geheimdienstchefs da solche Wünsche äußern. Damit kommen wir zum nächsten Thema. Der Anhörung zu den Spielräumen der nationalen Umsetzung bei der KI-Verordnung. Das war eine öffentliche Anhörung. Die könnt ihr euch auch komplett reinziehen. Ich verlinke euch die unten. Und natürlich habt ihr davon schon mal gehört. Wir haben ja auch in der letzten Folge, in Folge 32, über die nationale Umsetzung schon mal geredet. Aber der Unterschied zu diesmal, diesmal gab es den Fokus auf die Spielräume. Also was könnte denn Deutschland da machen? Und wir hatten eine Anhörung, bei der wir halt nicht mit der Bundesregierung geredet haben, sondern mit diversen Sachverständigen. Ich habe eingeladen Kilian Vieth-Dietelmann von Algorithm Watch. Vielen lieben Dank an Algorithm Watch, großartige Arbeit. Und ich möchte euch ans Herz legen, die diverse, wirklich gute Stellungnahmen, die verlinke ich euch auch unten, die könnt ihr euch selber durchlesen. Natürlich die von Algorithm Watch, aber auch die von Laila Fittic, eine freie KI-Expertin. Die Stellungnahme vom DGB, vom Gewerkschaftsbund mit einem Fokus auf Arbeitnehmerrechte. Dann die Verbraucherschutzzentrale Bundesverband mit sehr klaren Positionen zu Grundrechten, auch zum biometrischen ID-Fernerkennung im öffentlichen Raum. Wie gesagt, alles unten verlinkt. Ich werde es nicht in epischer Breite hier besprechen, weil es ist ja öffentlich gewesen, nachhörbar und war hier schon öfter Thema. Ein ganz kurzes Recap gibt es trotzdem. Also der AI-Act, der wird ja schrittweise in Kraft treten. In der 2. Juni-Hälfte 2024 soll am Amtsblatt der EU endgültig veröffentlicht werden und dann gelten Mitte dieses Jahres die Verbote sofort. Anfang 2025 die Regeln für die generative KI und Anfang 2026 gilt dann der ganze Rest.

In der Anhörung auch Vertreter von Wissenschaft und Industrie KI-Verband und ein Vertreter der Europäischen da, Start-up-Verband, Kommission aus der Generaldirektion CINECT war da. Ich finde spannend an diesem Thema oder die Linke überhaupt vor allem drei nämlich Sachen, einmal ein konsequentes Verbot biometrischer Überwachung und zwar von Echtzeit und sogenannte Retro-Grader-Identifikation im öffentlichen Dann natürlich Raum. die Frage der Aufsichtsstrukturen. Wie macht man die bürgerfreundlich und effektiv? Aber auch das Thema KI-Transparenzregister. Und für die drei Themen will ich euch ein bisschen zusammenfassen, was da gelaufen ist. Zur biometrischen Fernidentifikation im öffentlichen Raum. Da verbietet ja der AI-Act die Echtzeit- Identifikation komplett, aber es gibt etliche breite Ausnahmen, zum Beispiel für die gezielte Suche nach Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung, zum Abwenden einer konkreten, aber erheblichen und unmittelbaren Gefahr für das Leben, für die tatsächliche vorhersehbare Gefahr eines Terroranschlags und drittens, das ist ein bisschen breiter, für das Aufspüren oder Identifizieren einer Person, die der Begehung einer Straftat verdächtigt wird, wenn man damit strafrechtliche Ermittlungen durchführen kann. Und noch so ein paar Kleinigkeiten. Dann haben wir neben der Echtzeit-Biometrischen Fernidentifikation aber auch die Retrograde. Die steht in einem anderen Artikel drin, nämlich in Artikel 26. Das andere war Artikel 5. Da sind Anforderungen definiert, wann man KI einsetzen darf, um solche nachträgliche biometrische Fernidentifizierung durchzuführen. Zum Beispiel, wenn man eine gezielte Person sucht, die der Begehung einer Straftat verdächtigt wird oder aufgrund einer solchen verurteilt wurde. Für euch ganz wichtig zu verstehen, das war mir bis zur Anhörung nämlich auch selber noch gar nicht klar, so wie der AI-Act geschrieben ist, verbietet er jegliche biometrische Fernidentifizierung. Die genannten Ausnahmen, wo das dann doch erlaubt ist, die müssen erstmal in jedem Mitgliedstaat eine gesetzliche Grundlage bekommen. Das sind also Spielräume, die ausgenutzt werden können, aber gar nicht müssen. Und wenn man nichts tut, sind die alle verboten. Was man machen darf, ist die erlauben, aber man darf auch weitere Einschränkungen vornehmen. Also das ist völlig in Ordnung. Es könnte also auch biometrische

im öffentlichen Raum komplett verboten werden und das könnte nicht nur, das sollte auch, weil eigentlich steht es sinngemäß auch im Koalitionsvertrag drin. Für ein konsequentes Verbot in Deutschland ist übrigens sowohl der Bundesverband der Verbraucherzentralen eingetreten, aber natürlich auch Algoröwenwatch. Der Sachverständige von Algoröwenwatch, der hat nochmal ganz genau erklärt, warum das so wichtig ist. Das würde nämlich das Ende der Anonymität im öffentlichen Raum bedeuten und damit auch die Wahrnehmung von Grundrechten im öffentlichen Raum einschränken. Weil in dem Moment, wo du denkst, du bist nicht mehr anonym, nimmst du zum Beispiel dein Grundrecht auf Demonstrationsfreiheit nicht mehr in gleicher Maße wahr. Also er hat, Kilian Vieth-Diedelmann hat das, fand ich, sehr plastisch beschrieben. Er hat nämlich gesagt, wenn wir so eine biometrische Massenüberwachung im öffentlichen Raum haben, dann werden wir wandelnde QR-Codes auf zwei Beinen. Und genau das ist es. Und deswegen ist auch schon

der Aufbau einer solchen Infrastruktur mit einer abschreckenden Wirkung verbunden, also mit dem, was man immer so Chilling-Effekt nennt. Und er sagt, wenn man es einsetzen würde, hätte man auch garantiert starke Diskriminierungseffekte, dass also ganz bestimmte demografische Gruppen anders erkannt werden oder öfter falsch verdächtigt als andere Gruppen, je nachdem, von wem man so die Trainingsdaten benutzt. Und in der Regel ist es so, dass zum Beispiel sich dafür ein, dass biometrische Erkennung im öffentlichen Raum europarechtlich auszuschließen ist. Da gibt es keine Unterscheidung zwischen irgendwelchen Sorten. Und es steht drin, flächendeckende Videoüberwachung und den Einsatz biometrischer Erfassung zu Überwachungszwecken lehnen wir ab. Algorodsch hat deshalb zu Recht Beschluss folgert, so eine Technologie hat in einer demokratischen Gesellschaft einfach nichts zu suchen. Ich habe unseren Sachverständigen nochmal gefragt, ob denn diese Trennung zwischen Echtzeit und Retrograd Fernidentifikation irgendeinen Sinn macht. Also, nee, macht natürlich keinen Sinn, weil es ist ja in der Verordnung auch gar nicht klar gemacht, was das eine von dem anderen unterscheidet. Weil es ist ja in der Verordnung auch gar nicht klar was das eine gemacht, von dem anderen unterscheidet. Außerdem sind die Missbrauchspotenziale gleich, die Überwachungsgefahr ist gleich, die Diskriminierungsrisiken sind gleich. Es macht also logisch einfach mal gar keinen Sinn, das eine ganz zu verbieten und das andere nur ein bisschen. Im Übrigen gibt es durch die retrograde Fernidentifikation mit KI sogar weitere Risiken. Fernidentifikation mit KI sogar weitere Risiken. Das kann nämlich dazu führen, dass ich eine Vorratsdatenspeicherung von Video habe aus öffentlichen Quellen, also von Kameras, die so im öffentlichen Raum rumhängen, wo dann einfach später mal retrograd alles Mögliche identifiziert wird. Will man nicht haben. In seiner Stellungnahme hat Algorithm Watch übrigens auch geschrieben, dass wir teilweise solchen Einsatz ja schon haben und dass da auf den Rasterfahndungsparagrafen als Rechtsgrundlage verwiesen wird von Seiten der Polizei, dass das nicht zulässig ist. Es gibt faktisch keine Rechtsgrundlage dafür bisher. Und das wurde auch bestätigt durch einen anderen Sachverständigen, nämlich der Verwaltungsjurist Rot-Isigkeit. Der hat solange es kein neues nationales gesagt, Gesetz auch bestätigt durch einen gibt, anderen nämlich der Verwaltungsjurist Sachverständigen, Rot-Isigkeit. Der hat gesagt, solange es kein neues nationales Gesetz gibt, dass das explizit zulässt. Also eine Ermächtigungsgrundlage, die die Ausnahmen der EU-Verordnung abbildet, ist jegliche biometrische Fernidentifikation illegal. Relevant ist aber nicht nur der Zeitpunkt, also Echtzeit oder nachträglich, sondern auch wer diese biometrische Fernidentifizierung im öffentlichen Raum macht. Der AI-Act, der regelt ja nur, was staatliche Stellen zur Strafverfolgung dürfen. Dann gibt es die Datenschutz-Grundverordnung, die regelt, dass Individuen sowas nicht machen dürfen. Also es darf sich keiner in der U-Bahn gegenüber setzen und mich biometrisch fern identifizieren, das ist verboten. Aber irgendwie ungeregelt ist, was private Stellen machen dürfen. Zum Beispiel mit den Kameras, den Tankstellen, Sportplätzen, Supermärkten und so weiter herumhängen. Aber auch, was sonstige staatliche Stellen machen dürfen. Und das sind die Kameras, die auf Schulgeländen rumhängen, die bei Unis rumhängen oder bei irgendwelchen anderen staatlichen Institutionen, die keine Stellen zur Strafverfolgung sind. Solche Regelungslücken müssen unbedingt geschlossen werden.

Das hat also der Verbraucherschutzverband gefordert, das hat auch Algorithmwatch gefordert und Professor Roth-Isigkeit, der hat betont, dass zum Beispiel das Verbot bei privaten Stellen richtig leicht umsetzbar wäre, da könnte man einfach das Bundesdatenschutzgesetz an einer Stelle ein bisschen ändern. Ja, dann hatten wir natürlich das Thema Aufsichtsstrukturen. Da gibt es natürlich die Anforderungen, der EU muss unabhängig sein, unparteiisch, unvoreingenommen, muss angemessene Ressourcen haben. Es sind harte Anforderungen der EU. Die müssen gegeben sein. Was aber mehr Flexibilität hat, es ging ja um nationale Spielräume, ist, ob man das jetzt bundesweit ansiedelt, ob man das irgendwie bei den Ländern ansiedelt. Und dann auch ganz speziell nimmt man zum Beispiel den BFDI dafür, also den Bundesdatenschutzbeauftragten, oder aber die Bundesnetzagentur als quasi Oberaufsichtsbehörde. Da gibt es eine neue Studie übrigens von Beauftragten Bertelsmann, oder aber die Bundesnetzagentur als quasi Oberaufsichtsbehörde. Da gibt es eine neue Studie übrigens von Bertelsmann, die spricht sich aus für die Bundesnetzagentur als eine Option. Ich verlinke euch die auch mal unten in den Shownotes. Und ansonsten gab es keinen Konsens darüber, ob man zum Beispiel das auch mischen könnte. Ein Sachverständiger meinte, Mischverwaltung geht gar nicht. Also ein Teil bei Bund, ein Teil bei Ländern. Andere haben genau solche Konstrukte vorgeschlagen. So ähnlich wird das ja bei der DSA-Umsetzung auch gemacht. Da wird die Verantwortung geteilt und es scheint irgendwie nicht illegal zu sein. Die meisten Sachverständigen, die haben befürwortet, dass man das auf Bundesebene bündelt. Also nicht irgendwie dezentral organisiert, denn der Bund hätte die Kompetenz dafür. Das ging viel schneller, man hat irgendwie nicht 16 Ansprechpartner, sondern nur einen und man hätte viel weniger Reibungsverluste. Das heißt nicht, dass eine sektorale Zuständigkeit nicht trotzdem woanders liegen kann, also zum Beispiel die BaFin zuständig ist für Finanzkram, für Medizinprodukte, auch wer anders zuständig ist. Also solche sektoralen Zuständigkeiten sollen erhalten bleiben. Die Bundesnetzagentur haben relativ viele vorgeschlagen. Die ist nämlich schon eine sogenannte Marktüberwachungsbehörde. Und die KI-Verordnung ist ja eine Marktüberwachungsverordnung. Deswegen war die für manche Favorit. Aber es wurde deutlich gesagt, hier reicht es nicht, nur Fachstelle zu sein mit Marktüberwachungskompetenz. KI ist ein sozio-technisches System. Also man braucht sozio-technische Expertise, man braucht Grundrechtsexpertise. Das reicht nicht, wenn man nur weiß, wie man Märkte reguliert. auch im Gespräch, ob man eventuell lieber den Bundesdatenschutzbeauftragten nimmt, der hat ganz viel Überwachung im Bereich Grundrechte-Schutz, aber relativ wenig zur Marktüberwachung. Also egal, welche der beiden Institutionen man nimmt, man muss ein bisschen Kompetenz noch dazu entwickeln. Die BNSA braucht Grundrechte-Kompetenz mehr und der BFDI bräuchte mehr Marktüberwachungskompetenz. Also mal gucken, auf was es hinausläuft, aber ich glaube, wahrscheinlich wird es wieder die B-Netz-Arm. Gewünscht wurde von einigen Sachverständigen auch ein Beirat einzurichten, ähnlich zum Digitale-Dienste-Gesetz. So oder so kommt es aber vor allem darauf an, aus Sicht des Verbraucherschutzes, dass man ein vernünftiges Beschwerdemanagement hat. Also ein One-Stop-Shop, dass man nicht als

Bürgerin sich bei unterschiedlichen Stellen melden muss. Und dann, habe ich ja gesagt, gibt es für uns noch einen dritten Schwerpunkt, nämlich ein KI-Transparenzregister. Die KI-Verordnung, die schafft eine EU-Datenbank, steht in Artikel 70 der KI-Verordnung, aber in der tauchen nur Hochrisikosysteme auf und nach Schätzung eines Sachverständigen sind das so Pi mal Daumen 10 Prozent der KI-Systeme. Vielleicht sind es sogar noch weniger. Das reicht aber nicht. Also es braucht ein nationales KI-Register, das den gesamten Verwaltungssektor umfasst. Und zwar Bund, Länder, Kommunen, egal welche staatliche Stelle KI einsetzt, sollte sich in so ein Register eintragen. Das fordert auch Algorithmwatch. Aber ansonsten war das echt wenig Thema in der Anhörung. Also laut Leider. aber ansonsten Algorithmwatch, war das echt wenig Thema in der Leider. Anhörung. Also laut Algorithmwatch entstehen ja Risiken der KI vor allem durch den Einsatz. Und der Einsatz von KI in der Verwaltung, Stichwort Gewaltmonopol, ist natürlich mit besonderen Risiken verbunden. Und deswegen ist gerade da Nachvollziehbarkeit und Kontrolle besonders wichtig. Da braucht es wache Augen, es braucht mehr Transparenz. Kontrolle besonders wichtig. Da braucht es wache Augen, es braucht mehr Transparenz. Aber neben diesen Themen wäre so ein Register auch super hilfreich, um zum Beispiel Doppelentwicklung zu verhindern oder den Wissensaustausch in der Verwaltung zu fördern. Wer hat Erfahrung mit welcher Art KI-System? Was gibt es da überhaupt schon solche Sachen? Wir wären nicht die Ersten, denn ein KI-Register gibt es ja zum Beispiel schon in den Niederlanden. Was wir neu erfahren haben, ist, die EU-Datenbank soll erfreulicherweise offene Schnittstellen bekommen. Das heißt, wenn man so ein nationales Register macht, kann man das im Prinzip mit den gleichen offenen Schnittstellen umsetzen und dann kann das eine wie so Puzzelnöppel ans andere angedruckt werden. AlgoWatch hat übrigens auch konkrete Vorstellungen, was da reingehört. Das könnt ihr in der Stellungnahme nochmal nachlesen, weil wenn das oberflächlich gemacht ist, ist es nicht aussagefähig und dann ist es im Prinzip auch ein bisschen für die Füße. Man muss also einmal das Problem definieren, das das KI-System lösen soll. Das habe ich auch in meiner kleinen Anfrage zum Einsatz von KI im Bund gefragt. Keine einzige Behörde hat diese Frage beantwortet. Dabei ist das natürlich eine Schlüsselfrage. Was soll die KI eigentlich für ein Problem lösen? Da muss eine konkrete Zieldefinition rein. Soll das Entscheidungen unterstützen, Effizienz verbessern, Aufgaben automatisieren? Muss man wissen. Dann welche ethischen und rechtlichen Anforderungen werden gestellt? Datenschutz, Fairness, Erklärbarkeit, jada jada. Welche Grundrechtsauswirkungen gibt es? Welche Umweltverträglichkeit gibt es? Das sind so Sachen wie Energieverbrauch, Treibhausgas, Emissionen etc. In so einem Register muss auch drinstehen, wer ist denn verantwortlich? Ja, wen kann ich kontaktieren, wenn ich dazu Fragen habe? Und das Ganze funktioniert natürlich nur sinnvoll, wenn es verpflichtend ist, wenn also wirklich alle in öffentlicher Hand verwendeten KI-Systeme da auch eingetragen werden.

sich im Prinzip alle einig, möglichst wenig Regulierung, möglichst viel Freiheit für ihre unternehmerischen Tätigkeiten und auf gar keinen Fall strengere Regeln in Deutschland. Aber das hättet ihr euch auch von alleine so gedacht, nehme ich mal an. Also Fazit, die

Bundesregierung muss da mal zum Pott kommen, hat eine ganze Latte Hausaufgaben, muss sich aber vor allem erstmal einigen und da vor allem auf die Aufsicht und die Governance-Entscheidungen sind nicht wirklich eine Stärke der Ampel. Das war fast immer Mein Best Guess Hick-Hack. man einigt sich trotzdem ist, auf die Bundesnetzagentur. Da hat man das schon einmal durchdekliniert mit der Umsetzung des Digital Services Act. Und ansonsten gab es guten Input von den Sachverständigen zum zur Beirat, Transparenz, zu KI-Register, zur Wahrung der Grundrechte. Also da liegt der Ball jetzt im Feld der Bundesregierung. Unser letztes Thema heute ist das erste Meeting der nagelneuen ständigen DigitalministerInnen-Konferenz. Ganz formal heißt die ständige Fachkonferenz der Digitalminister. In der sind die Minister, Staatssekretäre, SenatorInnen der Bundesländer drin, die halt die Zuständigkeit für Digitales haben und das BMDV als Gast. Das ist nämlich eine Länderfachkonferenz. Und beim ersten Treffen am 19.04.2024 in Potsdam, da war auch Claudia Plattner dabei, die Präsidentin des Bundesamts für Sicherheit in der Informationstechnik. Jedes Jahr wechselt da der Vorsitz. Zurzeit hat ihn ein Staatssekretär meines Bundeslandes inne, nämlich Brandenburg. Und im Oktober gibt es dann das nächste Treffen. Und da wird Hessen der Gastgeber sein, wer es genau wissen will, am 24. Oktober 2024. Das Ganze soll den IT-Planungsrat nicht ersetzen, sondern nur ergänzen. Und es gab viele Themen bei dieser ersten Konferenz. Also die hatten einen Haufen zu tun. Da ging es um KI, um digitale Zwillinge, um smarte Regionen. Es ging um das Thema, wo kriegt man denn die Fachkräfte her, vor alles das. Und es ging um Arbeitsbedingungen beim Infrastrukturausbau für die digitale Infrastruktur. Da gibt es nämlich offenbar ein massives Problem, also Schwarzarbeit und solche Sachen vermutlich. Und natürlich ging es um Cybersicherheit, weil Präsidentin Plattner war ja da. Und die hat dort klargestellt, Basisanforderungen müssen auch für Kommunen gelten. Ich vermute mal, da ging es um den Grundschutz, weil das ist so eine Debatte. Viele Kommunen halten den BSI-Grundschutz nicht ein, ob das für die gelten muss oder nicht. Und ich glaube, dass deshalb dieses Kritis-Dach-Gesetz so lange nicht aus dem Knick kommt. Im Ausschuss war Staatssekretärin Kluckert aus dem BMDV da. Und weil wir schon fortgeschritten waren in der Zeit, wurde die Debattenzeit für die Fraktionen von vier auf drei Minuten gekürzt. Aber wie ihr ja wisst, ich kriege ja als kleine linke Gruppe nur die Hälfte der Zeit. Weil aber die Hälfte von drei Minuten absolut lächerlich ist, habe ich also äußerst freundlich darum gebeten, meine Zeit ausnahmsweise nicht auch zu kürzen, sondern bei zwei Minuten zu lassen, weil 90 Sekunden ist ja irgendwie für die Füße. Leider wurde das von der Vorsitzenden abgelehnt mit der Begründung, wir seien ja schon so spät dran. Die 30 Sekunden meiner Redezeit sollen da also wirklich einen Unterschied gemacht haben. Für mich hätten sie einen gemacht, für den Ausschuss nicht. Aber ja, so war das dann. Leider. Ein paar kleine Hot Facts aus der Debatte für euch. Es ging unter anderem um das krasse Scheitern des Online-Zugangsgesetzes 2.0 im Bundesrat. Das war also im Ausschuss, aber auch bei dieser Digitalministerkonferenz natürlich Thema. Und Staatssekretärin Kluckert hat da also vergleichsweise selbstkritisch gesagt, bei der Verwaltungsdigitalisierung sind wir in einer Oberkatastrophe. Kann man sagen, würde ich durchaus nicken. Und hat dann aber die Blockadehaltung beim OZG 2.0 durch die unionsgeführten Länder, hat sie natürlich auch kritisiert, wenn auch eher ein bisschen

vorsichtig. Es blieb ein bisschen unklar, inwieweit die Digitalministerkonferenz da jetzt was ändern kann. Also ihre Aussage war nur, Gespräche helfen ja irgendwie immer. Aber am Ende steht und fällt der Fortschritt mit den Standards. Und da blockieren die Länder einfach das OZG 2.0 im Bundesrat. Das Problem ist übrigens, dass die Länder da gebremst werden durch die Eigeninteressen ihrer eigenen IT-Dienstleister. Die sind nämlich überhaupt nicht interessiert an einheitlichen Standards. Die verdienen mehr an proprietären Insellösungen quasi pro Bundesland. Für die ist mehr Abhängigkeit besser. Und das ist jetzt für uns alle in Deutschland ein Problem. Ich hatte, wie gesagt, nur 90 Sekunden. Also was wollte ich wissen? Ich habe gefragt, ob bei der Digitalministerkonferenz beim Thema künstliche Intelligenz auch aus meiner Sicht relevante Themen zur Sprache kamen, nämlich ein gemeinsames KI-Register zwischen Bund und Ländern. Das will der Bund nicht alleine machen. Und standardisierte Risikobewertungswerkzeuge für KI. Würde total Sinn machen, wurde aber beides nicht diskutiert, denn man hatte offenbar als Unterthema nur KI in der Arbeitswelt. Gefragt habe ich auch danach, wie man diese Digitalministerkonferenz dazu nutzen kann, endlich das Online-Dashboard zum OZG-Umsetzungsstand zu verbessern. Das erfüllt nämlich den durchschnittlichen, ganz normalen Informationsbedarf von Menschen so null. Ich habe mal nachgefragt, warum das halt so kacke ist und man da nicht mehr Infos kriegen kann. Und da hat der Bund mir geantwortet, dass er die Daten der Länder halt leider nicht hat. Und da wäre doch eine richtig geile Idee, wenn diese Digitalministerkonferenz jetzt sich gemeinsam darauf kommittelt, alle nach einheitlichen Standards diese Daten für dieses Dashboard bereitzustellen. BürgerInnen interessieren sich nämlich nicht, wofür das Land und wofür der Bund zuständig ist. Die wollen diese eine Plattform, wo das alles draufsteht. Aber Staatssekretärin Kluckert meinte nur, das ist eine Länderfachkonferenz, da kann man als Bund nichts fordern. Ich finde, mitreden kann man auf jeden Fall. Man kann auch Wünsche äußern, man kann die Plattform nutzen, um darauf hinzuarbeiten. Rederecht hat ja der Bund da. auch 15.05.2024, einen sehr interessanten Familienausschuss. Und weil der immer öffentlich könnt ihr falls es euch interessiert, tagt, euch, diesen Abschnitt auch online selber anhören. Da ging es um den Rollout von Altersverifizierung im Internet.

Die Bundesregierung scheint davor zu haben, etwas, das am Ende zu Alterskontrollen für alle führt. Also nie wieder wirklich anonym im Internet. Sein Alter, irgendwie muss man sich da outen. Es wurde nicht klar gesagt, für welche Dienste es gelten soll. An einer Stelle wurden mal soziale Medien erwähnt, an anderen war das ein bisschen breiter. Gemeint ist, dass Kinder, die noch gar keinen E-Perso oder Perso haben, ein alternatives System nutzen können, das die Bundesregierung gerade entwickelt, wo Minderjährige digitale Altersnachweise, haltet euch fest, von Meldebehörden, von Schulen, sogar von privaten Banken ausgestellt bekommen sollen, und zwar digital, während sie sich online zum Beispiel für ein soziales Netz registrieren wollen oder später in größeren Zeitabständen, um vielleicht zu beweisen, dass sie jetzt schon 16 geworden sind oder so. Da soll nicht das Alter direkt übermittelt werden, sondern nur die Bestätigung, ob man einer bestimmten Alterskohorte angehört. Ich vermute mal sowas wie über 13, unter 18, also minderjährig, aber ich darf schon Instagram, so Sachen.

Im Herbst soll dazu eine technische Umsetzung mit einem sogenannten Demonstrator vorgestellt werden. Aber mir ist komplett unklar, wie will man denn bundesweit flächendeckend Schulen, Meldestellen, private Banken da einbinden? Das ist eine total schräge Vorstellung. Wie will man das technisch integrieren? Welche Prozesse will man machen? Wie will man die Kompetenzen dafür aufbauen? Wer will da welche Aufwände bezahlen? Und sieht dann zum Beispiel eine Schule, für welches soziale Netz sich dann Siebtklässler anmelden will und können die darauf Einfluss nehmen? Also zum Beispiel auch eine Kooperation verweigern? Und was ist mit allen anderen Usern, die gar keine Kinder sind? Muss ich immer und überall, zum Beispiel mit einem Perso, mein Alter nachweisen? Die Folge von so etwas wäre ganz klassisch eine Überidentifikation und das finde ich sehr, sehr bedenklich. Das soll den Digital Services Act umsetzen. Ich finde, dass das zu weit gesprungen ist, zu viel will. Der Kollateralschaden ist einfach zu hoch. Also wer sich das angucken will, ich verlinke euch das in den Shownotes. Öffentliche Sitzung, Familienausschuss. Ab einer Stunde, 15 Minuten, 30 Sekunden geht dieser Abschnitt los. Ansonsten ganz zum Schluss noch ein Hinweis auf einen Rekord, nämlich vier öffentliche Tagesordnungspunkte im nächsten Digitalausschuss am 5. Juni 2024. Da könnt ihr teilnehmen, entweder analog vor Ort oder per Livestream. Für die analoge Teilnahme müsst ihr euch anmelden. Da haben wir die Themen Meta, Konzern ist zu Gast, wegen Verstoß potenziell gegen DSA-Compliance. Da gibt es nämlich etliche Accountsperren politischer Organisationen mitten im Wahljahr, zum Beispiel Kreisverbände von bestimmten Parteien. Dann haben wir als Thema die Telekom-Mindestverordnung. Das ist zu Deutsch das Recht auf lahmes Internet und wie gut es umgesetzt wird. Und wir haben mal wieder das digitale Dienste-Gesetz, den Aufbau des digitalen Dienste-Koordinators, also die Bundesnetzagentur. Da wurde endlich das Gesetz veröffentlicht und damit ist die Bundesnetzagentur erst jetzt offiziell zuständig und die Plattform für Nutzerbeschwerden ist jetzt auch diese Woche online geschaltet worden. Ich verlinke euch die auch und man kann sich jetzt offiziell als Trusted Flagger dort registrieren lassen. Unser viertes Thema, auch öffentlich wird sein, die neue Gigabit-Richtlinie. Damit habt ihr jetzt wieder einmal alles gehört, was digital wichtig war und eine Rolle spielt im Digitalausschuss. Ihr habt gut durchgehalten, ihr seid gut informiert und ihr bleibt hoffentlich gut von der Sonne beschienen und wir treffen uns beim nächsten Mal akustisch nach dem 5. Juni 2024. Gebt mir gerne Feedback, nutzt den Hashtag derADBPodcast und wenn ihr es noch nicht abonniert habt, diesen wunderschönen Podcast, dann macht das einfach noch. Bis dahin.