Rechtsanwältin Karina Filusch, LL.M. | Friedrichstraße 95, 10117 Berlin | T: 030 219 11 555

„DaSou-Wahlcheck Part I“ zur aktuellen Datenpolitik

DaSou-Podcast-Folge mit Dr. Dennis-Kenji Kipker

Karina Filusch: Hallo und herzlich Willkommen beim DaSou Podcast. Ich bin Karina Filusch, Datenschutzanwältin und externe Datenschutzbeauftragte. In jeder Folge sprechen wir mit einer Expertin oder einem Experten über Datensouveränität, abgekürzt DaSou. Schön, dass du wieder dabei bist und reinhörst. Abonniere doch unseren Podcast, wenn er dir gefällt und hinterlass uns auch gerne eine Bewertung, darüber freuen wir uns sehr.

Jakob Schüssler: Herzlich Willkommen auch wieder von meiner Seite. Ich bin Jakob Schüssler und studiere Jura an der Universität Hamburg.

Karina Filusch: Schön, dass du wieder dabei bist, lieber Jakob, und mich unterstützt. Heute wollen wir über ein sehr politisches Thema reden, nämlich über Cybersicherheit und über die gesetzlichen Regelungen, die dazu in letzter Zeit ergangen sind. Da ist nämlich unglaublich viel passiert.

Jakob Schüssler: Politisch brandaktuelle Themen sind zurzeit beispielsweise das IT-Sicherheitsgesetz und ein Gütesiegel im Hinblick auf digitale Verbrauchersouveränität oder jetzt auch ganz neu aus der Innenministerkonferenz die Log-in-Fallen. Es geht darum, dass die Nutzerinnen und Nutzer digitaler Dienste die Möglichkeit haben, Kommunikation mit anderen Menschen, die sie als potenziell beleidigend einstufen, direkt über eine Plattform an die Behörden zu melden. Die Behörden stellen demjenigen Nutzer, der die beleidigende Äußerung verschickt hat, dann eine sogenannte Log-in-Falle. Bei der nächsten Anmeldung wird seine IP-Adresse an die Ermittlungsbehörden gesendet und diese können das dann an die entsprechenden Telekommunikationsanbieter weiterleiten, sodass sie von dort die gespeicherten Stammdaten, die Namen und die Anschrift enthalten. So soll also online eine Identifizierung möglich sein, mit der wiederum Anklage erhoben werden soll. Im Folgenden wollen wir uns den Sinn und den Unsinn derselben anschauen.

Karina Filusch: Du sagst es. Zudem wollen wir auch über Hass im Netz reden und was

es da für Möglichkeiten für Verbraucherinnen und Verbraucher gibt, sich zu schützen. Dazu haben wir Dr. Dennis-Kenji Kipker eingeladen. Er unterrichtet an der Universität Bremen, am HPI in Potsdam und an der Universität Riga. Er ist Herausgeber verschiedener Handbücher, Kommentierungen und Zeitschriften im Bereich Cybersecurity und es gibt einen großartigen Wikipedia-Eintrag über ihn. Bei seinen ganzen Aktivitäten frage ich mich: „Dennis, wann schläfst du eigentlich?“.

Dennis-Kenji Kipker: Erst einmal möchte ich mich herzlich bei euch beiden für die Einladung bedanken. Es freut mich sehr, heute dabei zu sein. Ich musste gerade eben schon fast lachen, als du von diesem Wikipedia-Eintrag gesprochen hast. Da habe ich selbst schon seit Monaten nicht mehr reingeschaut. Ich weiß gar nicht so richtig, was genau darinsteht. Aber um vielleicht zunächst auf deine erste Frage zurückzukommen: Natürlich, es ist ein Fulltime-Job. Momentan passiert im Bereich Digitalisierung, Gesetzgebung, technische Weiterentwicklung sehr viel. Ich will damit nicht sagen, dass ich mittlerweile einen 24/7 Job habe, aber davon bin ich nicht weit entfernt. Ich beobachte, was überhaupt passiert, wie der Gesetzgeber und wie die Politik auf neue digitale Herausforderungen reagieren und wie man das bewerten muss, sowie was man unter bestimmten Gesetzen zu verstehen hat. Zu entscheiden ist, ob etwas gut oder schlecht ist und wie sich das auf den Verbraucher sowie letzten Endes auch auf die Wirtschaft hierzulande auswirkt. Das sind alles wichtige Fragen. Ich finde das hochinteressant. Ich glaube, das ist auch so ein bisschen meine Motivation und mein Antrieb, sodass ich sage, man kann sich durchaus mal in seiner Freizeit damit beschäftigen. Man muss das jetzt nicht nur auf die Berufszeit von 8-16 Uhr begrenzen.

Karina Filusch: Ja, gut, dass du diese Leidenschaft hast. Es gibt nämlich nicht so viele Cybersecurity-Experten in Deutschland. Deswegen bist du auch so gefragt und tauchst bei diesen Themen immer wieder auf. Dein Name ist jedem ein Begriff, der sich mit Cybersecurity beschäftigt und du hast die Unternehmen angesprochen. Darüber wollen wir heute auch reden, vor allem über soziale Netzwerke. Da stellt sich uns natürlich die Frage: „Datenschutz und informationelle Selbstbestimmung im Verhältnis zu den sozialen Netzwerken. Woran hapert es und was ist eigentlich der Status quo bei dieser Fragestellung?“.

Dennis-Kenji Kipker: Das ist eine sehr vielschichtige Fragestellung und ich glaube auch nicht, dass man das in Kürze beantworten können wird. Soweit es hier um soziale Netzwerke und informationelle Selbstbestimmung geht, ist das ein Thema, was eigentlich schon seit Jahrzehnten irgendwo auf der digitalpolitischen Agenda steht und das mit ganz unterschiedlichen Facetten. Ich denke hier an dieses klassische Thema

der Einwilligungen. Gibt es die informationelle Selbstbestimmung überhaupt noch? Diese Frage ist gerade in Bezug auf soziale Netzwerke wie beispielsweise Facebook interessant. Weiterhin gibt es noch die Themen Auslandsdatenübermittlung und Hate Speech. Es gibt die schöne Aussage: „Das Internet vergisst niemals." Das großartige Recht auf Vergessen werden. In diesem Zusammenhang gibt es auch Gesichtspunkte, die eine wirtschaftliche Relevanz besitzen. Mir fällt da immer dieses Beispiel mit der australischen Regulierung für Verlagsvergütungen ein, was wir zu Beginn des Jahres hatten. Da ging es darum, dass ein nationaler Gesetzgeber solche transnational agierenden Großkonzerne wie z.B. Google oder Facebook regulieren wollte, damit eben auch Verleger eine bessere Vergütung erhalten. Es hieß dann auch, dass Google oder Facebook beispielsweise nicht mehr in Australien verfügbar wären, wenn die Rechtslage dort auf eine bestimmte Art und Weise geändert werden sollte. Die Großkonzerne wissen natürlich, dass sie eine erhebliche Marktmacht und damit natürlich auch eine erhebliche wirtschaftliche Macht haben. Daher versuchen sie, die nationalen Gesetzgeber so ein bisschen auszuhebeln. Deswegen wird Plattformregulierung meiner Meinung nach ein wichtiges Thema der Zukunft sein. Früher haben wir im Zusammenhang mit sozialen Netzwerken in erster Linie über Datenschutz und über die informationelle Selbstbestimmung gesprochen. Das hattest du einleitend auch gesagt. Meiner Meinung nach rückt dieses immer stärker in den Hintergrund oder wird auch ein Nebenaspekt, weil die Konzerne immer mächtiger sind und mittlerweile auch ganz andere Aspekte, beispielsweise auch wettbewerbsrechtliche oder kartellrechtliche Aspekte, dahinterstehen. Deswegen ist das ein sehr vielschichtiges Thema. Ich glaube, das wird eine Herausforderung des neuen Jahrzehnts, das gerade begonnen hat, sein. Ein weiteres Beispiel in diesem Zusammenhang ist auch die anstehende Bundestagswahl. Heute Morgen habe ich noch gelesen, dass sich tatsächlich viele Bundesbürger vor Desinformation fürchten. Gerade, wenn man Facebook, Instagram oder Ähnliches benutzt und sich auf die dort verfügbaren Informationen verlässt, die für einen zusammengestellt werden, kommt man ganz schnell in eine Filterblase rein, wo vielleicht auch nur die Daten und Informationen zur Verfügung gestellt werden, die man sehen oder hören will. Andere Sachen oder Themen, vielleicht auch kritische Stimmen, bekommt man dann gar nicht mehr mit. Gerade beim Thema Fake News, was auch mit Plattformen und Plattformregulierung zu tun hat, wird es letztlich immer schwieriger zu unterscheiden: „Was ist denn jetzt die Wahrheit und was ist falsch?". Selbst große Nachrichtenportale haben des Öfteren Artikel veröffentlicht, die nicht zu 100% richtig gewesen sind. Ich glaube, das Thema Plattformregulierung mit diesen ganzen unterschiedlichen Gesichtspunkten richtig und effektiv anzugehen, wird eine ganz große Herausforderung in diesem neuen Jahrzehnt - auch jenseits des Datenschutzes.

Karina Filusch: Ja, dazu gab es bereits ein paar Vorstöße von verschiedenen europäischen Ländern. Deutschland und Österreich haben auch schon Regulierungen gefunden. Auf europäischer Ebene gibt es den Digital Services Act. Vielleicht können wir später noch ein bisschen darüber sprechen. Du hast sehr viele spannende Aspekte angesprochen, sodass ich gar nicht weiß, wo ich anfangen soll. Lass uns doch vielleicht gleich beim Datenschutz und der Auslandsübermittlung bleiben. Wir haben schon in vorherigen Podcast-Folgen über Schrems II gesprochen. Dieses Urteil macht den Datentransfer in die USA, sagen wir es mal direkt, unmöglich, weil der EuGH festgestellt hat, dass in den USA kein angemessenes Datenschutzniveau herrscht. Deshalb sollen alle Unternehmen in Deutschland sofort den Datentransfer in die USA stoppen. Vielleicht können wir darüber reden. Wie sieht es in der Zukunft aus? Ist das überhaupt gut, dass der Datentransfer in die USA so kritisiert wird und wir gleichzeitig aber trotzdem Daten nach China transferieren?

Dennis-Kenji Kipker: Schrems II ist schon fast ein alter Hut. Schrems II ist mittlerweile in etwa ein Jahr und wir stehen im Wesentlichen dort, wo wir letztes Jahr gestanden haben, was ich ein bisschen kurios finde. Oftmals findet eine an sich nunmehr höchst unsichere bzw. gar rechtswidrige Datenübermittlung in die USA statt, weil die Unternehmen auf bestimmte Produkte angewiesen sind. Man sollte allein schon daran denken, wie viele Unternehmen Microsoft oder Microsoft 365 Pakete verwenden und gar nicht anders können. Dass das im Wesentlichen nicht sanktioniert wird, finde ich sehr problematisch, auch mit Blick auf den Datenschutz. Nach der zweiten Schrems-Entscheidung haben sich viele gedacht: „Ja, das ist jetzt das Richtige gewesen.“ Alle wussten, dass Safe Harbour kein besonders gutes Abkommen gewesen ist und das Privacy Shield letzten Endes auch im Wesentlichen nur ein Logo mit einigen Verschriftlichungen gewesen ist, die das Datenschutzniveau garantieren sollten. Wir wussten auch alle, wie lasch die Kontrollen in den USA seit jeher sind. Wir wussten, wie wenig sich die Federal Trade Commission darum gekümmert hat, obwohl sie ebenso für dieses Thema zuständig ist. Außerdem wurde schon bei Safe Harbor nicht viel gemacht. Zudem wussten wir, dass in den USA spätestens seit dem 11. September 2001 eine ganz erhebliche Datensammel-Gesetzgebung und Überwachungsgesetzgebung zu Zwecken der nationalen Sicherheit vorangetrieben wurde. Es ist klar, dass sich die USA nicht unterkriegen lassen und ihre gesamten Überwachungsgesetze von einem auf den anderen Tag abmildern oder abschaffen, nur weil der Europäische Gerichtshof sagt:“ Oh, jetzt ist die Datenübermittlung unzulässig.“ Wir als Europäer begeben uns mit diesen ganzen Schrems-Entscheidungen letzten Endes in eine Art Zwickmühle herein. Wir sagen: „Ja, wir haben noch ein gutes europäisches Datenschutzniveau“, wobei wir natürlich auch die

Überwachungsgesetzgebung vorantreiben. Vor seiner eigenen Haustür sollte man durchaus kehren. Vorratsdatenspeicherung z.B. ist ein Thema, was in der Europäischen Union immer wieder auftaucht. Dennoch sagen wir die ganze Zeit: „Ja, wir können die Daten nicht in die USA transferieren“, obwohl wir - jetzt kommt auch wieder das Thema digitale Souveränität auf, eigentlich noch auf viele Hard- und Softwareleistungen in den USA angewiesen sind. Letztendlich begeben wir uns in eine schwierige Situation. Deswegen muss man sich in der Praxis auch fragen: „Hat denn jetzt die Schrems II-Entscheidung, so gut das Ergebnis in der Theorie auch sein mag, in der Praxis wirklich einen Mehrwert gebracht?“. Meiner Meinung nach nicht wirklich. Das Datenschutzniveau kann trotz geänderter Standardvertragsklauseln nicht ohne Weiteres garantiert werden, selbst wenn man Auftragsverarbeiter mit Sitz in den USA hat, weil die Daten zur Verwendung wieder entschlüsselt werden müssen. Außerdem haben wir das Problem, dass Daten oftmals nach wie vor transferiert werden. Dies war aber eigentlich schon nach Schrems I so, obwohl es keine vernünftige Rechtsgrundlage gibt und die Aufsichtsbehörden das irgendwie einfach hinnehmen müssen. Damit machen wir uns, soweit es unser eigenes Datenschutzniveau anbelangt, in gewisser Hinsicht unglaubwürdig. Nicht nur für uns selbst, sondern auch mit Blick auf andere Staaten. Ein weiteres Problem in dem Zusammenhang ist eindeutig, dass wir uns immer nur auf den transatlantischen Datentransfer beziehen. Allerdings kommen nun mal auch ganz viele Produkte für den Verbraucher aus dem Bereich IoT und Smart Home und auch jenseits des Verbrauchers aus I-4. aus Fernost, also z.B. aus Taiwan und aus der Volksrepublik China. Das führt dazu, dass Datenströme auch dort hingehen. Wenn ich mir eine billige IP-Cam auf Amazon bestelle, die dann eben eine Software für mein Handy hat, worauf Daten gespielt werden können, dann muss einem als Verbraucher bewusst sein, dass die Daten nicht direkt von der IP-Cam auf mein Handy gehen, sondern erst auf den Server, der irgendwo in China steht. China hat eine umfassende Überwachungsgesetzgebung. Das ist bekannt. Zudem ist China auch nicht unbedingt als demokratischer Staat bekannt. Hier haben wir also gewaltige Probleme, soweit es um das Thema Datenschutz geht. Leider ist es so, dass die Vereinigten Staaten in dem Zusammenhang immer wieder als sehr böse dargestellt werden. Die Europäische Union hingegen wird als weißer Ritter dargestellt und alles andere wird in dieser ganzen Debatte meiner Meinung nach ausgeklammert. Wenn man jetzt wieder an das Thema Auslandsdatenübermittlungen denkt, wird von manchen schon über Schrems III gesprochen. Dies geschieht mit Blick auf den vor Kurzem trotz erheblicher Bedenken seitens des Europäischen Parlaments geschlossenen Angemessenheitsbeschluss für United Kingdom. Zu bedenken ist, dass das UK Mitglied der globalen Überwachungsallianz Five Eyes ist, zu denen auch die Vereinigten Staaten gehören. Es ist bekannt, dass das United Kingdom eine gute Überwachungsgesetzgebung hat. Das liegt unter anderem daran, dass dort in den letzten Jahren erhebliche Probleme mit terroristischen Anschlägen aufgetreten sind. Warum die Europäische Kommission darin

kein Problem sah, aber der Europäische Gerichtshof über die USA sagt, dass das Niveau definitiv nicht gewahrt werden kann, ist für mich nicht nachvollziehbar – gerade, wenn man bedenkt, dass das UK und die USA zusammenhängen, soweit es eben um Datenaustausch zu nachrichtendienstlichen Zwecken, zur Gefahrenabwehr und zur Strafverfolgung geht. Es handelt sich dabei um einen Bruch mit der Wertung, die der EuGH vorgenommen hat. Ich hoffe deshalb nicht, dass wir in der Zukunft dann auch noch eine Schrems III-Entscheidung kriegen, welche sagt, dass der Angemessenheitsbeschluss mit dem UK nun genauso hinfällig wie derjenige mit den USA ist. Wir begeben uns da auf sehr, sehr dünnes Eis, auch in wirtschaftlicher Hinsicht, weil wir noch nicht genügend technologische digitale Souveränität haben, um solche rein rechtlichen Wertungen auch praktisch hardwaremäßig umzusetzen.

Karina Filusch: Das hast du gerade richtig schön dargestellt. Scheinbar ist die Europäische Kommission auf einem Auge blind und verhält sich auch widersprüchlich. Ich bin gespannt, wie das mit Großbritannien letztendlich ausgeht und ob es auch zur Persona non grata wird. Ich bin gespannt, wie genau die Lösung schlussendlich aussehen wird. Man könnte jetzt überlegen, was könnte die Lösung sein, um wirklich souverän in Europa zu sein und um den Datenschutz wirklich für Verbraucherinnen und Verbraucher konsequent durchzusetzen, statt einfach den Datentransfer in bestimmte Länder zu verbieten. Eigentlich müsste es doch neben solchen Urteilen auch weitere politische Programme geben, um diese Unabhängigkeit zu stärken. Wie könnte man dieses Ziel erreichen?

Dennis-Kenji Kipker: Das ist meiner Meinung nach keine juristische Frage. Es ist begrenzt eine politische Frage, in erster Linie handelt es sich um eine wirtschaftliche Frage. Es ist wichtig, dass entsprechende Lösungen geschaffen werden und entsprechende Produkte bereitgestellt werden. Wenn wir z.B. über das Thema Datenschutz und die Datenschutzgrundverordnung reden, haben wir z.B. in Artikel 25 mit Privacy by Design und Privacy by Default gute Grundwerte, um solche technologisch souveränen und datenschutzkonformen Lösungen zu entwickeln. Das kann der Gesetzgeber nicht vorantreiben. Wir bewegen uns trotz aller Regulierung noch in einer sozialen Marktwirtschaft. Deshalb muss geschaut werden, welche Produkte gut sind, also welche Produkte das beste Preis-Leistungsverhältnis bieten. Diese Produkte setzen sich, sofern sie eine gute Usability haben, durch. Wenn diese Produkte US-Produkte sind, dann ist das so. Einerseits ist mir wichtig, dass Unternehmen nicht daran gehindert werden, solche neuen technischen Lösungen zu entwickeln, sondern dass sie darin gefördert und unterstützt werden. Andererseits ist mir das Thema Verbraucherawareness wichtig. Das klingt vielleicht etwas altmodisch, aber die

Verbraucherawareness ist in den letzten Jahren Passwort für alles Mögliche geworden. Meistens kann man, glaube ich, auch nicht so besonders viel damit anfangen. Wenn wir von informationeller Selbstbestimmung reden, dann reden wir auch davon, dass der Verbraucher selbstbestimmt darüber entscheiden kann, was mit seinen Daten geschieht. Das setzt voraus, dass er hinreichend informiert ist. Wenn ich eben sage: „Okay, ich möchte einen Dienst von Microsoft nutzen," kann ich das als Verbraucher auch tun. Das machen sehr viele Verbraucher. Ich muss dann aber akzeptieren, dass mein Kalender, den ich in meinem MS Outlook nutze, im Zweifelsfall möglicherweise eine Zugriffsoption für US-amerikanische Behörden bietet. Ich treffe also eine bestimmte Entscheidung. Ich kann Risiken einschätzen und dann trage ich bestimmte besonders sensible Daten vielleicht nicht in diesen Kalender ein oder verwende Pseudonyme oder Ähnliches. Ich kann es auch im Klartext machen, das ist mir völlig freigestellt. Damit will ich sagen, dass wir als Europäische Union trotz unserer erheblichen politischen und wirtschaftlichen Macht anderen Staaten in der Welt, die natürlich auch starke Verhandlungsposition haben, unsere Gesetzgebung nicht ohne Weiteres aufzwingen können. Das wird meiner Meinung nach nicht funktionieren. Was ich zurzeit mehr und mehr feststelle ist, dass der Gesetzgeber versucht, sämtliche Risiken, die in irgendeiner Weise mit der Digitalisierung zusammenhängen durch Gesetze auf null zu regulieren. Wir hatten eingangs gesagt, dass es ein sehr vielschichtiges Projekt ist. Ein solches Vorgehen ist nicht möglich und auch schädlich, da es Unternehmen und Verbraucher verunsichert und am Ende natürlich eine Menge Geld kostet. Das macht es uns als Juristen einerseits schwer, das Ganze zu durchschauen, andererseits besteht ein höherer Beratungsbedarf. Das ist nicht unbedingt gut. Im Endeffekt haben wir meiner Meinung nach zu viel digitale Gesetzgebung. Es wird immer mehr digitale Gesetzgebung und, weil das Ganze nicht kodifiziert oder in bestimmter Hinsicht systematisiert ist, steigen dem Gesetzgeber irgendwann auch die Unternehmen aufs Dach. Das ist eine zwangsläufige Konsequenz.

Jakob Schüssler: Ich würde gern nochmal einen ganz kleinen Schritt zurückgehen. Du hast gesagt, dass wir es in der Hand haben, ob wir die amerikanischen Produkte benutzen oder auf deutsche Produkte ausweichen. Jetzt könnte man dagegen argumentieren und sagen, Anbieter wie Microsoft sind mittlerweile so mächtig und im Prinzip auf allen Geräten, die wir kaufen, schon so omnipräsent, dass wir gar keine Möglichkeit mehr haben, dagegen zu steuern. Man muss sensible Daten nicht in solchen Kalendern speichern. Aber wenn das beispielsweise in Firmen jeder macht, muss man das mittelfristig doch. Bräuchte man dann nicht doch regulatorische Ansätze durch den deutschen Gesetzgeber, um kleineren Unternehmen, kleineren deutschen Unternehmen die Chance zu geben, gegen diese übermächtigen Anbieter anzukommen? Oder würdest du sagen, das regelt die Marktwirtschaft schließlich von selbst?

Dennis-Kenji Kipker: Ja, das ist sicherlich so. Es braucht einen bestimmten Rahmen an Gesetzen. Das ist klar. Es muss so sein, dass die technologische Souveränität von vielen dieser großen Konzerne, die im Laufe der letzten Jahrzehnte mittlerweile aufgebaut wurde, irgendwo so ein bisschen eingedämmt wird. Das heißt, wir können natürlich nicht in einem völlig rechtsfreien Raum leben und der Marktwirtschaft im Sinne des Sprichwortes „Das Recht des Stärkeren gilt" alles überlassen. Das ist derzeit schon nicht der Fall. Die Europäische Union bringt den digitalen Verbraucherschutz sehr gut voran und hat in den letzten Jahren auch einiges gemacht. Der Digital Service Act wurde schon angesprochen. Ein weiteres Thema ist z.B. der Digital Markets Act. Wir können nicht erzwingen, dass sich bestimmte Unternehmen aus der Europäischen Union durchsetzen, wenn sie schlechtere Produkte anbieten oder Produkte anbieten, die nicht die gleiche Usability oder Funktionalität haben, wie sie bestimmte Produkte aus dem Ausland haben. Man kann Innovation in erster Linie nicht durch Regulierung hervorrufen, sondern Innovation muss aus den Unternehmen selbst kommen. Das hat wieder mit dem Markt zu tun. Man kann den Markt nicht unreguliert lassen. Das hatte ich auch eingangs schon gesagt. Aber man kann nicht oder sollte nicht versuchen, sämtliche Risiken durch Gesetze oder durch die Politik zu regeln.

Karina Filusch: Da wir gerade beim Thema Verbrauchersouveränität sind: Wie erreichen wir diese am besten? Bedarf es vielleicht eines Gütesiegel oder mehr Awareness? Was kann man in dieser Hinsicht vielleicht noch tun, auch als Gesetzgeber oder vielleicht wir selbst als Verbraucherinnen und Verbraucher?

Dennis-Kenji Kipker: Das ist natürlich eine sehr, sehr gute Frage und auch eine sehr wichtige Frage, wo wir eben auch schon so viel über Verbrauchersouveränität gesprochen haben. Allein durch Gütesiegel kann man das, glaube ich, nicht machen. Man bedenke, wie viele Millionen Siegel auf Websites für Urlaubsbuchung oder Online-Shops im Internet kursieren. Es gibt dann hier noch ein TÜV-geprüft-Zeichen und da noch irgendein Siegel mit Sternchen. Siegel mag der Gesetzgeber sehr gerne. Wir haben jetzt z.B. das neue IT-Sicherheitsgesetz 2.0 bekommen. Dazu gehört ein freiwilliges IT-Sicherheitskennzeichen. Dabei handelt es sich nicht um eine Zertifizierung, sondern in erster Linie um ein Gütesiegel, woran der Verbraucher erkennen soll: „Ist das jetzt sicher oder ist es nicht sicher?". Ich glaube, die meisten Verbraucher wissen gar nicht, was hinter so einem Gütesiegel steht. Sehr viele Unternehmen verwenden einen Wald aus Siegeln und dadurch reduziert sich natürlich die Relevanz und Qualität des einzelnen Siegels. In erster Linie geht es tatsächlich darum, dass die Leute sich eben auch bewusst sein müssen, was mit den Daten passiert. Da würde ich nämlich eher

sagen, spielt so ein bisschen der Gesetzgeber mit rein. Gerade, wenn wir über Verbraucherprodukte reden, reden wir eigentlich in den meisten Fällen über Datenschutz und Datensicherheit. Ich vertraue meine personenbezogenen Daten diesen Produkten an und will nicht, dass diese sonst wo landen und, dass sie möglicherweise ins Ausland transferiert werden. Es hat genügend Fälle gegeben, auch beispielsweise von Netzwerkkameras, wo man festgestellt hat, dass der Betreiber oder der Hersteller dieser Netzwerkkamera tatsächlich Zugriff auf die Bilder hatte und dann irgendwie Leute im Schlafzimmer oder in sonstigen höchstpersönlichen Bereichen beobachten konnte, was tatsächlich auch passiert ist. Gerade sowas wollen wir ausschließen, das ist der worst case. Das heißt, wenn ich bestimmte Produkte mit einer bestimmten Anzahl an Sensoren oder Kameras etc. nutze, muss ich mir dessen bewusst sein, dass diese natürlich auch kompromittiert werden können oder sie unsicher sein können. Das ist eigentlich das Bewusstsein, die awareness, also nicht im Sinne von juristischer awareness, sondern einfach nur gesunder Menschenverstand. Ich muss mir eben bewusst sein, dass die Risiken zwangsläufig steigen, je mehr Technologie ich in mein Haus einbringe und je vernetzter das Ganze ist.

Karina Filusch: Ich bin bei deinem Redebeitrag eben innerlich zusammengezuckt, weil ich mich selbst bei sowas erwischt habe. Jetzt hattest du schon vom IT-Sicherheitsgesetz 2.0 gesprochen. Vielleicht können wir nochmal kurz darüber reden. Brauchen wir dieses Gesetz? Was fehlt da? Ist das überhaupt sinnvoll? Wie würdest du das einordnen?

Dennis-Kenji Kipker: Es gibt zwei Sicherheitsgesetze. Das erste IT-Sicherheitsgesetz ist aus 2015 – das ist ein bisschen länger her. Seinerzeit habe ich den Entstehungsprozess verfolgt. Das ist meiner Meinung nach ein handwerklich gutes Gesetz. Es hat viele sinnvolle Regelungen, aber man übertreibt es da auch relativ schnell. Ich habe manchmal den Eindruck, dass sich die Leistungsfähigkeit eines Politikers in einer Legislaturperiode mittlerweile daran bemisst, wie viele Gesetze er zu einem bestimmten Thema gemacht hat. Gerade im digitalpolitischen Bereich werden Probleme einfach mit Gesetzen gelöst – zumindest hört man das oft. So einfach ist es aber nicht. Genauso kann man digitale Souveränität nicht auf einmal durch irgendein Gesetz herstellen. Dasselbe ist gilt für dieses IT-Sicherheitsgesetz 2.0. Davon sind jetzt beispielsweise Unternehmen von besonderem öffentlichen Interesse betroffen, die nicht kritische Infrastrukturen (also Wasserversorger, Energieversorger etc.) sind, aber die darunter fallen. Es ist aber noch völlig unklar, wann ein Unternehmen von besonderem öffentlichem Interesse sein soll. Wahrscheinlich werden auch sehr viele KMU unter diese Regelung fallen, weil auch sogenannte Zuliefererunternehmen von solchen

Unternehmen besonderen öffentlichen Interesse erfasst werden. Wir haben so ein bisschen die Blackbox gekriegt. Weiterhin regelt das Gesetz eine Lieferketten-Regelung bzw. Garantieerklärung für die IT-Sicherheit. Wenn bestimmte Produkte eine kritische Steuerungsfunktion in einer kritischen Infrastruktur wahrnehmen, dann muss irgendwie sichergestellt sein, dass sie IT sicher sind. Das bedeutet, dass es beispielsweise keine externen Kontrollmöglichkeiten gibt, die Hardware sicher ist und so weiter. Man hat auch gesehen, dass der Bedarf dafür besteht. Insbesondere, wenn Mikroelektronik aus Fernost kommt – aus China oder beispielsweise auch aus den USA – muss man sicherstellen, dass diese wirklich zu 100 % sicher ist. Den Unternehmen wird aufgebürdet, einen Lieferkettennachweis und solche Garantieerklärungen zu erbringen, um sicherzustellen, dass diese Produkte IT-sicher sind. Wenn man sich heute vorstellt, wie so ein Produkt eigentlich zustande kommt, muss man sich vor Augen führen, wie komplex das eigentlich ist und was gerade bei eingebetteten Systemen, also embedded systems, an Hardware und Software, Open Source oder an proprietären Produkten mit hineinspielt. Betrachtet man all dies, dann sollte einem schon klar sein, dass das nicht so ohne weiteres möglich ist, obwohl diese Idee erst einmal einleuchtend klingt. Bei den Entscheidungen, ob ein Produkt sicher ist, mischt das Innenministerium wieder stark mit. Das heißt, man hat diese ganze politische Dimension und Überformung. Hier wird eine rein technische Fragestellung am Ende wieder zu einem Politikum gemacht. Das hat natürlich auch zur Folge gehabt, dass man sehr lange über dieses Gesetz diskutiert und debattiert hat oder dies derzeit auch im Hinblick auf das Thema Netzausbau Huawei 5G tut. Das hat dazu geführt, dass sich das ganz erheblich verzögert hat und es nun Regelungen gibt, die meiner Meinung nach nicht nur eine Blackbox sind, weil sie nicht hinreichend konkretisiert sind, sondern gleichzeitig eben auch ziemlich unstrukturiert sind und wieder einen erheblichem Mehrkostenbedarf für Unternehmen schaffen, ohne, dass überhaupt klar ist: „Kann denn das Ziel, was diese Regelung so schön propagiert hat oder was auch Horst Seehofer propagiert hat überhaupt das Ziel erreichen? Oder machen wir uns nicht wieder mehr Aufwand und schaffen mehr Gesetze?“. Nun müssen alle wieder sehr viel machen. Die Anwälte freuen sich, weil sie wieder mehr beraten können. Am Ende jedoch ist dies nicht zielführend. Das ist eine Entwicklung in diesem Bereich der IT-Regulierung, die ich immer öfter sehe und, die ich höchst bedenklich finde.

Karina Filusch: Anknüpfend an das IT-Sicherheitsgesetz. Wie sieht es da so im Vergleich in anderen Staaten aus?

Dennis-Kenji Kipker: Andere Staaten regulieren das Thema. Auch die US-Amerikaner regulieren mittlerweile nicht nur den Datenschutz, sondern auch Cybersecurity. In China

hat es ein prominentes Cyber-Sicherheitsgesetz gegeben, das 2017 in Kraft getreten ist. Dieses betrifft auch hierzulande viele Unternehmen, weil es auch darum geht, ob man exportierte Technologieprodukte überhaupt in China verkaufen kann. In diesem Zusammenhang stellt sich z.B. die Frage, welchen Zertifizierungsvoraussetzungen diese Produkte beispielsweise genügen müssen. Daran sieht man den globalen Trend zu mehr Cybersecurity und mehr gesetzlicher Regulierung in dem Bereich. Dieser Trend führt dazu, dass die Rechtsordnungen ein bisschen miteinander verschmelzen. Ein deutsches Unternehmen kann an den Cybersecurity-Regelungen in China oder in Japan kein Desinteresse mehr zeigen. Die dortigen Regelungen sind von Interesse für sie, da sie ihre Produkte auf dem Markt platzieren wollen. In diesem Zusammenhang geht es nicht nur um Safety – also, dass ich keinen Stromschlag kriege, wenn ich ein Produkt einsetze oder dieses nicht richtig isoliert ist, sondern es geht eben auch um solche Security-Geschichten, also um Software und technische Belange. Grundsätzlich sind wir in diesem Bereich immer gut aufgestellt gewesen. Tatsächlich möchten die Chinesen derzeit ein neues Datenschutzrecht schaffen und dabei sehr viele Prinzipien aus der Datenschutzgrundverordnung übernehmen. Dennoch müssen wir aufpassen, dass wir in diesem globalen Wettlauf um die Gesetzgebung nicht immer mehr Gesetze schaffen und uns dadurch letzten Endes selbst schaden, weil wir eigenen Unternehmen in Deutschland und der Europäische Union viel mehr aufbürden, als es im internationalen Kontext der Fall ist. Dadurch entstehen auch deutliche Mehrkosten, die sich dann vielleicht auch gar nicht in dem Output widerspiegeln, den man sich eigentlich wünscht.

Karina Filusch: Lass uns nochmal zum Hass im Netz zurückkommen. Wir hatten das Thema eingangs schon angerissen. In verschiedenen Ländern gab es hierzu schon verschiedene Regelungen und mittlerweile gibt es eine europäische Regelung. Was denkst du, sind die effektivsten Mittel, um gegen Hass im Netz vorzugehen?

Dennis-Kenji Kipker: Ich glaube, es gibt da nicht die eine Lösung, die nur vorteilhaft ist. Man muss auch hier wieder Interessen in den Einklang bringen. In diesem Zusammenhang wird oft zur Abwägung von Meinungsfreiheit gegen den Schutz von Persönlichkeitsbeeinträchtigungen diskutiert. Man wird sicherlich nicht die perfekte Lösung finden, das ist immer so. Dies wird mir auch im Hinblick auf die derzeitigen Regelungen ersichtlich. Das Netzwerkdurchsetzungsgesetz hat jüngst zwei Novellen erfahren. Es besteht die Tendenz, zu versuchen, eben jedes mögliche Risiko irgendwo zu regulieren. Wie eingangs bereits gesagt, kann ein solches soziales Netzwerk, was auch nicht nur mit Blick auf Beleidigungsdelikte, sondern auch mit Blick auf Desinformation und Datenschutz eine ganz erhebliche Verantwortung hat, natürlich nicht unreguliert bleiben. Man muss schauen, was letztlich praktikabel ist, sodass hier

nicht wieder Regelungen geschaffen werden, die am Ziel vorbeischießen. Das beste Beispiel in dem Zusammenhang ist die sogenannte Login-Falle, die jüngst auf der Innenministerkonferenz beschlossen wurde. Die Login-Falle soll bei Beleidigungsdelikten auf sozialen Netzwerken greifen. Wenn man der Meinung ist, als Nutzer beleidigt worden zu sein oder feststellt, dass andere beleidigt wurden, dann gibt es so eine Art Button, den man dann anklicken kann. Beim nächsten Mal, wenn sich dann der besagte Nutzer, der dieses mögliche Beleidigungsdelikt begangen hat, einwählt, wird seine IP-Adresse erfasst und an Polizeibehörden oder Strafverfolgungsbehörden weitergegeben, die dann über eine Bestandsdatenauskunft beim Provider herausfinden können, wer konkret hinter diesem Nutzer steckt. Sie erhalten den Klarnamen, die Adresse und so weiter hinter dieser IP-Adresse. Das finde ich, ist eine höchst bedenkliche Entwicklung. Menschen haben ein Recht darauf, nicht unbefugt im Netz beleidigt zu werden. Dennoch laufen wir Gefahr, dass dann auch an sich legitime Meinungsäußerungen unterlassen werden, weil man zweifelsfrei davon ausgeht, dass irgendjemand androht, diesen Knopf zu drücken oder tatsächlich diesen Knopf drückt und möglicherweise ein Beleidigungsdelikt geltend gemacht wird. Es gibt berechtigte, hitzige, netzpolitische Diskussionen und die muss es auch geben. Das gehört zum Wesen einer Demokratie hinzu. Führen wir nun eine Art digitales Denunziantentum ein, indem wir auch das wieder überregulieren wollen, dann schaden wir der Meinungsfreiheit mehr, als es eigentlich der Fall sein sollte. Dann ist das Verhältnis zwischen dem Schutz der Persönlichkeit und dem Schutz der Meinungsäußerungsfreiheit (und damit auch mittelbar der Informationsfreiheit) meiner Meinung nach nicht mehr wirklich gegeben.

Karina Filusch: Die Login-Falle löst bei mir Bauchschmerzen aus. Ich habe Angst davor, dass sie dazu führt, dass eine bei einer Behörde konzentrierte Vorratsdatenspeicherung stattfindet. Das ist dieses Buzzword, was wir alle ungern hören. Meiner Meinung nach sollte der Staat sich erst einmal ein bisschen an seine eigene Nase greifen und versuchen dieses Problem zunächst durch Kompetenz und durch Personal zu lösen, anstatt das ständig auf Private überzustülpen, die dann diese Meldepflichten usw. auferlegt bekommen. Wie siehst du das? Wie könnte man das sonst noch lösen?

Dennis-Kenji Kipker: Selbst, wenn es so eine Meldepflicht gibt, also wenn dieser Meldeknopf mittels dieser Login-Falle tatsächlich eingeführt werden sollte, stellt sich auch die Frage bei wem die Daten letzten Endes landen und wie oft dieser Knopf meinetwegen deutschlandweit gedrückt wird. Einmal in einer Stunde, am Tag oder in einer Woche? Wer soll das Ganze auswerten? Bevor man überhaupt darüber nachdenkt, jetzt wieder mehr Kompetenzen, Behörden, Schwerpunkte und Staatsanwaltschaften

oder Ähnliches zu schaffen, sollte man überlegen, was man letztlich durch das ganze Thema erreichen will. Ferner sollte man bedenken, wie viele Ressourcen man effektiv für die vernünftige Erreichung des festgeschriebenen Ziels brauchen würde. Da genügt es meiner Meinung nach nicht, wenn man dann 20 oder 30 Polizisten darauf abstellt, die das dann überwachen. Man muss schließlich auch davon ausgehen, dass dieser Knopf missbräuchlich betätigt wird. Jeder von uns hat auch eine andere Schwelle, ab wann er sich vielleicht mal persönlich angegriffen fühlt. Den einen kann man im Netz beleidigen, wie man will und das interessiert den überhaupt nicht, währenddessen ein anderer dann vielleicht schon sagt, dass etwas für ihn die Grenze zur Beleidigung überschreitet, wenn jemand etwas schreibt, was ihm einfach nicht gefällt. Wir alle leben in einer gewissen Risikosphäre und ich finde dieser Gedanke geht irgendwie verloren. Wir alle gehen Risiken ein. Wir gehen das Risiko ein, dass wir vom Auto überfahren werden. Wir gehen das Risiko ein, etwas zu kaufen, was möglicherweise viel zu teuer oder schädlich für unsere Gesundheit ist. Das sind alles Risiken, die wir eingehen. Auch im Online-Bereich gibt es solche Risiken. Wenn wir irgendwo interagieren und wenn wir uns an Diskursen beteiligen, können wir sehen, um was für eine Art von Diskurs es geht. So müssen wir abschätzen, ob diese einen gewissen Sprengstoff haben, sodass es da vielleicht tatsächlich auch zum Shitstorm kommen kann. Wenn ich z.B. eine öffentliche Podiumsdiskussion völlig analog mache, gibt es auch Leute, die ihr Missfallen lautstark zum Ausdruck bringen. Das kann man am besten bei Politikern beobachten. Diese gehen sich den ganzen Tag über an, auch in Talkshows. Wenn man sich in eine bestimmte Risikosphäre begibt, muss man auch damit rechnen, dass es in einem gewissen Maße auch zu einer Realisierung von Risiken kommt. Es ist nicht allein die Aufgabe des Gesetzgebers, sich darum zu kümmern, sondern natürlich auch desjenigen, der sich an diesen Diskursen beteiligt.

Jakob Schüssler: Um nochmal kurz auf die Login-Fallen zurückzukommen: Es ließe sich immer argumentieren, dass diejenigen, die wissen, dass sie z.B. Straftaten im Netz begehen, zumeist VPN verwenden oder auf anderem Wege ihre eigentliche IP-Adresse verbergen. Das ist zunehmend auch mit weniger Aufwand oder technischer Kenntnis möglich. Selbst Apple hat in die aktuellen Betas einen eigenen VPN implementiert, der standardmäßig aktiviert ist. Angesichts der daraus resultierenden Problematik des Wertes von IP-Adressen, wenn diese beispielsweise durch ein VPN gewissermaßen verfälscht werden, frage ich mich: Wie erfolgsversprechend sind die Login-Fallen denn wirklich? Gerade unter dem Gesichtspunkt trifft es die Richtigen? Ergeben Login-Fallen als geistiger Ausfluss des Gesetzgebers deines Erachtens überhaupt Sinn?

Dennis-Kenji Kipker: Das ist ein wichtiger Punkt. Den hat die IMK, also die

Innenministerkonferenz tatsächlich überhaupt nicht berücksichtigt. Ich glaube, der wird auch in dem Lösungsvorschlag dieser Login-Falle gar nicht thematisiert. Man geht eben davon aus, dass man mit der IP-Adresse auch immer an diejenige Person herankommt, die dahintersteht. Aber das ist genau, was ich meine. Die Idee klingt erst mal gut, ganz interessant, umsetzbar und wertvoll, weil sie in gewisser Hinsicht Grundrechte schützt. Über die Umsetzung hingegen macht man sich wenige Gedanken.

Karina Filusch: Wir sind heute richtig politisch. Das gefällt mir. In Anbetracht der bevorstehenden Bundestagswahl finde ich das auch richtig gut. Eine Frage wird auch zunehmend mehr diskutiert und wird auch regelmäßig auf der Bundespressekonferenz gefragt, und zwar die Frage nach einem Digitalministerium. Brauchen wir das oder kann das weg?

Dennis-Kenji Kipker: Ich würde sagen, es kann weg. Also, wenn es da wäre. Man muss sich überlegen, was bislang unter Dorothee Bär als Digitalstaatsministerin passiert ist. Ich glaube, das kann niemand so richtig beantworten. Man muss ihr natürlich zugutehalten, dass sie nicht wirklich Befugnisse hat. Aber kann damit so eine Position nicht generell wegfallen? Das ist die erste Frage und die zweite Frage, die man sich stellen muss, ist: Muss diese Position ausgeweitet werden, um mehr Sinn zu ergeben? Die Aussage hinter einem Digitalministerium ist ja, diese ganzen Ressorts, in denen digitalpolitische Themen oder Fragestellungen anfallen in einem Ministerium zusammenzufassen. In diesem Ministerium soll das alles bewertet werden und es soll die erste Anlaufstelle sein. Zudem soll das dann in die anderen Ressorts der Bundesregierung weitergegeben werden. Wenn man einen Blick auf die politische Meinung wirft, wird man feststellen können, dass viele sagen: „Ja, wir brauchen ein Digitalministerium." Ich glaube, dass bislang noch keiner den konkreten Nutzen eines solchen Digitalministeriums formuliert hat. Wenn gar nicht so richtig klar ist, was man damit erzielen will, dann kann man sich diesen Aufwand von vornherein sparen. Des Weiteren fragt sich: Was soll denn dieses Digital- oder Zukunftsministerium genau koordinieren, wenn die Themen für die eigentliche Entscheidung doch wieder in die Fachressorts zurückgeführt werden sollen? Meines Erachtens ist dieses Digitalministerium ein Feigenblatt dafür, dass man Digitalpolitik den letzten Jahrzehnten sehr stiefmütterlich betrieben hat und, dass man sich jetzt auf die Fahnen schreiben möchte: „Ja, mit einem Digitalministerium haben wir ein wichtiges Thema. Das verfolgen wir jetzt auch und damit zeigen wir, dass wir es verfolgen." Die nächste Frage, die sich stellt, ist: Woher bekommen wir die ganzen Experten, die in einem Digitalministerium, was relativ zügig arbeitsfähig sein muss, die entsprechenden Entscheidungen treffen sollen? Fragen über Fragen. Der Punkt ist tatsächlich: Wie

sinnvoll ist das wirklich in der Praxis? Das ist wieder so ein bisschen wie mit den gesetzlichen Regelungen. Es handelt sich um gute Ideen, aber ich sehe es eben nicht ein, dass Unternehmen darunter leiden, dass der Verbraucher darunter leidet, dass jetzt auch der Steuerzahler darunter leidet und dass immer mehr Verwaltungsapparate für alles Mögliche geschaffen werden, nur damit man das Thema offiziell behandeln kann. Dafür habe ich mittlerweile kein Verständnis mehr. Deswegen muss ich auch ganz klar sagen, dass die Idee eines Digitalministerium, so wie es zurzeit geschildert wird, zu verwerfen ist.

Karina Filusch: Leider sind wir schon am Ende unseres Podcasts, was total schade ist. Ich könnte noch stundenlang mit dir quatschen. Deshalb stelle ich dir jetzt die Frage, die wir allen unseren Gästen stellen. Was ist denn DaSou für dich?

Dennis-Kenji Kipker: Für mich ist DaSou, dass die Verbraucher noch besser als bisher dazu befähigt werden, für sich selbst zu entscheiden, was in Digitalisierungshinsicht für sie gut ist und was für sie schlecht ist. DaSou bedeutet für mich, dass die informationelle Selbstbestimmung, wenn wir von Datenschutz reden, eben nicht nur ein Thema ist, dass durchgeklickt wird, sondern, dass es tatsächlich irgendwo Relevanz besitzt. Datensouveränität bedeutet nicht hundertprozentige Kontrolle, sondern Kontrolle in dem Risikorahmen, in dem ich mich bewege. Das ist letzten Endes selbstbestimmtes Entscheiden. Jede Entscheidung im Leben ist mit irgendwelchen Konsequenzen bzw. mit irgendwelchen Risiken verbunden. Das bezieht sich auch auf Digitalisierung, auf IT, auf Datenschutz und auf Cybersicherheit. Ich wünsche mir, dass dieses Verständnis beim Verbraucher und insbesondere auch beim Politiker wächst.

Karina Filusch: Das klingt nach einem schönen Appell. Liebe Politikerinnen, liebe Politiker hört uns aufmerksam zu und werdet ein bisschen besser darin. Das wäre sehr wünschenswert, dass das auch in Zukunft passiert. Ja, lieber Dennis, ich danke dir ganz herzlich dafür, dass du dir so viel Zeit genommen hast. Du hast so viel zu tun und trotzdem hast du Zeit gefunden, mit uns zu sprechen. Ganz, ganz herzlichen Dank.

Dennis-Kenji Kipker: Ich kann den Dank nur zurückgeben. Vielen Dank für das schöne Gespräch und für die Einladung, heute dabei sein zu können.

Karina Filusch: Diese Folge fand ich sehr spannend, weil sie ausnahmsweise sehr politisch war. In Anbetracht dessen, dass die Wahlen kurz bevorstehen, können wir uns

jetzt auf jeden Fall einen guten Überblick über das verschaffen, was in den vergangenen Jahren im Bereich Digitalpolitik geschehen ist.

Jakob Schüssler: Insbesondere die Forderung nach einem Digitalministerium kommt mittlerweile von vielen Seiten – sowohl aus der Politik, aber auch von Verbänden und Branchen. Ich glaube, dass in diesem Bereich auf jeden Fall etwas passieren wird. Mal schauen, wie die Ausgestaltung dann aussehen wird. Gegebenenfalls ist diese dann auch abhängig von den neuen Regierungsparteien.

Karina Filusch: Am 26. September sind die Wahlen. Dann können wir als Wählerinnen und Wähler darüber entscheiden, wie es weitergehen soll, auch im Bereich der Digitalpolitik. Wir haben eine Folge dazu vorbereitet, in der wir die Wahlprogramme im Bereich vom Datenschutz und der Digitalpolitik zusammen mit unserem Gast analysieren.

Jakob Schüssler: Wenn es euch gefallen hat, dann hört doch gerne beim nächsten Mal wieder rein und abonniert den Podcast, damit ihr dabei seid, wenn wir wieder über Datensouveränität sprechen. Habt ihr Fragen zu DaSou? Dann schickt uns gerne eine Mail an hallo@dasou.law oder eine Nachricht über Twitter oder Instagram.

Karina Filusch: Danke fürs Zuhören und bis zum nächsten Mal.

Jakob Schüssler: Bis zum nächsten Mal.

Karina Filusch: DaSou ist eine Produktion der Kanzlei Filusch. Mehr Infos findet ihr auf unserer Webseite dasou.law. Der Jingle wurde komponiert von Mauli. Die Idee zu DaSou hatte Axel Jürs. Das Cover hat Hélène Baum erstellt. Beraten wurden wir von Susan Stone. Editiert wurde der Podcast von Christoph Hinners.