20. Wahlperiode

Deutscher Bundestag
Rechtsausschuss

Wortprotokoll
der 68. – öffentlichen – Sitzung*

Rechtsausschuss
Berlin, den 11. Oktober 2023, 12:01 Uhr
Berlin, Paul-Löbe-Haus, Saal 2.600

Vorsitz: Elisabeth Winkelmeier-Becker, MdB

Tagesordnung - Öffentliche Anhörung

Einziger Tagesordnungspunkt **Seite 7**

Antrag der Fraktion der CDU/CSU

IP-Adressen rechtssicher speichern und Kinder vor sexuellem Missbrauch schützen

BT-Drucksache 20/3687

Federführend:
Rechtsausschuss

Mitberatend:
Ausschuss für Inneres und Heimat
Wirtschaftsausschuss
Ausschuss für Familie, Senioren, Frauen und Jugend
Ausschuss für Digitales

Berichterstatter/in:
Abg. Sebastian Fiedler [SPD]
Abg. Dr. Volker Ullrich [CDU/CSU]
Abg. Helge Limburg [BÜNDNIS 90/DIE GRÜNEN]
Abg. Dr. Thorsten Lieb [FDP]
Abg. Fabian Jacobi [AfD]
Abg. Clara Bünger [DIE LINKE.]

* Dieses Wortprotokoll wurde auf Grundlage automatischer Transkription erstellt und summarisch durch das Sekretariat überprüft. Für den exakten Wortlaut wird auf die Videoaufzeichnung der öffentlichen Anhörung verwiesen, die in voller Länge über die Mediathek des Deutschen Bundestages unter www.bundestag.de/mediathek/ausschusssitzungen abrufbar ist.

Mitglieder des Ausschusses

	Ordentliche Mitglieder	Unterschrift	Stellvertretende Mitglieder	Unterschrift
SPD	Dilcher, Esther	☐	Dieren, Jan	☐
	Eichwede, Sonja	☐	Döring, Felix	☐
	Fechner, Dr. Johannes	☐	Echeverria, Axel	☐
	Fiedler, Sebastian	☒	Esken, Saskia	☐
	Karaahmetoğlu, Macit	☐	Müller, Bettina	☐
	Licina-Bode, Luiza	☐	Roloff, Sebastian	☐
	Limbacher, Esra	☐	Scheer, Dr. Nina	☐
	Mansoori, Kaweh	☐	Schieder, Marianne	☐
	Martens, Dr. Zanda	☐	Schisanowski, Timo	☐
	Plobner, Jan	☐	Wiese, Dirk	☐
	Wegge, Carmen	☒		
CDU/CSU	Heveling, Ansgar	☒	Amthor, Philipp	☐
	Hierl, Susanne	☒	Gutting, Olav	☐
	Jung, Ingmar	☒	Hoffmann, Alexander	☐
	Krings, Dr. Günter	☒	Hoppenstedt, Dr. Hendrik	☐
	Mayer (Altötting), Stephan	☒		
	Müller, Axel	☒	Lehrieder, Paul	☐
	Müller (Braunschweig), Carsten	☒	Lindholz, Andrea	☐
			Luczak, Dr. Jan-Marco	☐
	Oellers, Wilfried	☒	Santos Wintz, Catarina dos	☐
	Plum, Dr. Martin	☒		
	Ullrich, Dr. Volker	☒	Thies, Hans-Jürgen	☐
	Winkelmeier-Becker, Elisabeth	☒	Warken, Nina	☐
			Weiss, Maria-Lena	☐
BÜNDNIS 90/DIE GRÜNEN	Bayram, Canan	☐	Aeffner, Stephanie	☐
	Benner, Lukas	☐	Beck, Katharina	☐
	Limburg, Helge	☒	Künast, Renate	☐
	Rottmann, Manuela, Dr.	☐	Notz, Dr. Konstantin von	☐
	Steffen, Dr. Till	☐	Schönberger, Marlene	☐
	Tesfaiesus, Awet	☐	Steinmüller, Hanna	☐
FDP	Fricke, Otto	☐	Kubicki, Wolfgang	☐
	Hartewig, Philipp	☐	Kuhle, Konstantin	☐
	Helling-Plahr, Katrin	☐	Schröder, Ria	☐
	Lieb, Dr. Thorsten	☒	Skudelny, Judith	☐
	Willkomm, Katharina	☒	Thomae, Stephan	☐
AfD	Brandner, Stephan	☐	Beckamp, Roger	☐
	Jacobi, Fabian	☒	Haug, Jochen	☐
	Peterka, Tobias Matthias	☐	Wirth, Dr. Christian	☐
	Seitz, Thomas	☐		☐

	Ordentliche Mitglieder	Unterschrift	Stellvertretende Mitglieder	Unterschrift
DIE LINKE.	Bünger, Clara	☐	Mohamed Ali, Amira	☐
	Hennig-Wellsow, Susanne	☐	Domscheit-Berg, Anke	☒

Weitere Mitglieder des Deutschen Bundestages

		Unterschrift
SPD	Baldy, Daniel	☒
CDU/CSU	Henrichmann, Marc	☒
FDP	Adler, Katja	☒
AfD	Benkstein, Barbara	☒

Sprechregister Abgeordnete

Sprechregister Sachverständige

Die Vorsitzende **Elisabeth Winkelmeier-Becker**: Seien Sie alle herzlich gegrüßt zur 68. Sitzung des Rechtsausschusses. Ich begrüße vor allem die Abgeordneten im Saal und die Sachverständigen hier im Saal überwiegend, aber auch teilweise zugeschaltet. Wir haben dann als Vertreterin der Bundesregierung Frau Abteilungsleiterin Dr. Neuhaus mit ihrem Team. Sind Sie herzlich willkommen und wir haben Zuhörer und Zuhörerinnen auf der Tribüne . Gegenstand der heutigen Sitzung ist der Antrag der Fraktion der CDU/CSU zur rechtsicheren Speicherung von IP-Adressen. Die Fraktion führt aus, dass die Digitalisierung den sexuellen Kindesmissbrauch auf eine neue Stufe gehoben hat, nämlich die Veröffentlichung von entsprechenden Fotos und Videos im Internet, die ein erschreckendes Ausmaß angenommen haben.Zugleich sieht die Fraktion ein Aufklärungsdefizit in Deutschland, weil die zur Ermittlung der Täter notwendigen Daten nicht bzw. nicht lang genug gespeichert würden. Hier geht es um die IP-Adressen, die auf inkriminierten Seiten aufgefallen sind und gemeldet werden und dann nicht mehr zugeordnet werden können. Nach Forderung der Fraktion soll der vom Europäischen Gerichtshof eingeräumte gesetzgeberische Spielraum genutzt und insbesondere eine sechsmonatige Speicherverpflichtung von IP-Adressen vorgesehen werden. Das ist grob das, worum es geht in dem Antrag, zu dem wir heute die Sachverständigenanhörung durchführen.

Vorweg einige Hinweise zum Ablauf: Die Sachverständigen erhalten als erstes die Gelegenheit zu einem vierminütigen Statement. Wir beginnen alphabetisch bei Herrn Danisch, der zugeschaltet ist. Die roten Namensschilder deuten darauf hin, dass die Sachverständigen zugeschaltet sind, und dann geht es alphabetisch der Reihe nach rum. Wir haben eine Uhr, die auf dem Bildschirm rückwärtsläuft. Wenn die also bei null und darüber hinaus im roten Bereich ist, dann müssen Sie dringend zum Ende kommen. Besser wäre vorher. Dann gibt es eine Fragerunde, eine erste Fragerunde, die läuft bei uns so ab, dass die Kolleginnen und Kollegen in jeder Fragerunde höchstens zwei Fragen an bis zu zwei Sachverständige stellen können. Und mit der Bitte vielleicht den Wunsch, auch hier schon per Handzeichen anzukündigen. Ich habe schon eins gesehen. Wir führen die Liste der Meldungen. Und weil wir hier auch viele dabeihaben, möglichst konkret und präzise die Fragen stellen, damit wir da nicht viel Zeit verlieren. Wenn es dann in die Antwortrunde geht, dann geht es in umgekehrter alphabetischer Reihenfolge. Also, in der ersten Fragerunde würde Professor Wollenschläger mit der Antwort beginnen und richten Sie sich bitte, liebe Sachverständige, daran aus, maximal zwei Minuten je Frage, die an Sie gestellt ist, zu antworten. Das ist jedenfalls mal das Zeitkontingent, mit dem wir starten, wenn wir merken, dass wir zu viele Fragen haben, dann wird das vielleicht auch noch mal verkürzt. Also, wenn wir dann Zeit haben, gibt es noch eine zweite Fragerunde, dann geht es wieder in der Reihenfolge und bei der dritten einer möglichen dritten wieder andersrum.

Dann möchte ich noch eine Besonderheit ankündigen: Wir haben alle die Nachrichten über die Terrorangriffe der Hamas auf Israel zur Kenntnis genommen und dazu wird es eine Gedenkminute geben. Um 13:00 Uhr wird die Bundestagspräsidentin hiermit das Plenum eröffnen und wir haben vorher besprochen, dass wir dazu gerne die Sitzung hier ein paar Minuten unterbrechen möchten. 15 Minuten, 20 Minuten wird uns das Kosten, damit wir auch daran teilnehmen können. Und wir würden die Zeit dann hinten dranhängen. Es geht also nicht auf Kosten der Beratungen, aber ich würde Sie bitten, dafür Verständnis zu haben. Auch diejenigen, die uns vielleicht zuschauen und die Zeit dann hinten dranzuhängen und für uns dann auch darüber hinaus da zu sein. Insgesamt wird das schätzungsweise etwa 20 Minuten kosten, gilt für die Regierungsseite auch. Ja, gut.

Dann noch der Hinweis: Diese Anhörung ist öffentlich und wird live im Parlamentsfernsehen sowie auf der Website des Bundestages übertragen. Anschließend gibt es eine Aufzeichnung in der Mediathek des Bundestages, auch abrufbar. Und wir fertigen natürlich auch ein Wortprotokoll an.

An die Zuhörerinnen und Zuhörer auf der Tribüne: Wir freuen uns, dass Sie da sind und sich für unsere Beratungen interessieren. Ich muss aber immer standard-mäßig darauf aufmerksam machen, dass Bild- und Tonaufnahmen nicht gestattet werden. Auch Beifalls- und erst recht Missfallensbekundungen

wollen wir hier nicht hören, sondern jetzt steht ganz die Sache im Vordergrund und unsere Beratungen hier. In diesem Sinne erst mal danke für die Aufmerksamkeit und wir starten mit dem Eingangsstatement von Herrn Danisch.

Herr Danisch, Sie haben das Wort und ich muss noch sagen, es gibt ein technisches Problem mit der Uhr. Also zur Not greife ich jetzt zur Glocke und dann wissen Sie auch, dass die Zeit abgelaufen ist. Jetzt haben Sie das Wort, Herr Danisch.

SV **Hadmut Danisch**: Ja, Frau Präsidentin! Sehr geehrte Damen und Herren! Vielen Dank. Ich möchte zunächst mal darstellen, dass ich meine Schätzung abgebe. Ich bin als Informatiker, seit es das Internet gibt, tätig. Ich war bei mehreren Internet-Providern, davon drei Jahre in der Rechtsabteilung eines großen deutschen Internet-Providers, 2009 habe ich ein Jahr lang die Vorratsdatenspeicherung dort geleitet, knapp 2000 Fälle bearbeitet. Verfüge also insofern über praktische Erfahrung und war auch im Jahr 2009 im Bundestag und beim Bundeskriminalamt in die damalige Sache Kinderpornos involviert, habe also große berufliche Erfahrung und bearbeite solche Themen auch seit über zehn Jahren. Was mir zunächst auffällt, ist, dass im Antrag verschiedene Fehler sind. Das geht einmal um die Sache mit der Portspeicherung. Da merkt man, dass da verschiedene Sachen nicht verstanden sind.

Die **Vorsitzende**: Ja, Herr Danisch, wir haben hier wirklich Übertragungsprobleme und ich muss jetzt noch mal gerade die Vorschläge hören, wie wir das beheben sollen, Herr Limburg.

Abg. **Helge Limburg** (BÜNDNIS 90/DIE GRÜNEN): Mein Vorschlag wäre, dass wir zunächst mit einem Sachverständigen aus dem Raum weitermachen und in der Zeit versuchen, es zu beheben.

Die **Vorsitzende**: Bild oder Ton?

Abg. **Helge Limburg** (BÜNDNIS 90/DIE GRÜNEN): Ich finde es gerade wirklich schwer.

Die **Vorsitzende**: Der Ton ist immer wieder unterbrochen. Vielleicht wird es auch besser, wenn wir sie nur hören. Haben wir eine Chance, hier die Technik, die Möglichkeit, das Problem einzukreisen und zu beheben? Gut, dann stellen wir Sie gerade einen Moment zurück. Sie können gleich noch mal neu starten. Und damit wir das gleiche Problem nicht mit Frau Hackenbroch haben, beginnen wir dann hier mit Herrn Hiéramente.

SV **Dr. Mayeul Hiéramente**: Sehr geehrte Abgeordnete, vielen Dank für die Möglichkeit, hier sprechen zu können. Ich spreche hier im Namen des Deutschen Anwaltsvereins, der mir dankenswerterweise die Einladung weitergeleitet hat. Vielleicht kurz ein paar Worte vorab, damit wir wissen, worüber wir sprechen.

Zur Bedeutung der Vorratsdatenspeicherung bezüglich IP-Adressen. Es wäre eine Maßnahme, die sämtliche Bürgerinnen und Bürger betrifft, da keine Speicherung bezüglich eines konkreten Anlasses erfolgt, sondern eine anlasslose Speicherung. Ermöglichen tut dies unter anderem eine umfassende Nachverfolgung der vom Internetnutzer besuchten Internetseiten. Das ist nicht meine Formulierung, das schreibt der EuGH. Also, um das mal plastisch darzustellen: Es ermöglicht nachzuvollziehen, welche Internetseiten ein Nutzer besucht. Damit kann man rausfinden, politische Interessen zum Beispiel, sexuelle Vorlieben, Krankheiten oder ähnliches, wenn man das denn für diese Suche nutzen würde. Selbstverständlich können Mobiltelefone und Computer auch zur Begehung von Straftaten genutzt werden. Das ist, glaube ich, evident. Aber vor allem kriminelle Nutzer können ihre Identität verschleiern. Das ist einmal technisch möglich, aber auch ganz banal, indem sie einen Anschluss nutzen, der nicht der ihrige ist. Dementsprechend bei Nutzung eines offenen WLAN, Hotspots oder ähnlichem. Das heißt, wir sprechen über eine Maßnahme, die viele Personen betrifft und möglicherweise oder jedenfalls nicht alle kriminellen Nutzer erfasst. Eindeutig ist aber auch, dass selbst bei besonders kriminellen Nutzern auch dort eine Klar-IP festgestellt werden kann und dass bestimmte, zum Beispiel Kenntnisse von einem bestimmten Server, der zur Verbreitung von Kinderpornografie genutzt wurde, wenn man denen als Ermittlungsbehörde davon Kenntnis erlangt, dass man da selbstverständlich auch in Einzelfällen auch Klar-IP ermitteln kann. Das heißt, man hat

eine Maßnahme, die durchaus aus meiner Sicht geeignet ist. Allerdings, die Frage stellt sich, ob eine solche anlasslose Sicherung vertretbar und rechtspolitisch gewollt ist. Der DHV, das ist ganz klar und das haben wir auch mittels einer Stellungnahme schon mehrfach artikuliert, bevorzugt eine anlassbezogene Sicherung von Daten, jetzt bekannt unter dem Schlagwort Quick Freeze. Quick Freeze hat den Vorteil, dass es eine rechtssichere Lösung ist, europarechtlich ist sie unbedenklich und sie wäre dementsprechend bei Verabschiedung kurzfristig einsetzbar. Die Schaffung einer potenziell rechtswidrigen Lösung könnte allerdings dazu führen, dass faktisch über Jahre hinweg Ermittlerinnen und Ermittler eben keine geeignete Maßnahme zur Verfügung steht, weil diese möglicherweise durch die oder die Speicherpflicht ausgesetzt wird und eine Klärung des EuGHs erfolgen muss. Aus diesem Grund vertritt der DAV die Rechtsansicht, dass eine Pflicht zur Speicherung, da diese rechtlich problematisch oder europarechtswidrig ist, nicht zu bevorzugen ist. Ichkann gleich bei der Fragerunde gerne noch darauf eingehen. Damit das Risiko einhergeht, dass diese gekippt werden wird und den Ermittlern nicht geholfen ist. Wir bevorzugen eindeutig eine anlassbezogene Sicherung, da wir in Europa eine sechs Monats Frist für europarechtswidrig halten. Danke schön.

Die **Vorsitzende**: Vielen Dank, Herr Hiéramente. Dann kommen wir noch einmal zurück zu Herrn Danisch und die Technik sagt uns, dass Sie am besten den Hintergrund abschalten und möglicherweise auch das Video insgesamt abschalten, damit wir hier die Hoffnung haben, eine ungestörte Verbindung zu haben. Ja, dann starten Sie jetzt noch mal.

SV **Hadmut Danisch**: Können Sie mich jetzt hören? Kurze Anmerkung: Ich bin gerade auf Zypern, das ist im Mittelmeer und ich habe heute Morgen hier schon ungewöhnliche Flugbewegungen beobachtet und gehört. Die Störung könnten also auch kriegsbedingt sein. Ja, im Antrag habe ich bereits verschiedene Fehler entdeckt, nämlich, dass man die Sache mit der Portspeicherung *[unverständlich]* und nicht gemerkt hat, dass im Gegensatz zum Internet diese Ports nur für Millisekunden oder kurze, sehr kurze Zeit *[unverständlich]* kleine Uhren hat, die genau genug gehen und das ein Eingriff ins Post- und Fernmeldegeheimnis ist. Und *[unverständlich]* Rechtsicherung Speicherung muss, ich sagen, es gibt im Internet keine Rechtssicherheit, weil das Internet nie dazu spezifiziert oder gebaut war. Also diese Rechtssicherheit, die gibt es gar nicht. Maßstab ist hier das Urteil des EuGH, in dem ganz am Ende des Urteilstextes im Absatz steht, dass eben klare und präzise Regeln sicherstellen müssen. Und weil das die materiellen und prozeduralen Voraussetzungen sind und ein Schutz vor Missbrauch besteht. Nach meiner Feststellung und Einschätzung ist Deutschland derzeit nicht in der Lage, diese Anforderungen des Europäischen Gerichtshofs zu erfüllen. Wir haben zwar entsprechende Verbrecher und Verbrechen, aber unsere drei Staatsgewalten sind nicht in der Lage und nicht in einem Zustand, diese Anforderungen zu erfüllen. Wir haben derzeit einen massiven Missbrauch, auch auf Seite der Polizei. Polizei, Staatsanwaltschaft, Strafverfolgung sind eindeutig politisch infiltriert und nach meiner Einschätzung ist die Kinderpornografie hier in dem Fall auch nur eine Art Vorwand, um andere Abfragen *[unverständlich]*. Ich komme deshalb zu dem Ergebnis, dass der Antrag und die Vorratsdatenspeicherung derzeit in Europa vor dem Europäischen Gerichtshof nicht als jeder der genug Insiderkenntnis hat und genug Wissen hat davon, was vor sich geht, in der Lage ist, eine Vorratsdatenspeicherung ohne Weiteres wegzuklagen. Die weiteren Details finden Sie dann in meiner Ausarbeitung, die Ihnen ja zugegangen ist. Und ich hoffe, dass man mich jetzt verstanden hat.

Die **Vorsitzende**: Vielen Dank, Herr Danisch. Es gab schon mal kurze Aussetzer. Das war nicht optimal, aber ich denke dann auch im Kontext mit Ihrer schriftlichen Stellungnahme ist schon verstanden worden, was Sie uns mitteilen wollten. Vielen Dank. Bei uns geht es dann weiter mit der Sachverständigen Marina Hackenbroch vom Bund Deutscher Kriminalbeamter. Guten Morgen! Die Leitung steht? Ja, wunderbar. Können Sie mich hören?

SVe **Marina Hackenbroch:** Ja.

Die **Vorsitzende**: Wunderbar, Sie haben das Wort. Wir hören Sie hervorragend. Vielen Dank.

SVe **Marina Hackenbroch:** Sehr geehrte Frau Vorsitzende, sehr geehrte Abgeordnete, sehr geehrte Damen und Herren! Hallo nach Berlin und vielen Dank für die Einladung zur heutigen Anhörung. Ich möchte Sie kurz bitten, sich vor allem einen Sachverhalt vorzustellen. Wir haben eine Plattform im Darknet, die ausschließlich zur Verbreitung von Missbrauchsdarstellungen von Kindern und Jugendlichen genutzt wird. Diese Plattform hat mehr als 60.000 Nutzer und im Rahmen einer international organisierten Operation gelingt es eben IP-Adressen von Nutzern dieser Plattform sicherzustellen. 200 dieser IP-Adressen weisen einen Deutschlandbezug auf, weshalb diese IP-Adressen dann an das BKA übermittelt werden. Leider waren die IP-Adressen aber bei Übermittlung dann schon mehrere Monate alt, sodass wir eben keine Abfrage mehr bei den Providern machen konnten und keine Zuordnung mehr zu Anschlüssen erfolgen konnte. Andere Ermittlungsansätze gab es nicht oder liefen trotz aller Bemühungen ins Leere und letztendlich wurde dadurch dann kein einziger der knapp 200 vermutlich deutschen Nutzer identifiziert. Andere Länder hingegen können Administratoren und Abonnenten der Plattform identifizieren und können sogar Missbraucher feststellen, sodass Menschen, oder Kinder aus Missbrauchssituationen gerettet werden können und konnten. Das alles ist genauso passiert im Rahmen der Operation Black Forest im Jahr 2018. Und ich denke, Ihnen ist klar, worauf ich hier hinaus möchte. Hätten wir Mindestspeicherfristen von IP-Adressen gehabt, hätten wir die Anschlüsse zuordnen können oder zumindest weitere Ermittlungsansätze generieren können. Und das ist jetzt nur ein Beispiel für gescheiterte Ermittlungen aufgrund des Fehlens von Speicherverpflichtungen von IP-Adressen. In dem jetzt gerade von mir dargestellten Fall ging es um Abonnenten einer Plattform, das heißt um die Verbreitung von Missbrauchsdarstellungen. In anderen Ermittlungsverfahren kann es aber auch um Missbraucher gehen, die ebenfalls nicht ermittelt werden können und wir dadurch andauernden Missbrauch nicht unterbinden können. Wir hören immer wieder den Vorwurf, dass wir die Diskussion um die Mindestspeicherfristen von IP-Adressen durch den Verweis auf eben diesen Phänomenbereich künstlich dramatisieren würden. Meine Damen und Herren, ich kann Ihnen als Polizistin sagen, dass es nach meinem ganz persönlichen Empfinden nur wenig Deliktsbereiche gibt, die vergleichbar schrecklich sind. Was aus fachlicher Sicht aber wirklich dramatisch ist, ist meines Erachtens, dass die vom EuGH eingeräumten Möglichkeiten nicht ergriffen werden und wir aus diesem Grund nicht selten nur wirklich langwierige und häufig auch eben nicht erfolgreiche Ermittlungen führen können und deshalb eben teilweise schwerer sexueller Missbrauch nicht unterbunden wird. Jetzt mal abgesehen vom andauernden Leid der Opfer ist für Außenstehende, glaube ich, schwer nachvollziehbar, wie frustrierend das für Polizistinnen und Polizisten ist, die in diesem ohnehin schon extrem belastenden Bereich arbeiten. Darüber hinaus verlieren wir als deutsche Strafverfolgungsbehörden aber auch im internationalen Kontext zunehmend an Ansehen, wenn wir übermittelte Daten immer wieder nicht nutzen können. Das mag jetzt erst mal trivial klingen, aber ich kann Ihnen sagen, dass das alles andere als trivial ist. Wenn ausländische Partnerbehörden IP-Adressen übermitteln und wir als deutsche Strafverfolgungsbehörden immer und immer wieder sagen müssen, dass wir leider keine Informationen mehr dazu haben. Für eine effektive Bekämpfung von Kriminalität, die über das Internet begangen wird, sind wir aber häufig auf internationale Zusammenarbeit angewiesen und diese fehlenden Regelungen erschweren diese Zusammenarbeit zunehmend. Quick Freeze bringt in solchen Fällen, wie ich Ihnen gerade geschildert habe, leider rein gar nichts. Es gibt Fallkonstellationen, in denen Quick Freeze sinnvoll ist. Aber um Daten einzufrieren müssen auch Daten da sein. Und wir müssen zeitnah von Sachverhalt wissen, Kenntnis erlangen. Und das ist leider eben nicht immer der Fall. Immer dann, wenn wir unbekannte Tatverdächtige über das Internet ermitteln müssen, wird Quick Freeze nicht zum Erfolg führen, solange die deutschen Provider so speichern, wie sie es aktuell tun. Das, was ich gerade ausgeführt habe, gilt für den im Antrag genannten Phänomenbereich, aber auch in anderen Bereichen der schweren Kriminalität müssen Strafverfolgungsbehörden IP-Adressen auch rückwirkend zuordnen können. Kriminalität verlagert sich immer stärker in das Internet und wir brauchen einfach die notwendigen Mittel, um Tatverdächtige identifizieren zu können. Deshalb

befürworten wir ausdrücklich, dass die vom EuGH geschaffenen Möglichkeiten zur Speicherung von IP-Adressen ergriffen werden und in praktikabler und rechtssicherer Art und Weise umgesetzt werden. Vielen Dank.

Die **Vorsitzende**: Vielen Dank, Frau Hackenbroch. Bei uns geht es dann weiter mit Tom Jennissen von der Digitale Gesellschaft e.V. Berlin.

SV **Tom Jennissen**: Hallo und vielen Dank für die Einladung, Frau Vorsitzende, meine Damen und Herren. Vielen Dank für die Möglichkeit, hier sprechen zu können. Es ist ein bisschen eigenartig, dass wir im Jahr 2023 noch weiterhin über die Vorratsdatenspeicherung sprechen. Die Idee kam 2002 zum Ersten Mal auf. Die Geschichte ist allgemein bekannt. Alle Anläufe sind bislang vor den Gerichten gescheitert. Das lässt sich primär auf zwei grundlegende Punkte runterbrechen. Das massenhafte Speichern von Kommunikationsdaten der gesamten Bevölkerung steht in einem grundlegenden Widerspruch zu den durch die Grundrechtecharta und das Grundgesetz garantierten Grundrechten der Bevölkerung. Zum anderen hätten wir daraus lernen können oder können wir daraus lernen, dass so eine Politik, die immer auf das Ausreizen des verfassungsrechtlich gerade noch Möglichen ausgerichtet ist, letztlich dazu führt, dass wir über Jahrzehnte mittlerweile in so einem Schwebezustand sind. Wir haben keine Rechtssicherheit für die Ermittlungsbehörden und auch so einem massiven Misstrauen der Bevölkerung, die Proteste seinerzeit sprechen dafür Bände. Ich glaube, jeder weitere Versuch, eine Vorratsdatenspeicherung einzuführen, wird zu einer Verlängerung dieses Zustands führen. Es ist nur schwer möglich, eine rechtssichere Vorratsdatenspeicherung einzuführen. Um es vorwegzusagen: Der vorliegende Antrag wäre nicht dazu geeignet. Wenn ansatzweise nach diesem Konzept ein Gesetzentwurf oder ein Gesetz beschlossen würde, würde es scheitern. Das liegt an verschiedenen Punkten, auf die ich gerne in der Fragerunde eingehe. Ich würde so ein paar Punkte kurz mal rausgreifen. Zum einen der Korridor, den der EuGH aufmacht für eine mögliche IP-Adressen-Speicherung, ist sehr, sehr eng. Er setzt sehr hohe Maßstäbe, die nur schwer gerecht werden können. Es gibt da noch sehr, sehr viele Punkte, die noch nicht ausbuchstabiert sind. Das betrifft die Speicherfrist. So viel vorab. Ich glaube, sechs Monate entsprechen in keiner Weise dem durch das EuGH-Urteil oder wiederholten EuGH-Urteile klar gemachten, auf das absolut Notwendige beschränkte und für den zur Zielverfolgung absolut notwendig beschränkten Zeitraum. Dazu bedarf es objektiver Kriterien, die sind in keiner Weise ersichtlich. Sechs Monate ist so aus der Luft gegriffen. Das BKA selbst, also unabhängige Zahlen, Gutachten bestehen da nicht. Das BKA selbst spricht von mehreren Wochen, die ausreichen würden zur Bekämpfung von Kindesmissbrauchsdarstellung oder sexualisierte Darstellung, sexualisierter Gewalt gegen Kinder. Ein anderer Punkt sind die Portnummern. Das ist keineswegs einfach ein Beiwerk zur IP-Adress-Speicherung, sondern Portnummern, das ist noch mal ein ganz schwerwiegender Eingriff in diverse Grundrechte. Das kann ich gerne noch mal ausführen, da deutlich mehr Daten gespeichert werden, die es ermöglichen, relativ detaillierte Profile von Nutzer:innen allein durch die gespeicherten Daten. Selbst wenn keine Kommunikationsinhalte selbst erhoben werden oder die damit verknüpft werden. Das liegt einfach an der technischen Ausgestaltung von Portnummern. Es gibt diverse Alternativen, Quick Freeze wurde angesprochen, aber vor allem sollten wir mal den Fokus legen auf einen ernsthaften Kinderschutz der Prävention in den Mittelpunkt stellt. Es gibt, als digitale Gesellschaft erleben wir das ständig, keine ernsthafte Aufklärung in Schulen. Betroffene werden alleingelassen mit Missbrauch. Das wäre ein Ansatz, mal ranzugehen. Der wird weiterhin nicht verfolgt. Es liegt einiges im Argen. Stattdessen wird seit Jahrzehnten behauptet, dass die Vorratsdatenspeicherung, also die anlasslose Überwachung der gesamten Bevölkerung, der Königsweg sei. Es hat sich gezeigt, das ist gescheitert. Es ist an der Zeit, dass wir andere Wege gehen. Vielen Dank.

Die **Vorsitzende**: Vielen Dank, Herr Jennissen. Dann geht es weiter mit Professor Ulrich Kelber. Der ist auch in Persona Bundesbeauftragter für den Datenschutz und die Informationsfreiheit.

SV **Prof. Ulrich Kelber**: Sehr geehrte Frau Vorsitzende, meine sehr geehrten Damen und Herren Abgeordneten, herzlichen Dank für die Einladung zur heutigen

Sachverständigenanhörung. Vorneweg: Wir hatten den Einladungstext nicht so verstanden, dass eine schriftliche Stellungnahme gewünscht war. Frau Vorsitzende hat mich auf diesen Irrtum, für den ich mich entschuldigen möchte, hingewiesen. Wir werden sie kurzfristig nachliefern. Der Europäische Gerichtshof hat dem möglichen Korridor einer Vorratsdatenspeicherung von IP-Adressen umrissen, fest umrissen. Wenn eine gerichtsfeste Gesetzgebung erfolgen soll, dann muss dieser Korridor diesmal zwingend eingehalten werden. Und das bedeutet, dass Regelungen, die der Europäische Gerichtshof offengelassen hat, grundrechtsschonend umgesetzt werden müssen. Das Urteil stellt klar, eine anlasslose Speicherung von Verkehrs- und Standortdaten, wie sie im deutschen Recht vorgesehen war und immer wieder vorgeschlagen wird, ist nicht mit europäischem Recht vereinbar. Der Europäische Gerichtshof sagt, dass eine allgemeine und anlasslose Speicherung der IP-Adressen einen schweren Grundrechtseingriff darstellt, weil sie eben, und es ist gerade auch angesprochen worden, in Verbindung auch mit den Portadressen, was notwendig ist, technisch, können wir sicherlich nachher ausführen, sehr genaue Rückschlüsse auf das Privatleben zulässt und gleichzeitig eine abschreckende Wirkung, das ist jetzt der deutsche Teil der Ausübung, von Freiheitsrechten nach dem Grundgesetz darstellen. Selbstverständlich gilt aber, wenn es um die Bekämpfung schwerer Kriminalität gibt, dass solche, auch widerstreitenden Rechte und berechtigten Interessen mit in die Betrachtung einbezogen werden müssen. Also ein schmaler Grat, einer grundrechtskonform allgemeinen und unterschiedslosen Vorratsdatenspeicherung bei IP-Adressen. Drei Elemente des Gerichtshofs: Erstens, Schutz der nationalen Sicherheit, auch das anlassbezogen, Bekämpfung schwerer Kriminalität, Verhütung schwerer Bedrohungen der öffentlichen Sicherheit. Die Dauer der Speicherung muss im Hinblick auf das verfolgte Ziel, auf das absolut Notwendige beschränkt werden und eine strenge Voraussetzung auch für Garantien, hinsichtlich der Auswertung der Daten. Dafür braucht es klare materielle und prozedurale Vorgaben. Ich begrüße, in meiner Funktion als Datenschutzbeauftragter, die Entscheidung des Europäischen Gerichtshofs. Es ist wichtig und richtig, dass Daten unbescholtener Bürgerinnen und Bürger, eben nur gezielt oder zum Schutz besonders herausragender Schutzgüter, gespeichert werden. Wer eine Vorratsdatenspeicherung möchte nach diesem Urteil, muss darlegen können, dass zum Beispiel die geplante Dauer der Speicherung das absolut notwendige Maß nicht überschreitet. Im vorliegenden Antrag werden sechs Monate vorgeschlagen. Hier ist eine Verhältnismäßigkeit auch mit Zahlen, wie sie die Ermittlungsbehörden vorlegen, für mich nicht erkennbar. Der Europäische Gerichtshof hat der Speicherung von IP-Adressen keinen endgültigen Riegel vorgeschoben, das ist klar, aber die Frage muss man sich natürlich stellen. Wie nützlich ist dieses Instrument? Denn die Nützlichkeit ist ebenfalls abzuwägen mit dem erheblichen Grundrechtseingriff. Und wir haben auch seit 2002 Entwicklungen gehabt, dass eben Umgehungsmöglichkeiten anhand von VPNs, von Browsern, die die IP-Adressen verschleiern, dass es allen Täterinnen und Tätern einfach und niederschwellig möglich ist, die IP-Adresse nicht anzugeben bei ihren Tätigkeiten. Von daher sind andere Alternativen natürlich zu vergleichen. Und ich bitte auch darum, in Betracht zu ziehen, dass das Verfassungsgericht gesagt hat, dass wir eine Überwachungsgesamtrechnung brauchen, damit weitere Erhebungsmaßnahmen nicht zu einer Abkühlung der Ausübung der Freiheitsrechte führt. Dementsprechend muss jede Gesetzesinitiative darauf abzielen, auch gerichtsfest Bestand zu behalten. Weitere Stoppsignale der obersten europäischen und deutschen Verfassungsgerichte würden das Vertrauen der Bevölkerung untergraben.

Die **Vorsitzende**: Vielen Dank, Ulrich Kelber. Dann schalten wir nun zu Dr. Benjamin Krause. Er ist Oberstaatsanwalt bei der Zentralstelle für Bekämpfung der Internet- und Computerkriminalität in Frankfurt. Die Leitung steht.

SV **Dr. Benjamin Krause**: Ja, das hoffe ich auch, dass die Leitung steht.

Die **Vorsitzende**: Sieht gut aus. Dann haben Sie das Wort.

SV **Dr. Benjamin Krause**: Ja, sehr schön. Vielen Dank, Frau Vorsitzende, sehr geehrte Abgeordnete, meine Damen und Herren! Auch ich möchte mich zunächst bedanken, dass ich zu

diesem, für die Strafverfolgungspraxis wichtigen Thema, zu Ihnen sprechen darf. Ich möchte mit meiner Stellungnahme meine ganz eigenen praktischen Erfahrungen als langjähriger Staatsanwalt für die Verfolgung von Internetkriminalität in Ihre Diskussion einbringen. Was ist das bei mir? Seit 2010 ist einer meiner beruflichen Schwerpunkte die Verfolgung der massenhaften Verbreitung von Kinderpornografie im Netz über alle möglichen Formen der Internetkommunikation und damit verbunden auch die Aufklärung und die Erkennung von Realfällen des sexuellen Missbrauchs von Kindern. Und aus dieser praktischen Erfahrung heraus empfehle ich Ihnen, den gesetzgeberischen Spielraum zu nutzen, den die Rechtsprechung des EuGH, aber auch des Bundesverfassungsgerichts und des Bundesverwaltungsgerichts einräumen. Ich bin persönlich aufgrund meiner Erfahrung der Auffassung, dass die Einführung einer solchen EuGH konformen Speicherung von IP-Adressen und Portnummern die strafrechtlichen Ermittlungen zur Verfolgung von Kinderpornographie, aber auch und zur Verfolgung sexuellen Kindesmissbrauchs wesentlich vereinfachen und wesentlich effektivieren würde. Warum bin ich der Auffassung, warum ist die Speicherung von IP-Adressen für die Strafverfolgung so notwendig? Beim Internet begangenen Straftaten, das hat der EuGH uns ja auch gesagt, kann die IP-Adresse der zur Tatbegehung genutzten Internetverbindung der einzige Ermittlungsansatz sein. In diesen Fällen ist es eben evident. Aber aus meiner persönlichen Erfahrung ist die IP-Adresse der werthaltigste Ermittlungsansatz auch in anderen Fällen, nämlich, wenn weitere Anhaltspunkte zur Identifizierung unbekannter Täter vorliegen, wie etwa verwendete Kennungen bei Plattformen oder E-Mail-Adressen, denn E-Mail-Adressen oder Kennungen bei Onlineplattformen können kostenlos und ohne Identitätskontrolle durch die Verwendung frei erfundener Personalien registriert werden. Die Internetzugang Dienste erheben, aber dagegen verifizierte Personendaten ihrer Kunden, eben um die Bezahlung der Dienstleistung sicher zu stellen und ihre Ansprüche notfalls gerichtlich durchzusetzen. Deswegen sind diese Daten für uns wesentlich werthaltiger. Das Ziel unserer Internetermittlung ist es daher immer, aktuelle IP-Adressen der unbekannten Täter zu ermitteln, um diese dann über Bestandsdatenanfragen den Anschlussinhabern zuzuordnen. In der Praxis geht es also an sich und fast immer "nur" um die Zuordnung einer bereits bekannten tatrelevanten IP-Adresse zu dem jeweiligen Anschlussinhaber. Und das gilt im Übrigen auch für die Verfolgung von Kriminalität im Darknet. Frau Hackenbroch hat ein negatives Beispiel dafür schon angeführt. Ich könnte Ihnen positive Beispiele nennen, wie etwa die Darknet Plattformen Elysium und Boys Town, bei denen wir die Betreiber identifizieren konnten. Diese sind allerdings diese Ermittlungserfolge aus meiner persönlichen Sicht zu oft vom Zufall abhängig, wie alt die IP-Adresse ist, welche Internetzugang Dienste die Täter nutzen und ob und wie lange die Daten dort aus unternehmerischen Gründen gespeichert werden. Denn es ist sicherlich nicht so und da sind wir uns einig, dass die Zuordnung IP-Adresse zu Kunden derzeit mindestens sieben Tage ist, sondern es ist einfach unklar für die Strafverfolgungsbehörden. Ich bitte Sie also, da zu berücksichtigen in Ihren Beratungen, dass das die Notwendigkeiten der Strafverfolgungsbehörden bei der Verfolgung von Internetkriminalität sind. Herzlichen Dank.

Die **Vorsitzende**: Herzlichen Dank, Herr Dr. Krause. Dann geht es bei uns hier im Saal weiter mit der Vizepräsidentin beim Bundeskriminalamt, Frau Martina Link. Sie haben das Wort.

SVe **Martina Link**: Ja, vielen Dank, Frau Vorsitzende, sehr geehrte Abgeordnete, meine Damen und Herren. Auch ich bedanke mich herzlich für die Gelegenheit, hier heute einige Impulse aus Sicht des BKA setzen zu können. Und mir geht es insbesondere um die Bedeutung der IP-Adresse für die polizeiliche Arbeit. Mit der fortschreitenden Digitalisierung finden auch kriminelle Tatvorbereitungen und Tathandlungen zunehmend im digitalen Raum statt. Und während in den Jahren 2015 bis 2022 die registrierten Straftaten um rund 11 Prozent zurückgegangen sind, haben wir im gleichen Zeitraum beispielsweise bei Computer- und Cyberkriminalität einen Anstieg von 156 Prozent festzustellen. Auch bei den Meldungen, die wir vom US-amerikanischen Zentrum, dem sogenannten NCMEC, National Center for Missing

and Exploited Children erhalten, stellen wir seit Jahren einen Anstieg fest. In diesem Jahr rechnen wir mit rund 180.000 solcher Meldungen. Und diese Meldungen beinhalten als Ermittlungsansatz in nahezu allen Fällen die IP-Adresse, in geringerem Umfang auch Registrierungsdaten, wie beispielsweise E-Mail-Adressen oder Telefonnummern. Insbesondere die E-Mail-Adressen sind aber in der Regel nicht verifiziert. Das heißt, entsprechende Ermittlungen laufen regelmäßig ins Leere. Über die IP-Adresse, bei dynamisch vergebenen, mit Zeitstempel lässt sich ermitteln, welchem Anschluss eine Internetverbindung zugewiesen war, über die zum tatrelevanten Zeitpunkt zum Beispiel kinderpornografische Inhalte geteilt wurden. Die hierzu bei den Providern vorliegenden Daten, das hat Herr Krause bereits gesagt, sind verifiziert, weil die Provider diese Daten für IT-Sicherheitszwecke, beispielsweise zur Störungsbeseitigung vereinzelt auch noch für Abrechnungszwecke benötigen. Und aus diesem Grund ist die IP-Adresse der wichtigste und der wertigste Ermittlungsansatz zur Identifizierung eines Täters. Die Telekommunikationsanbieter speichern derzeit diese Daten aufgrund der fehlenden Mindestspeicherfristen lediglich, wenn dies zu eigenen Geschäftszwecken erforderlich ist und die Speicherdauer bei den unterschiedlichen Anbietern ist unterschiedlich und beträgt in der Regel einen bis sieben Tage. Ob dann eine Bestandsdatenabfrage zur IP-Adresse erfolgreich ist, hängt aktuell vom Zufall ab. Das heißt, nutzt der Tatverdächtige einen ausländischen oder einen deutschen Anschluss und wenn er ihn in Deutschland nutzt, von welchem Anbieter stammt dieser Anschluss? Wir haben die Auswirkungen der derzeit fehlenden Speicherfristen auf die polizeiliche Ermittlung mit einer Stichprobe von 1.000 strafrechtlich relevanten Vorgängen aus dem NCMEC Prozess erhoben. In 41 Prozent dieser Vorgänge konnte die IP-Adresse einem Nutzeranschluss zugeordnet werden und damit konkrete weitere Ermittlungen durchgeführt werden. In 34 Prozent waren sie beim Telekommunikationsanbieter nicht mehr gespeichert und weitere 24 Prozent waren aus anderen Gründen nicht mehr auskunftbar, beispielsweise weil die zusätzlich zur Identifizierung erforderlichen Portnummern nicht vorlagen. Im Ergebnis mussten, obwohl wir jede Informationsansatz und Ermittlungsansatz genutzt haben, etwa 25 Prozent der NCMEC-Vorgänge aus dieser Auswertung der Staatsanwaltschaft zur Einstellung vorgelegt werden, weil eine Zuordnung nicht möglich war. Der Europäische Gerichtshof hat in seinem Urteil die anlasslose Speicherung von IP-Adressen zugelassen, allerdings nur für eine auf den absolut notwendigen begrenzten Zeitraum. Und vor diesem Hintergrund haben wir geprüft, wie alt die IP-Adressen sind, die dem BKA als Ermittlungsansatz zur Verfügung stehen. Im Umkehrschluss: Wie lange müssten Speicherfristen bemessen sein, damit die uns vorliegenden IP-Adressen noch einem Nutzer zugeordnet werden können? Im NCMEC-Prozess waren 88,4 Prozent der mitgeteilten IP-Adressen bis zu drei Wochen alt. Das bedeutet, dass in diesem sehr etablierten, weitgehend automatisierten Prozess eine Speicherverpflichtung von 2 bis 3 Wochen bereits einen signifikanten Sicherheitsgewinn darstellen würde. Und das könnte je nach Ausgestaltung auch für die Umsetzung des Digital Services Act und der aktuell verhandelten Child Abuse gelten. Das ist allerdings nicht übertragbar auf Deliktsbereiche und Prozesse, bei denen die Tat relevante IP-Adresse erst später bekannt oder sogar erst aufwendig ermittelt werden muss. Beispielsweise in komplexen Ermittlungsverfahren, bei Ermittlungen zu Strukturen des Terrorismus oder organisierter Kriminalität, bei Cybercrime, aber auch in Ermittlungsverfahren im Bereich des sexuellen Missbrauchs von Kindern, wo die IP-Adressen deutlich älter sind.

Die **Vorsitzende**: Vielen Dank, Frau Link. Ich glaube, alles weitere wird dann in den Fragerunden noch mal angesprochen werden können. Bei uns geht es dann weiter mit Dr. Bijan Moini von der Gesellschaft für Freiheitsrechte in Berlin. Sie haben das Wort.

SV **Dr. Bijan Moini**: Vielen Dank! Sehr geehrte Damen und Herren, Abgeordnete!

Die **Vorsitzende**: Frau Link macht Ihr Mikro bitte aus.

SV **Dr. Bijan Moini**: Sehr geehrte Damen und Herren Abgeordnete. Das Ziel des Antrags, Missbrauchsdarstellung von Kindern im Netz besser verfolgen zu können, ist unbedingt zu

begrüßen. Mit der Vorratsspeicherung von IP-Adressen schlägt der Antrag jedoch ein Mittel vor, das die Grundrechte der Internetnutzer:-innen, also nahezu aller Menschen in diesem Land, verletzen würde. So unverhältnismäßig es im analogen Leben wäre, monatelang nachvollziehen zu können, welche Orte Menschen besuchen, wen sie dort treffen, was sie dort sagen oder tun, so wenig wäre es angemessen, das Verhalten vieler unschuldiger Menschen im Netz auf vergleichbare Weise nachvollziehbar zu machen. Ich möchte in meinem Statement den Schwerpunkt auf das Gewicht des Eingriffs legen, den die Vorratsspeicherung von IP-Adressen hat, denn das trägt unsere Bewertung maßgeblich. Im Übrigen verweise ich auf meine schriftliche Stellungnahme. Vorratsspeicherung von IP-Adressen ist anlasslose Massenüberwachung. Sie greift tief in Grundrechte ein. Es ergibt sich einerseits aus der Sensibilität von IP-Adressen. Sie erlauben es nämlich, nachzuvollziehen, was Internetnutzer:innen gelesen, gehört, gesehen oder gesucht haben, welchen Meinungsbeitrag sie veröffentlicht, welche Datei sie heruntergeladen oder welche Produkte, Dienstleistungen und Applikationen sie betrachtet oder bestellt bzw. genutzt haben. Über mich persönlich sagen die Spuren meiner IP-Adressdaten sehr viel mehr aus als meine Standortdaten. Und das gilt wahrscheinlich für so gut wie jeden hier im Raum. Die gestiegene Zahl der Internet-nutzer:innen und der Anstieg der Nutzungsdauer erhöhen zudem die Quantität und, weil sich zugleich immer wesentlichere Teile des Lebens ins Netz verlagern, die Sensibilität der potenziell mit IP Adressen verknüpft waren Internet-kommunikation, was den Eingriff weiter vertieft. Aufgrund der Sensibilität von IP-Adressdaten ist der Vergleich, den der Antrag zwischen IP-Adressen und Kfz-Kennzeichen zieht, nicht nur schief, sondern er liegt quer. Das Pendant zur Vorratsspeicherung von IP-Adressdaten wäre nicht einfach die Speicherung der Kfz-Kenn-zeichen beim Kraftfahrtbundesamt. Der IP-Vorratsspeicherung würde im realen Leben entsprechen von Kfz-Fahrer:innen entsprechen, über mehrere Monate einen Abgleich zu ermöglichen, zwischen allen Kfz-Kennzeichen und jenen Orten, die Fahrzeuge mit diesen Kennzeichen besucht haben, also Arztpraxen, die Strafverteidiger:innen, die politische Veran-staltung usw. Das Gewicht des Eingriffs durch die IP-Vorratsspeicherung ergibt sich konkret aus den Gefahren für die gespeicherten Daten. Und die sind vielfältig. IP-Adressdaten können versehentlich oder absichtlich zweckentfremdet oder von kriminellen oder Nachrichtendiensten entwendet und zur Schädigung der Betroffenen eingesetzt werden. Es wird heute dadurch wahrscheinlicher, dass die Instrumente zur KI gestützten Massendatenverarbeitung sowie zur zunehmend ebenfalls KI gestützten Ausnutzung der erworbenen Erkenntnisse zu Erpressungen und Betrugsmaschen immer leichter zugänglich sind. Nicht zu unterschätzen ist zudem, dass sich durch die Vorratsspeicherung von IP-Adressen die Gefahr von falschen Verdächtigungen und unberechtigten Folgemaßnahmen erhöht. Es drohen mehr Vorladungen, Beschlagnahmungen, Hausdurchsuchungen oder gar Anklagen von Unschuldigen. Diese und weitere Erwägungen führen die Gesellschaft für Freiheitsrechte zu dem Ergebnis, dass die Gefahren einer Vorrats-speicherung von IP-Adressen, deren Vorteile für die Aufklärung der Verbreitung von Kindesmiss-brauchsdarstellung im Internet überwiegen. Die mit dem Antrag geforderte Regelung wäre unverhältnismäßig und würde damit Grundrechte verletzen. Was schließlich die schon wiederholt vorgetragene Rechtsprechung des EuGH angeht: Verfassungsrechtsprechung ist kein politisches Programm. Nur, weil etwas vor Gericht Bestand haben könnte, ist es nicht legitim. Sicherheits-politik sollte nicht den Anspruch haben, sich am Rande des Zulässigen zu bewegen. Anlasslose Massenüberwachung ist und bleibt eine gefährliche Versuchung, der wir als Gesellschaft nicht nachgeben sollten. Vielen Dank.

Die **Vorsitzende**: Vielen Dank, Herr Dr. Moini. Dann geht es bei uns weiter mit Dr. Oliver Piechaczek vom Deutschen Richterbund. Sie haben das Wort.

SV **Dr. Oliver Piechaczek**: Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren. Zunächst einmal danke ich für die Gelegenheit, an dieser Anhörung teilnehmen zu dürfen und die Position des Deutschen Richterbundes darzutun. Der Deutsche Richterbund begrüßt, dass mit dem Antrag von CDU/CSU verfolgte Ziel ausdrücklich. Aus Sicht der Strafverfolgungs-

praxis besteht das Bedürfnis, den vom Europäischen Gerichtshof eingeräumten gesetzgeberischen Spielraum auszunutzen und allgemeine und unterschiedslose Vorratsdatenspeicherung von IP-Adressen bei schwerer Kriminalität zu ermöglichen. Dies gilt in besonderem Maße für den Gegenstand des Antrags, nämlich die Verfolgung sexuellen Missbrauchs von Kindern und der Kinderpornografie, aber auch und darauf möchte ich mal den Blick lenken, im Bereich des Staatsschutzes. Lassen Sie mich dies an folgendem fiktiven Beispiel, das der Realität aber gar nicht mehr so fern liegt, verdeutlichen. Ein ausländischer Geheimdienst übermittelt dem BKA-Hinweise, zu einem in naher Zukunft bevorstehenden Terroranschlag und übermittelt zugleich eine IP-Adresse, die zu einem Tatverdächtigen führen könnte. Diese IP-Adresse ist allerdings acht Tage zuvor verwendet worden. Die Abfrage der IP-Adresse folgt bei einem Anbieter, der die Adressen für die Dauer von lediglich sieben Tagen speichert. Und das entspricht der gängigen Speicherpraxis von der Deutschen Telekom, von Vodafone, Telefonica. Der Tatverdächtige ist infolgedessen gar nicht oder nur unerheblich oder nur erheblich verzögert identifizierbar. Ein zeitnaher Zugriff ist unter diesen Umständen nicht möglich. Ein Anschlag kann nicht vereitelt werden. Und natürlich, das ist Gefahrenabwehr, aber zugleich auch Strafverfolgung, die sich nämlich dann anschließen würde. Dieses Fallbeispiel zeigt zweierlei. Es sind mehrere hochsensible Bereiche, in denen IP-Adressspeicherung wichtig sein kann, eben auch für den Staatsschutz und die Terrorabwehr. Und das Zweite, was das Bundesministerium für Justiz derzeit favorisiert, dieses Quick Freeze Verfahren, läuft in einem solchen Fall ins Leere. Nämlich dann, wenn die Hinweise, häufig kommen sie aus den USA, zu spät kommen. Wenn keine Daten mehr bei den Providern gespeichert sind, funktioniert das geplante Einfrieren nicht mehr. Nur noch einmal zurück zu dem Deliktfeld des sexuellen Missbrauchs von Kindern. In der rechtspolitischen Debatte ist mitunter zu hören, die Vorratsdatenspeicherung sei nicht erforderlich. Und das aus zwei, nach meinem Dafürhalten, kritisch zu beleuchtenden Annahmen heraus. Die erste Annahme, darauf ist Herr Krause schon eingegangen, der Austausch kinderpornografischer Dateien. Das erfolgt in der Regel im Darknet und dort würden uns die IP-Adressen nicht weiterhelfen. Herr Krause hat das eben aufgezeigt. Dazu muss ich mich nun nicht wiederholen. Es gelingt eben auch im Darknet erfolgreich Ermittlungen durchzuführen. Und auch da sind IP-Adressen ein werthaltiger Ermittlungsansatz. Die zweite Annahme hat statistischen Charakter. Es geisterte eine Zeit lang hier eine Zahl umher. Das BKA, ist inzwischen auch ein bisschen geradegerückt von der Aufklärungsquote von 97 %. Oder eben umgekehrt gewendet. Lediglich 3 % aller verfolgten Fälle der Verbreitung von Kinderpornographie im Internet seien nicht aufgedeckt worden, weil die Betreiber mangels Speicherung die IP-Adresse nicht mehr einer Person zuordnen konnten. Diese Argumentation ist nach meinem Dafürhalten verkürzt und ich halte sie teilweise auch für zynisch. Denn wir haben in diesem Bereich ganz enorme Fallzahlen. Mit Aufklärungsquoten kann man hier nicht argumentieren, denn wenn wir das in reale Zahlen wenden, dann ist klar, mehrere 1.000 Fälle pro Jahr sind nicht aufklärbar, weil die ermittelte IP-Adresse als einziger Ermittlungsansatz aufgrund der fehlenden Speicherung bei den Providern keinem Nutzer zugeordnet werden kann und darüber hinaus in diesem Kontext bitte ich zu bedenken, in einer Vielzahl dieser Fälle kommt es zum Realmissbrauch oder ein solcher Missbrauch, das sind die schlimmsten Fälle, die wir in der Praxis beachten, der dauert an. Jeder Realmissbrauch, gerade auch der schwere sexuelle Missbrauch von Kleinkindern, ist ein schweres Verbrechen, das in den Grenzen rechtsstaatlich zulässigen Instrumenten maximal effektiv verfolgt werden muss. Ich komme zum Ende. Danke für die Aufmerksamkeit.

Die **Vorsitzende**: Vielen Dank für Ihr Statement und wir schaffen zumindest noch eins, nämlich von Frau Sabine Witting. Sie ist von der Universität Leiden, dort Assistenzprofessorin und ich hoffe, die Leitung zu ihr steht.

SV **Dr. Sabine Witting**: Ich hoffe das auch. Können Sie mich hören?

Die **Vorsitzende**: Ja, klappt alles wunderbar. Und dann haben Sie das Wort.

SV **Dr. Sabine Witting**: Wunderbar. Sehr geehrte Vorsitzende, sehr geehrte Abgeordnete. Zunächst möchte ich mich auch bedanken für die Gelegenheit, heute hier mit Ihnen sprechen zu dürfen und verweise für zusätzliche Erläuterungen auf meine Stellungnahme. Zu meinem ersten Punkt. Der Antrag sieht vor, dass zusätzlich zu den IP-Adressen auch die Portnummern mitgespeichert werden sollen. In diesem Kontext muss man zwischen statischen und dynamischen IP-Adressen unterscheiden. In eine Vielzahl private Internet User:innen benutzen vornehmlich dynamische IP Adressen und nur mit zusätzlichen Daten, wie Portnummern, ist eben eine rechtssichere Zuordnung von dynamischen IP-Adressen zu konkreten User:Innen möglich. Der EuGH unterscheidet allerdings in seiner Rechtsprechung nicht zwischen statischen und dynamischen IP-Adressen und er erwähnt auch Zusatzdaten, wie die Portnummer nicht. Er spricht nur von IP-Adressen ganz allgemein. Allerdings, wie schon ausgeführt, könnte die zusätzliche Speicherung von Portnummern zu einer erhöhten Eingriffsintensität führen, damit hier eine noch genauere Profilbildung möglich ist. Es ist damit unklar, inwieweit der Antrag überhaupt vor dem EuGH-Bestand haben würde, wenn er denn einschließt die Speicherung von Portnummern. Zu meinem zweiten Punkt. Der Antrag sieht eine Speicherfrist von sechs Monaten vor und die auch schon gesagt, ohne jegliche Begründung oder empirische Grundlage zu nennen, wie denn diese Speicherfrist dem vom EuGH vorgegebenen Kriterium eines auf das absolut notwendigen begrenzten Zeitraums entspricht. Eine evidenzbasierte, überprüfbare Begründung ist unentbehrlich, denn der vom EuGH vorgegebene, stark limitierte zeitliche Rahmen ist ein Kernelement der engen Ausnahmemöglichkeiten. Und ob eine solche Begründung, falls sie dann nachgereicht wird, dann der rechtlichen Überprüfung des EuGH standhalten wird, ist auch fraglich, denn der EuGH hat sich bisher nicht dazu geäußert, wie er den Begriff auf den absolut notwendig begrenzten Zeitraum interpretiert. Zu meinem dritten Punkt. Die im Antrag vorgeschlagene Regelung muss dem Grundsatz der Verhältnismäßigkeit entsprechen. Und obwohl der Antrag natürlich einen legitimen Zweck verfolgt, ist bereits die Geeignetheit der Maßnahme fragwürdig. Der Antrag nimmt an, dass relevante Straftaten nicht aufgeklärt werden konnten, weil die notwendigen IP-Adressen nicht mehr zur Verfügung standen. Aber selbst beim Vorhandensein der IP-Adresse kommt es aufgrund von deren teils limitierter Aussagekraft und der mit VPN und Tor verbundenen Verdunkelungsrisiken nicht automatisch zu einem Ermittlungserfolg. Zudem hat eine Studie des Max-Planck-Instituts aus dem Jahr 2011 festgestellt, dass es keine belastbaren Hinweise darauf gebe, dass die Schutzmöglichkeiten durch den Wegfall der Vorratsdatenspeicherung reduziert worden wären, was insbesondere auch für den Bereich der Darstellung von sexualisierter Gewalt gegen Kinder gelte. Es bestehen außerdem erhebliche Bedenken im Bereich der Erforderlichkeit, denn es gibt jedenfalls eine Vielzahl mildere und wirksame Mittel. Zunächst ist eine umfassende Investition in die technischen und personellen Ressourcen der Strafverfolgungsbehörden zur Bekämpfung sexualisierter Gewalt gegen Kinder unentbehrlich. Eine andere grundrechtsschonender Maßnahme ist zudem das konsequente Löschen von Darstellungen sexualisierter Gewalt gegen Kinder. Allerdings wird das Löschen gegenwärtig unzureichend priorisiert, was mit fehlenden Ressourcen und mit einer fehlenden Rechtsgrundlage für das BKA begründet wird. Es ist daher zu empfehlen, das Schaffen einer solchen Rechtsgrundlage dringend voranzutreiben. Als weitere Maßnahme ist das vom Bundesministerium der Justiz vorgeschlagene Quick Freeze Verfahren zu erwähnen. Diese anlassbezogene Sicherung Verkehrsdaten erfolgt für einen festgelegten Zeitraum aufgrund richterlicher Anordnung und es ist damit das deutlich datensparsame und rechtssichere Datensicherungsverfahren. Es gibt daher eine Vielzahl grundrechtsschonender und zugleich wirksamere Maßnahmen zur Bekämpfung von sexualisierter Gewalt gegen Kinder. Wir sollten uns daher nicht in Diskussionen um punktuelle technische Lösungen verlieren, denn diese lenken oftmals von den grundlegenden systematischen Interventionen ab, die dringend notwendig sind, um das gesamtgesellschaftliche strukturelle Problem von sexualisierter Gewalt gegen Kinder wirksam anzugehen. Vielen Dank.

Die **Vorsitzende**: Vielen Dank, soweit an die Sachverständigen. Mit Blick auf die Uhr und zu dem vorhin schon geschilderten Zweck, dass wir jetzt zu der zu Beginn des Plenums und bei der Gedenkminute der Präsidentin dabei sein können, unterbreche ich die Sitzung, unterbreche auch den Stream, damit alle Zuschauer Bescheid wissen und wir treffen uns hier wieder, ich denke mal um zehn nach eins.

(Die Sitzung wird um 12:51 Uhr unterbrochen und ab 13:17 Uhr fortgesetzt.)

Die **Vorsitzende**: So, dann würde ich bitten, wieder Platz zu nehmen, damit wir fortfahren können mit der Anhörung. Zunächst noch einmal vielen Dank für Ihr Verständnis, aber ich glaube, es war gut und wichtig, dass wir Gelegenheit hatten, bei dieser besonderen Schweigeminute auch dabei zu sein, in Anwesenheit des israelischen Botschafters. Vielen Dank dafür. Mit Blick auf die Uhr, würde ich mal sagen, kommt das ziemlich genau hin, wenn wir eine halbe Stunde dranhängen. Also bis 14:30 Uhr. Und hoffe, dass das für alle auch organisatorisch so machbar ist. Ach so, also Herr Jacobi meldet sich. Wir hören da jetzt zunächst noch Professor Dr. Wollenschläger von der Uni Augsburg. Und dann habe ich auch schon eine Reihe von Wortmeldungen vorliegen. Sie haben das Wort.

SV **Prof. Dr. Ferdinand Wollenschläger:** Ja, vielen Dank, Frau Vorsitzende. Meine Damen und Herren. Um das Gesamtergebnis vorwegzunehmen: Die im Antrag vorgeschlagene Einführung einer generellen Speicherung von IP-Adressen steht im Ermessen des Gesetzgebers, der die ja schon bei meinen Vorrednerinnen und Vorrednern vielfach angeklungenen Belange von Freiheit und Sicherheit abwägen muss. Aus rechtlicher Perspektive ist jedoch klar und auf die Beschränke ich mich in meinem. In meiner Kurzstellungnahme ist festzuhalten, dass die Speicherung sich in verfassungs- und auf unionsrechtskonforme Weise realisieren lässt. Einleitend möchte ich festhalten, dass der deutsche Gesetzgeber völkerverfassungs- und unionsrechtlich verpflichtet ist, Kinder effektiv vor sexuellem Missbrauch zu schützen. Und hierzu rechnet natürlich auch der Einsatz des Strafrechts, einschließlich einer wirksamen Verfolgung und Verhütung von Straftaten. Der vorliegende Antrag dient der Realisierung dieser Schutzpflicht, indem er auf eine generelle Speicherung von IP-Adressen zur Verfolgung der Straftaten des sexuellen Kindesmissbrauchs und der Kinderpornographie zielt. Um nicht missverstanden zu werden, angesichts des weiten Spielraums des Gesetzgebers bei der Realisierung von Schutzpflichten, besteht natürlich keine Pflicht des Gesetzgebers, eine solche Speicherung einzuführen. Vielmehr erweist sich diese Speicherung als Grundrechtseingriff von relativ hoher Intensität und ist damit ihrerseits rechtfertigungsbedürftig. Eine Rechtfertigung ist allerdings nach den hier primär maßgeblichen Anforderungen des EU-Sekundärrechts und der Europäischen Grundrechtecharta in seiner Auslegung durch den Europäischen Gerichtshof möglich und auch hinreichend konsolidiert. Was sind die Anforderungen der Verhältnismäßigkeit, die der Europäische Gerichtshof einstellt? Einmal ist die mögliche Zwecksetzung qualifiziert. Eine Speicherung von IP-Adressen ist nur zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit zulässig. Hierzu rechnet die Bekämpfung des sexuellen Missbrauchs von Kindern und die Kinderpornographie. Insoweit liegt der Antrag hier im Rahmen des Zulässigen. Hinzufügen möchte ich aber auch, dass er diesen Rahmen des Zulässigen mit Blick auf die erfassten Straftatbestände nicht ausschöpft. Die Speicherung ist auch geeignet, da sie die Identifikation von Personen, die das Internet zur Begehung von Straftaten nutzt, ermöglicht. Und damit ist die Eignung zu bejahen. Ich möchte auch darauf hinweisen, nachdem da Missverständnisse zu bestehen scheinen, dass Eignung im verfassungsrechtlichen Sinne bedeutet, dass eine Maßnahme zur Zielerreichung förderlich ist. Es ist aber nicht erforderlich, dass es, sozusagen, ein Optimum, ein Tauglichkeitsoptimum darstellt oder weiter, sondern zur Zielerreichung förderlich. Und ich denke, das steht außer Frage. Die Maßnahme ist auch erforderlich, da kein milderes, gleich wirksames Mittel ersichtlich ist. Es reicht nicht aus, zu sagen, dass eine grundrechtsschonende Alternative besteht, sondern, die muss auch gleich wirksam sein. Und ein solches ist das Quick Freeze Verfahren schon deshalb nicht, weil es mangels Gewährleistung der Speicherung keine gleich effektiven Aufklärungsmöglichkeiten

bietet. Die entscheidende Frage ist damit die Frage der Angemessenheit. Und hier ist auf der Basis der Rechtsprechung des Europäischen Gerichtshofs zu sagen, dass die Speicherung von IP-Adressen unter den geltenden Kautelen für zulässig erachtet wird. Der Europäische Gerichtshof geht, anders als für die generelle Speicherung von Verkehrs- und Standortdaten, von einem generellen Sensibilitätsgrad von IP-Adressen aus und betont auch deren Relevanz für die Aufklärung von im Internet begangenen Straftaten, weshalb er eine anlasslose und unterschiedslose Speicherung solcher Daten zulässt. Unter Kautelen einmal die beschränkten Zwecke, dann die limitierte Speicherdauer und natürlich ist auch die Auswertung und Speicherung dieser Daten weiteren Kautelen, die ja auch Herr Kelber schon angesprochen hat, zu unterwerfen. Letzter Punkt die Speicherung. Ich habe es ja schon erwähnt, ist auf den absolut notwendigen Zeitraum zu beschränken. Was absolut notwendig ist, beschränkt sich zunächst einmal nach dem Ziel der wirksamen Bekämpfung von Straftaten. Das ist eine fachliche Frage. Hierzu hat sich Frau Link geäußert. Wenn ich Sie richtig verstanden habe, ist dieser 2 bis 3 Wochen Zeitraum, sozusagen ein Minimum. Aber es ist ein darüber hinaus gehender Zeitraum fachlich notwendig. Und für diesen weiteren Zeitraum, der fachlich da zu tun ist, wirkt diese Beschränkung auf das absolut Notwendige dann als normatives Korrektiv, insbesondere für den Grenznutzen, wenn sozusagen nur gerade bei zunehmender Speicherdauer der Grenznutzen abnimmt, dann bestehen hier Grenzen. Natürlich lädt

Die **Vorsitzende**: Kommen Sie zum Schluss.

SV **Prof. Dr. Ferdinand Wollenschläger**: Letzter Satz ist, nachdem vielfach auch die nichtrechtssicher mögliche Realisierung angesprochen wurde, ist es nicht möglich, ist aus dem Europarecht oder aus der Verfassung einen auf die Sekunde bestimmten Zeitraum abzuleiten. Wichtig ist nur, wenn Sie dieses Vorhaben realisieren müssen, dass Sie eben auch valide fachlicher Grundlage einen entsprechenden Zeitraum festlegen. Und dann kann man dieses letzte Prozess Risiko in Kauf nehmen. Vielen Dank.

Die **Vorsitzende**: Herzlichen Dank für die Stellungnahmen. Mir liegen jetzt Wortmeldungen vor. Ich lese diese gerade vor, dann weiß auch jeder ungefähr, wann er dran ist: Volker Ullrich, Helge Limburg, Günter Krings, Carmen Wegge, Ingmar Jung, Kollege Fiedler, Kollege Dr. Plum und Kollege Jacobi, Dr. Lieb, Domscheit-Berg, haben wir noch. Also von daher würde ich wirklich bitten, sich möglichst kurz zu fassen. Herr Baldy, damit wir das große Interesse hier auch zum Zuge kommen lassen können. Und Volker Ullrich hat als Erster das Wort.

Abg. **Dr. Volker Ullrich** (CDU/CSU): Frau Vorsitzende, meine Kolleginnen und Kollegen. Ich möchte anknüpfen an die Schutzpflicht des Grundrechtsgebundenen Staates gegenüber den Opfern von sexualisierter Gewalt. Diese Schutzpflicht muss hier abgewogen werden mit anderen Grundrechtseingriffen. Ich möchte Herrn Professor Wollenschläger fragen, inwieweit der EuGH nach einer längeren Judikative tauglicherweise diese Abwägung vornimmt und inwieweit dann auch unser Antrag dem Abwägungsgebot standhält. Und zweitens würde ich gerne von ihm wissen, ob überhaupt das Quick Freeze Verfahren dann diesen Anforderungen an die Abwägung standhalten kann, wenn es vor dem Hintergrund mangelnder Erfolgsaussichten eben gerade diese Schutzpflicht nicht erfüllen kann?

Die **Vorsitzende**: Vielen Dank. Helge Limburg.

Abg. **Helge Limburg** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Frau Vorsitzende. Erst einmal vielen Dank an Sie alle für Ihre Darstellung. Ich habe eine Frage an Frau Professor Witting. Sie haben in Ihrer Stellungnahme, sowohl schriftlich als auch mündlich ausgeführt, dass es eine Vielzahl grundrechtsschonender, milderer und zielführender Maßnahmen gibt, um Kinder vor sexualisierter Gewalt und deren Darstellung im Internet, also um diesen Schutz zu verbessern. Ein paar, haben Sie angerissen, können Sie das noch mal näher ausführen, die aus Ihrer Sicht wichtigsten genau ausführen und die zweite Frage mache ich auch direkt jetzt ja. Eine Frage hätte ich an Herrn Dr. Bijan Moini, knüpft auch ein bisschen an das gerade eben Gesagte zur Frage Abwägung zwischen den verschiedenen Sphären, Freiheit, Sicherheit. In

der rechtspolitischen Diskussion, wo würden Sie da die Vorratsdatenspeicherung von IP-Adressen verorten? Zwischen Schutz der Privatsphäre der Einzelnen jedes Einzelnen, jeder einzelnen Person und den Sicherheit- und Strafverfolgungsinteressen der Allgemeinheit? Wenn Sie das noch mal ausführen könnten. Sie haben so deutlich gemacht, dass aus Ihrer Sicht der Schutz der IP-Adressen ein hohes Gewicht hat. Wenn Sie das noch mal ausführen könnten.

Die **Vorsitzende**: Danke. Günter Krings.

Abg. **Dr. Günter Krings** (CDU/CSU): Ja, vielen Dank. Zunächst vielleicht eine Frage an Herrn Wollenschläger, aber vielleicht noch einen Satz. Ich freue mich jedenfalls, dass wir die Anhörung heute durchführen, konnten nach einem Jahr. Und es zeigt auch ist hochnötig darüber zu sprechen, da ja auch dankenswerterweise auch die Expertise quer durch die von den Fraktionen benannten Experten gehen. Und auch das finde ich auch sehr gut, auch wir auch bestätigt werden von Experten, die wir gar nicht selber benannt haben. Das ist ja bei manchen Anhörungen auch unterschiedlich. Ich wollte den Herr Wollenschläger fragen, weil ja die Begriffsverwirrung bei einzelnen Beiträgen auftauchte, Vorratsdatenspeicherung, IP-Adressenspeicherung, auch in der Frage der Grundrechtsqualität, des Grundrechtseingriffs ist ja hier eine ganz andere, weil es ja eben nicht eine allgemeine Speicherung von Verbindungsdaten ermöglicht wird, sondern nur die IP-Adressen gespeichert werden. Wie beurteilen Sie den Unterschied zu der altdiskutierten Vorratsdatenspeicherung, zu der IP-Adressenspeicherung auch in grundrechtlicher Hinsicht? Wie unterscheidet sich der Grundrechtseingriff nach Tiefe, nach Qualität bei IP-Adressenspeicherung versus der früher diskutierten Frage der Vorratsdatenspeicherung, die dann in der Tat nicht identisch ist mit unserem Vorschlag? Dann würde ich gerne, greife mal raus, Frau Link, ich könnte auch jemand anders fragen. Aus der Praxis heraus gibt es die Sorge, die auch eben geäußert worden ist, dass da Profile gebildet werden können? Sehen Sie die Gefahr von Profilbildungen, wenn man aus einer IP-Adresse die Zuordnung zu einer Person machen kann, eben ja nicht den umgekehrten Weg beschreitet, also nur eine IP-Adresse in einem Auftauchen zur Person? Kann man damit Profile bilden und wenn ja, oder unabhängig davon auch die Frage, gibt es da Missbrauchserfahrungen aus anderen Ländern, die das haben? Also ist diese Missbrauchssorge, hat die irgendeine empirische Fundierung?

Die **Vorsitzende**: Vielen Dank, Kollegin Wegge.

Abg. **Carmen Wegge** (SPD): Ja, auch von mir vielen lieben Dank für die Ausführungen. Ich habe zwei Fragen an Professor Dr. Uli Kelber. Die erste Frage ist eher, was für Feinschmecker der IP-Adressenmaterie, denn es wurde ja schon viel von dynamischen IP-Adressen zum Beispiel gesprochen und deswegen würde ich gerne mal fragen, ob Sie erläutern können, warum eine dynamisch hohe IP-Adresse als Verkehrsdatum und nicht als Bestandsdatum einzuordnen ist? Relevante Frage für die Debatte und dann darüber hinaus. Der Antrag zieht den Vergleich zu den Autokennzeichen in der digitalen Welt, das wären IP-Adressen, ist jetzt in der Sachverständigenstatements auch schon mal aufgekommen. Aber ich würde gerne auch noch mal von Ihnen hören, ob Sie diesen sehr häufig herangezogenen Vergleich tatsächlich auch teilen oder mal dazu Ausführungen machen könnten?

Die **Vorsitzende**: Kollege Jung.

Abg. **Ingmar Jung** (CDU/CSU): Ich muss mich nächstes Mal wieder früher melden. Ich würde mal dann Frau Link und Frau Hackenbroch gerne dieselbe Frage stellen, denn wir haben ja immer so diese Gegenüberstellung IP-Adressenspeicherung und Quick-Freeze-Verfahren und die allermeisten gehen auf das von ihnen bevorzugte ein und das anderen kurz, deswegen würde ich Sie jetzt mal beide gerne nach dem von Ihnen nicht bevorzugten Verfahren fragen? Es klingt immer so schön einfach, dass, wenn ich einen Anlass habe, friere ich einfach ein, dann habe ich alle Daten und kann doch genauso ermitteln und habe kaum noch einen Grundrechtseingriff. Warum priorisieren Sie eigentlich dieses Verfahren nicht und sprechen sich für ein anderes aus?

Die **Vorsitzende**: Vielen Dank. Herr Kollege Fiedler.

Abg. **Sebastian Fiedler** (SPD): Vielen herzlichen Dank! Ich richte meine Fragen an Frau Hackenbroch und Herrn Krause. Zunächst an

Frau Hackenbroch. Ich würde, es geht so ein bisschen in die gleiche Richtung, allerdings anders formuliert als mein Vorredner. Ich würde erst mal fragen, ist es überhaupt eine Alternative, also Quick Freeze? Und ich höre immer irgendwie, wird so dargestellt, als sei das eine Alternative oder sind vielmehr andere Sachverhalte betroffen? Und auch eine andere schon gestellte Frage, möchte ich gerne in diesem selben Zusammenhang gerne noch mal verstehen wollen, nämlich, weil jetzt schon zweimal von Sachverständigen gesagt worden ist, man könne quasi Surfverhalten irgendwie nachvollziehen. Das verstehe ich sachlich und fachlich nicht. Also zum einen glaube ich, gibt es ja schon Ermittlungsmaßnahmen, wo man Server überwachen kann, und Onlinedurchsuchung machen kann? Aber könnte jetzt, sagen wir mal, jetzt die Telekom Surfverhalten nachvollziehen, wenn IP-Adressen gespeichert würden? Also, das würde ich gerne noch mal verstehen, habe ich bisher einfach nicht. Dann würde ich von Herr Dr. Krause gerne wissen, ich würde auch noch mal eine andere grundrechtsbasierte Frage stellen. Ich habe so ein bisschen auch als Nichtjurist mir erlaubt, ein bisschen rumzusurfen und habe ein paar Urteile des Bundesverfassungsgerichts gefunden, die unter anderem ausgesagt haben, dass Rechtsstaatsprinzip auch die Berücksichtigung der Belange einer funktionsfähigen Strafrechtspflege beinhaltet oder "die Verhinderung, Verfolgung, Aufklärung von Straftaten kommt nach dem Grundgesetz eine hohe Bedeutung zu". Da gibt es zahlreiche Fundstellen, würde diesen Anker, diesen verfassungsrechtlichen, gerne vor dem Hintergrund zweier Themen, die damit verwoben sind, gerne noch notwendiger Weise verstehen. Der eine Teil bezieht sich da, und das haben Sie im Prinzip deutlich gemacht, das haben wir noch nicht so gesagt. Es gibt bisher nur einen Quick-Freeze-Vorschlag und der ist ja verbunden mit einer IP-Adressenspeicherung. Also ich habe zumindest keine andere Quelle als den Vorschlag von Frau Leuthäuser-Schnarrenberger gefunden. Und da war notwendige Voraussetzung für Quick Freeze ja IP-Adressenspeicherung. Wir haben das aber bisher immer gesondert diskutiert. Das würde ich gerne in dem Zusammenhang verstehen und einen Aspekt, der gar nicht beleuchtet worden ist in dem Zusammenhang. Sie sagen, Quick Freeze würde voraussetzen, dass komplett neue Speicher- und Auskunftssysteme geschaffen werden müssten. Was bedeutet das aus Sicht der Provider für den finanziellen und administrativen Aufwand, wenn Sie das noch mal ausschöpfen könnten? Das haben Sie kurz angesprochen. Das ist, glaube ich, auch ein relevanter Aspekt.

Die **Vorsitzende**: Vielen Dank. Als Nächster hat das Wort Kollege Plum.

Abg. **Dr. Martin Plum** (CDU/CSU): Ja, vielen Dank. Meine erste Frage möchte ich stellen an Herrn Dr. Piechaczek. Sie haben die Praxis der Telekommunikationsunternehmen angesprochen, wie lange heute in der Regel die IP-Adressen gespeichert werden, haben gesagt, das sind so rund sieben Tage. Ist das eine allgemeine Praxis? Gibt es da Unterschiede bei den Telekommunikationsunternehmen und werden die Daten vollständig gespeichert? Gibt es da Lücken, Unterschiede? Was ist insbesondere mit der jetzt auch vielfach thematisierten Speicherung der Portnummern neben den IP-Adressen? Die zweite Frage würde ich gerne an Herrn Professor Wollenschläger richten. Wir haben jetzt intensiv auch über die EuGH-Rechtsprechung diskutiert. Ich würde an zwei Stellen mich freuen, wenn Sie da etwas beitragen können zum Begriffsverständnis. Der EuGH sagt einerseits, dass IP-Adressen gespeichert werden können. Wir haben jetzt eben gehört, es wird in Zweifel gezogen, dass das auch die Portnummern umfasst. Teilen Sie die Bedenken, die da geäußert sind? Um Zum Zweiten geht es um Fälle schwerer Kriminalität. Welche Straftatbestände, Delikte fallen aus Ihrer Sicht darunter? Reden wir da insbesondere über den Bereich von Straftaten, die den sexuellen Missbrauch von Kindern betreffen? Wirkt sich da möglicherweise auch eine Strafrahmenverschiebung aus, die derzeit diskutiert wird, und welche anderen Deliktsbereiche können hiervon noch erfasst sein?

Die **Vorsitzende**: Danke, dann hat das Wort Kollege Jacobi.

Abg. **Fabian Jacobi** (AfD): Ja, vielen Dank. Ich habe für diese Runde eine eher technische Frage. Eine Frage, die ich richten möchte, sowohl an Herrn Danisch als auch an Herrn Jennissen. Sinn und Zweck der ganzen Veranstaltung, über die wir hier reden, ist das letztlich eine vorhandene,

irgendwie ermittelte IP-Adresse einem Nutzer einer Person zuzuordnen und das dann möglichst, da es um Strafverfolgung geht, auch gerichtsfest, also beweisverwertbar. Nun spricht der CDU-Antrag selbst schon an, dass über die eigentliche IP-Adresse hinaus auch die sogenannte Portnummer gespeichert werden soll. Das liegt daran, nach meiner Kenntnis, man korrigiere mich gegebenenfalls, dass die nackte IP-Adresse in vielen Fällen eben nicht ausreicht, um einen tatsächlichen Internetnutzer zu identifizieren oder eine konkrete Internetnutzung, die strafbarer Natur sein soll, einer Person zuzuordnen. Es sind also danach weitere Daten über die IP-Adresse selbst hinaus zu erheben und zu speichern, wobei ich den technischen Ausführungen des Sachverständigen Danisch in seiner schriftlichen Ausarbeitung, Seite 12 bis 17, meine ich zu entnehmen, dass diese weitergehenden Daten üblicherweise bisher bei den Internetanbietern gar nicht erhoben oder gespeichert werden, sondern dies erst zukünftig dann angeordnet werden müsste, dass sie die speichern müssen. Und in diesem Kontext, entnehme ich den Ausführungen an eben genannter Stelle, dass in vielen Fällen die technische Beschaffenheit des Internets mit der vermischten Nutzung von verschiedenen Internetprotokollen, Version vier, Version sechs, dazu führt, dass die zusätzlichen Daten im Rahmen der Porterfassung, die dann erst gespeichert werden müssten, in einer sehr hohen Frequenz bis in den Sekunden oder sogar Mikrosekundenbereich hinein fluktuieren. Dieses verbunden mit den weiteren Ausführungen in dem erwähnten schriftlichen Bericht, das die technische Zeiterfassung bei Internetnutzenden Geräten mit gewissen Unsauberkeiten oder Unsicherheiten behaftet ist, vielfältig die Systemzeit von entsprechenden Maschinen nicht wirklich geeicht, kalibriert ist, sodass solche Fluktuationen und Abweichungen in sehr engem, sehr kurzen Zeittakt dazu führen können, dass eine Zuordnung technisch am Ende de facto nicht mehr wirklich möglich ist. Meine Frage deshalb, inwieweit ist der Antrag, über den wir hier reden, von der Fraktion CDU/CSU unter technischen Aspekten zielführend? Inwieweit ist es möglich, auf diesem Wege, der hier vorgeschlagen wird, eine gerichtsfeste Zuordnung eines Internetnutzers zu einem Internetnutzungsvorgang am Ende überhaupt vorzunehmen? Oder inwieweit sind die technischen Gegebenheiten so, dass man diesen Beweiswert, diese eindeutige Zuordnung dann eben mit höchsten Zweifeln sehen muss oder zumindest mit Zweifeln, die eine Gerichtsverwertbarkeit doch stark beeinträchtigen? Das wäre meine Frage.

Die **Vorsitzende**: Das war an die eine Frage an die beiden. Vielen Dank! Dann hat als Nächster das Wort Dr. Lieb.

Abg. **Dr. Thorsten Lieb** (FDP): Vielen herzlichen Dank, Frau Vorsitzende. Ganz herzlichen Dank an die Sachverständigen für den Vortrag. Ich habe eine Frage an Herrn Dr. Hiéramente und eine Frage an Herrn Professor Dr. Kelber. In Richtung von Herrn Hiéramente geht die Frage zu dem Vergleich zwischen dem, was der EuGH jetzt entschieden hat, nämlich nur ein möglichst beschränkter Zeitpunkt im Lichte des Antrages, der auf sechs Monate abzielt? Vor dem Hintergrund, dass der Europäische Gerichtshof vor vielen Jahren, ist ja fast schon Rechtsgeschichte, zur Vorratsdatenspeicherungsrichtlinie mal entschieden hatte, dass ein Jahr jedenfalls zu lang sei und gegen europäisches Recht verstößt. Da bitte ich Sie um eine Einordnung, wie Sie in einem zeitlichen Korridor zwischen sechs Monaten und einem Jahr das juristisch einschätzen? In Ihre Richtung, Professor Kelber, weil Sie es vorhin auch angedeutet haben, würde ich gerne das Thema noch mal vertiefen, was die Eingriffsqualität, wenn ich es so formulieren darf, im Vergleich von reiner IP-Adressenspeicherung zu dem zusätzlich in dem Antrag adressierten Thema der Portspeicherung, über welche zusätzlichen Daten wir da sprechen, und wie sieht das dementsprechend im Lichte der EuGH-Rechtsprechung, die das nicht konkret anspricht, beurteilen? Vielen Dank.

Die **Vorsitzende**: Dann hat sich gemeldet Kollegin Domscheit-Berg.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Ja, herzlichen Dank. Ich habe zwei Fragen an den Vertreter der digitalen Gesellschaft, Tom Jennissen. Und zwar bezieht sich die Union in ihrem Antrag auch auf das EuGH-Urteil, suggeriert aber, dass ihr Antrag konform wäre mit dem EuGH-Urteil. Sachverständiger Tom Jennissen schreibt jedoch in seiner Stellung-

nahme, dass das eben nicht so ist und verweist unter anderem auf zwei Aspekte, nämlich einmal auf diese sechs-Monats-Frist und zum anderen auf die Speicherung der Portnummern. Und beide kommen ja in der Form in dem Urteil gar nicht vor. Deswegen würde ich gern Tom Jennissen fragen: Warum sind denn schon diese beiden Aspekte, die sechs Monatsspeicherfrist und die anlasslose Speicherung der Portnummern ein wahrscheinlicher Verstoß gegen europäische Grundrechte? Meine zweite Frage wäre auch an Tom Jennissen, der in seiner Stellungnahme kritisiert, dass die von der Union vorgeschlagene anlasslose Vorratsdatenspeicherung eben nicht verhältnismäßig sei, da es auch grundrechtssensiblere Alternativen gibt, die geeigneter sind, das gewünschte Ziel, über das wir uns ja einig sind, zu erreichen. Und da wüsste ich gerne, da hier oft nur Quick Freeze genannt worden ist, welche auch nicht technischen, aber auch sonstigen technischen Alternativen meinen Sie denn, die als Alternativen mit weniger Grundrechtseingriff in Frage kämen?

Die **Vorsitzende**: Vielen Dank, Kollege Baldy.

Abg. **Daniel Baldy** (SPD): Danke schön. Meine Frage ginge an Frau Link. Es gibt ein Positionspapier des BKA vom Juli dieses Jahres, wo dargestellt wird, wie mit den Daten der NCMEC verfahren wird, dass wir 75 Prozent Erfolgsquote haben, 41 Prozent davon aufgrund der IP-Adressen die noch da sind. Die restlichen Prozente, 28 Prozent, über die Telefonnummernverfolgung und 6 Prozent über die Mailverfolgung und in demselben Positionspapier gibt es dann eine Art Tabelle, die davon ausgeht, bei welchem hypothetischen Tages- oder Speicherlängen wir welche hypothetische Erfolgsquote haben. Bei sieben Tagen sind es dann um die 80 Prozent, bei 14 Tagen um die 90 Prozent. Und gleichzeitig wird sich das ja aber auch irgendwann, IP-Adressen, Telefonnummern, Mails, ab einer gewissen Speicherlänge ja auch miteinander verrechnen, weil sonst wären wir ja bei einer Erfolgsquote von über 100 Prozent, was zwar wünschenswert wäre, aber mathematisch ja dann noch schwierig. Deshalb meine Frage. An welcher Stelle, sagen wir jetzt mal sieben oder 14 Tage Speicherlänge, was so Ihre Prognose wäre, bei welcher Erfolgsquote wir dann insgesamt wären, IP-Adressen plus Mails plus Telefonnummer? Danke schön.

Abg. **Elisabeth Winkelmeier-Becker** (CDU/CSU): Ich selbst möchte auch noch mal eine Frage stellen an Frau Marina Hackenbroch. Und zwar: Wir müssen ja eine Abwägung treffen zwischen verschiedenen Grundrechtseingriffe, verschiedenen Rechten? Und deshalb wäre mir noch mal wichtig, wirklich ganz genau zu sagen, welche Gefahren drohen bei einer IP-Adressenspeicherung, die, in der Tat, zu unterscheiden ist von einer Vorratsdatenspeicherung? Hier geht es nur um die Kontakte zwischen zwei Computern, nicht um Standortdaten, geschweige denn um Inhalte? Was wäre jetzt im Worst-Case-Szenario seitens des Staates daraus abzulesen oder auch seitens eines Hackers, welche Gefahren sehen Sie da? Sehen Sie da die Gefahr einer Profilbildung, wie hier gesagt wurde? Und die gleiche Frage würde ich dann auch noch richten an Dr. Krause. Vielen Dank. Und dann starten wir in die Antwortrunde und damit beginnt Professor Dr. Wollenschläger. Sie hatten vier Fragen, nämlich von Dr. Ullrich zwei, eine von Dr. Krings und eine von Dr. Plum. Theoretisch würde das zu sechs Minuten berechtigen. Ich würde aber alle bitten, möglichst kurz sich zu fassen und das nicht auszuschöpfen. Sie haben das Wort.

SV **Prof. Dr. Ferdinand Wollenschläger:** Genau. Dann fange ich an. Ich kann vielleicht auch insofern zusammenfassen, als Herr Ullrich und Herr Krings sich ja beide auf die Angemessenheit bezogen haben und auch da noch mal eine Klarstellung wollten. Das ist ebenso, dass der Europäische Gerichtshof, wie auch das Bundesverfassungsgericht, mal für die allgemeine Speicherung von Verkehrs- und Standortdaten von hohen Eingriffsintensität ausgeht, wegen der großen Streubreite, zumal auch, nicht in Bezug zu konkreten Straftaten stehende Personen, betroffen sind. Er verweist auf die große Aussagekraft der Daten und auch auf die abschreckende Wirkung, die aus einem solchen Datenvolumen resultieren kann und auch auf die Missbrauchsgefahren. Der Europäische Gerichtshof differenziert dann aber bei einer Abwägung zwischen verschiedenen Datenkategorien, die hier eben bei den TK-Standorten und Verkehrsdaten für besonders hoch erachtet.

Die IP-Adressen attestiert der Europäische Gerichtshof demgegenüber einen, wie es in der Rechtsprechung heißt, geringeren Sensibilitätsgrad, weil eben, mit Blick auf die erwähnten Aspekte, weniger Informationen als über den Kommunikationsadressaten zum Beispiel ablesbar sind und deswegen wird eben auch anders als die allgemeine TK Standort- und Verkehrsdatenspeicherung unter den skizzierten Voraussetzungen hier eine anlasslose Speicherung der IP-Adressen für generell zulässig erachtet. Herr Ullrich hatte mich da noch gefragt: Ist nicht, wenn man zu dem Ergebnis kommt, dass das Quick-Freeze-Verfahren kein gleich effektives Mittel ist, daraus zu schließen, dass schon aufgrund staatlicher Schutzpflichten der Gesetzgeber gehalten wäre, hier von dieser Maßnahme abzusehen? Da ist es wichtig, man muss zwei Aspekte unterscheiden. Einmal die Frage der erforderlichen Zeit im Rahmen der Verhältnismäßigkeitsprüfung, für die sich mit Blick auf das Quick-Freeze-Verfahren die Frage stellt, ist es nicht nur milder, sondern genauso wirksam wie die generelle Adressspeicherung, was aus den genannten Gründen Sicherstellung, keine Sicherstellung der Speicherung zu verneinen ist. Eine andere Frage ist aber daraus abzuleiten, dass eine staatliche Schutzpflicht bestünde. Für Schutzpflichten ist festzuhalten, dass da nur das sogenannte Untermaßverbot greift, da ist der Gesetzgeber nicht verpflichtet, auf das effektivste Mittel zu rekurrieren, sondern eher auch in Abwägung, eben dieses Grundrechtskonflikt von Freiheit und Sicherheit, eine angemessene Gefahrenbekämpfung, Straftatenverfolgung gewährleisten muss. Da ist die Frage nach dem Quick Freeze Verfahren primär eine fachliche Frage, meines Erachtens. Nachdem, was ich gelesen habe, kann man aber nicht sagen, dass das Untermaßverbot jetzt hier betroffen ist, wenn man jetzt die IP-Speicherung nicht einführen würde. Frage, bestehen einer Schutzpflicht zu unterscheiden von weitem Spielraum eben bei der Realisierung. Dann zu Herrn Dr. Plum. Sie hatten einmal gefragt nach der Frage: Was lässt sich über den Unionsantrag hinaus noch unter schwere Kriminalität fassen? Da ist es nun so, dass anders als das Bundesverfassungsgericht, der Europäische Gerichtshof das jetzt noch nicht weiter konkretisiert hat. Man findet in dieser alten Digital-Rights-Entscheidung aus dem Jahr 2014 einen Verweis auf die organisierte Kriminalität und den Terrorismus. Im Übrigen ist der Begriff der schweren Kriminalität ein Begriff, den das Primärrecht verwendet, in bestimmten Bestimmungen im Bereich des Strafrechts. Und da enthält dann die Eurojust-Verordnung und die Europol-Verordnung Konkretisierungen auch im Anhang. Da ist allerdings der Straftatenkatalog weit. Da sind zum Beispiel allgemein Betrugsdelikte genannt. Da wird man jetzt sicherlich nicht für jedes Betrugsdelikt sagen können, dass da automatisch ein Zugriff gerechtfertigt ist, sondern da wird man sich dann eher an der Rechtsprechung des Bundesverfassungsgerichts orientieren müssen, die ja zum Beispiel in der Entscheidung aus dem hundertfünfzigsten Band zur Vorratsdatenspeicherung festgehalten hat, dass es eben eine schwere Straftat sein muss, was primär am Strafrahmen abzulesen ist und dass auch beim Zugriff im Einzelfall auch die Tat im Einzelfall entsprechend schwer wiegen muss. Letzter Punkt dazu: Die Bundesverfassungsgerichtsrechtsprechung, sowohl zur Vorratsdatenspeicherung als auch zur Bestandsdatenauskunft lässt anklingen, dass eine auf die IP-Adressspeicherung beschränkte anlasslose Speicherung unter Umständen unterhalb einer geringeren Gefahrenschwelle denkbar wäre. Das ist allerdings auf der Basis der EuGH-Rechtsprechung nicht zulässig. Aber, wenn man da Inspiration sucht, wäre der Verweis derjenige auf das Bundesverfassungsgericht, der ja auch rechtlich relevant ist, denn insoweit besteht Spielraum, auch für die Definition der schweren Kriminalität. Diese Rechtsprechung ist noch relevant. Und vielleicht noch ein Satz zu den Portnummern. Ich denke, da gab es ja auch noch weitere Fragen, die Sie dann gerade auch technisch noch aufklären werden. Da würde ich den Europäischen Gerichtshof so verstehen, dass sofern die Portnummer zusätzlich zur IP-Adresse notwendig ist zur Identifikation, dass auch wegen eines vergleichbaren Sensibilitätsgrades noch gedeckt ist. Dazu finden sich auch Ausführungen in meiner Stellungnahme. Da bin ich auch noch unter den acht Minuten geblieben.

Die **Vorsitzende**: Ja, wunderbar. Vielen Dank. Dann antwortet nun Frau Dr. Witting auf die Frage vom Kollegen Limburg.

SVe **Dr. Sabine Witting**: Vielen Dank für Ihre Frage, Herr Limburg. Aufgrund der begrenzten Zeit möchte ich mich hauptsächlich auf das Löschen von Darstellungen beschränken. Aber Sie finden weitere Ausführungen zu milderen Maßnahmen auch in meiner Stellungnahme. Das Löschen von Inhalten, ist ja eben nicht nur wichtig, um das weitere Verbreiten zu bekämpfen, sondern vor allem auch deswegen, um zielgerichtet Foren zu stören und, um eben auch die Normalisierung von solchen Darstellungen in solchen Foren entgegenzuwirken. Und wir haben ja schon die Löschen-statt-Sperren-Initiative, wo das BKA auf Grundlage von Hinweisen tätig wird und eben Löschungen vornimmt. Und das ist natürlich eine sehr begrüßenswerte Initiative. Aber aufgrund der schieren Menge der Inhalte ist eben fraglich, ob dieses gegenwärtige Engagement in diesem Bereich ausreicht. Und im Vergleich: Wir haben einen Versuch, wo Panorama Journalisten rund 80.000 Links innerhalb von wenigen Stunden gesammelt haben und die waren dann innerhalb von zwei Tagen offline. Und wenn man sich im Vergleich die Daten des BKA anschaut, dann liegen die Links, die das BKA hat löschen lassen, letztes Jahr um ein Vielfaches geringer als in diesem Versuch. Die Frage ist also nun, wie können wir im Bereich des Löschens von Proaktiva tätig werden, unabhängig davon, ob Hinweise eingegangen sind. Ein Kernproblem scheint eben hier zu sein, ob das BKA zuständig ist, oder die Staatsanwaltschaft. Das BKA sagt, sie können nur handeln, wenn es ihnen von der Staatsanwaltschaft angeordnet ist. Die Staatsanwaltschaft sagt: Es ist nicht unsere Aufgabe. Das ist eine Gefahrenabwehrrechtliche Aufgabe. Und dafür wäre das BKA zu zuständig. Also, falls das proaktive Löschen in den Verantwortungsbereich des BKA fällt, ist eben die Frage, ob dazu noch eine rechtliche Grundlage benötigt wird. Und das hängt wiederum maßgeblich davon ab, ob das BKA das Löschen anordnet oder nur das Löschen anregt, also, ob es rechtsverbindlich angeordnet wird oder eben nicht rechtsverbindlich angeregt wird. Und da muss man natürlich auch beachten, dass in diesem Bereich keine aktuell laufenden Beweissicherungsverfahren, Ermittlungsgefahren im In- und Ausland gefährdet werden, aber während das Löschen eben noch eine hohe Priorität hatte, letztes Jahr in der Innenministerkonferenz, ist es eben dieses Jahr völlig von der Tagesordnung verschwunden, zugunsten der IP-Vorratsdatenspeicherung. Und das halte ich für das völlig falsche Signal. Und das ist eben ein Bereich, in dem wir auf jeden Fall mehr investieren müssten, sowohl rechtlich als auch mit Ressourcen. Vielen Dank!

Die **Vorsitzende**: Vielen Dank. Dann antwortet Dr. Piechaczek auf Dr. Plum.

SV **Dr. Oliver Piechaczek**: Ja, ich kann mich in der Tat recht kurzfassen. Die Praxis der Anbieter. Da muss man zum Verständnis vielleicht noch mal klar machen, die Anbieter speichern aus Gründen der Störungsbeseitigung, zu Abrechnungszwecken und zur Missbrauchsbekämpfung. Und das ist eben abhängig auch vom Geschäftsmodell, auch was da abgerechnet wird. Deswegen kann man die gegenwärtige Praxis abfragen und das BKA, vielleicht kann die Frau Link möglicherweise noch was dazu sagen? Wir haben eben in der Spitze sieben Tage. Aber es gibt auch Anbieter, die durchaus darunter liegen, was auch in der Praxis teilweise ganz erhebliche Folgen zeigen kann. Zu dem Thema Ports: Die werden bei der gegenwärtigen Praxis nicht gespeichert. Das ist eben mit einem enormen Aufwand verbunden und deswegen wäre hier eine gesetzliche Regelung tatsächlich erforderlich. Danke schön.

Die **Vorsitzende**: Vielen Dank. Es antwortet dann Herr Moini auf die Frage von Herrn Limburg.

SV **Dr. Bijan Moini**: Danke schön. Ich wurde zu einer rechtspolitischen Einordnung und der Frage des Spannungsverhältnisses zwischen Individualinteressen und Allgemeininteressen gefragt. Und was uns in diesem Zusammenhang auffällt, ist, dass Gesetzesvorhaben, die neue Instrumente für die Ermittlungsbehörden einführen sollen, in der Vergangenheit oft mit dem Kampf gegen den Terrorismus begründet wurden. Und jetzt der Kindesmissbrauch, auch ein wichtiges Thema, gar keine Frage. Aber nach unserem Eindruck wird das einfach häufig verwendet als, oder nicht verwendet, sondern es ist absehbar, dass es Begehrlichkeiten weckt, die über diesen Anwendungsbereich der-- Ich bin das nicht gewohnt, dass man dazwischen spricht.

(Unverständlicher Zwischenruf)

Die **Vorsitzende**: Nein, nein, nein! Schluss, Schluss! Herr Dr. Moini hat das Wort.

SV **Dr. Bijan Moini**: Also, ich habe überhaupt nichts unterstellt. Aber, dass es Möglichkeiten schafft, auf die dann andere Behörden unter anderen Bedingungen zugreifen möchten. Also, jetzt geht es um Strafverfolgung hinsichtlich des Kindesmissbrauchs. Es ist absehbar und das ist auch in Stellungnahmen schon mündlich und schriftlich angeklungen, dass auch Interessen bestehen, Gefahrenabwehr zu stützen auf IP-Adressverarbeitung, dass es auch nicht nur um Kindesmissbrauch gehen könnte, sondern auch um andere Phänomenbereiche. Alles legitime Interessen, aber trotzdem setzt das einfach eine Entwicklung in Gang, die wir problematisch finden. Auch Nachrichtendienste können Begehrlichkeiten entwickeln, die auf diese IP-Adressen gerichtet sind und das summiert sich dann auf und wir plädieren dafür, das einfach zu berücksichtigen, dass wenn man solche Instrumente einführt zur Massenüberwachung, dass die einfach diese Begehrlichkeiten wecken und sich dann neue Initiativen daran anknüpfen können und ein Bereich, der jetzt auch politisch gerade aktuell diskutiert wird, sind die sogenannten Chatkontrollen. Auch dort geht es erst mal um Kindesmissbrauch. Auch das ein wichtiges Anliegen, keine Frage. Aber natürlich haben auch andere Phänomenbereiche ein Interesse daran, Chats zu kontrollieren. Und es kann auch zu anderen Zwecken eingesetzt werden. Und das wird dann auch legitim klingen. Das heißt, ich plädiere einfach dafür, all das schon zu berücksichtigen, wenn man ein solches Instrument neu einführt und es nicht nur jetzt auch juristisch streng auf diesen einen Anwendungsbereich isoliert zu bewerten, sondern eben diese Entwicklung vorherzusehen und das ganzheitlich zu betrachten.

Die **Vorsitzende**: Vielen Dank! Es hat dann das Wort Frau Martina Link. Sie hatten Fragen von Dr. Krings, von Herrn Kollegen Jung und Kollegen Baldy.

SVe **Martina Link**: Ja, vielen Dank. Ich beginne mal mit der Frage von Herrn Dr. Krings. Stichwort Bildung von Profilen. Profile könnte man dann bilden, wenn man den Telekommunikations-dienstanbieter abfragen würde, uns mitzuteilen, alle IP-Adressen zum Anschluss einer Person herauszugeben. Das heißt, dass ich auf dieser Basis dann die Möglichkeit hätte, natürlich das Telekommunikationsverhalten in diesem Zeitraum, den ich dann anfrage, zu rekonstruieren. Das, worum es hier geht, ist aber der genau umgekehrte Ansatz. Ich weiß, was ein Täter gemacht hat. Ich weiß, er hat auch Zugriff auf eine kinderpornografische Seite oder irgendwelche Tausche gemacht und mir geht es jetzt darum, festzustellen, von welchem Anschluss diese Aktivität erfolgt ist. Das heißt, hier geht es überhaupt nicht um Profile, sondern wir kennen den Zugang. Wir wissen nur nicht, wer ist derjenige, von dem dieser Zugang ausgegangen ist. Und deshalb können mit dieser Art und Weise von Überprüfungen auch keinerlei Profile erstellt werden. Zur Frage Quick Freeze von Herrn Jung, warum das aus unserer Sicht nicht geeignet ist. Quick Freeze zielt darauf, eine anlassbezogene Speicherung in Bezug auf tatrelevante Daten, also beispielsweise Verbindungs- und Standortdaten, herzustellen. Wenn ich aber bei Straftaten im Internet solche Daten dann auch einfrieren möchte, muss ich ja zunächst mal den Anschluss der Betroffenen feststellen, nämlich über Zuordnung der IP-Adresse zu einem Kunden. Und wenn ich eine solche Zuordnung nicht oder nicht mehr gespeichert habe, ist es mir auch nicht möglich, den entsprechenden Anschluss festzustellen. Und deshalb ist für diese und ausdrücklich für diese Art und Weise, das heißt für die Identifizierung eines Täters, diese Maßnahme nicht geeignet. Und zur letzten Frage von Herrn Baldy zum Positionspapier. Die 41 Prozent Erfolgsquote basieren darauf, dass die IP-Adressen vorhanden und gespeichert waren. Es gab dann zwei Möglichkeiten, wenn das nicht zum Erfolg geführt hat. Zum einen, weil die Verfristung eingetreten ist, das heißt die Speicherdauer zu kurz gewesen ist. Zum anderen, wenn es Fälle gab, in denen keine Portadresse dazu gespeichert war oder aber auch beispielsweise Hotspots, WLAN-Anschlüsse genutzt worden sind. Hier haben wir keine explizite Auflistung, wann das in welchen Fällen gewesen ist, weil uns diese Informationen von den Providern nicht gegeben werden. Dort, wo wir über die IP-Adresse nicht zum Erfolg gekommen sind, haben wir den nächsten Schritt gemacht, über Telefonnummern oder E-Mail-Adressen in den Ermittlungen zum Erfolg zu kommen. Und da

ist der Anteil eben deutlich geringer. Bei den Telefonnummern immerhin noch 28 Prozent und bei den E-Mail-Adressen 6 Prozent. Insofern ist die Aussage, wie jetzt eine hypothetische Erfolgsquote aussähe, wenn man jetzt alle drei hätte, und das gespeichert würde, aus meiner Sicht nicht möglich. Wir gehen davon aus, dass wir die IP-Adressen als werthaltigsten und erfolgsträchtigsten Ansatz, wenn wir hier Speicherfristen haben, für den Prozess NCMEC, habe ich gesagt, 2 bis 3 Wochen wären hier aus unserer Sicht schon ein signifikanter Gewinn, bei dem wir davon ausgehen, dass wir die Rate von 41 Prozent auf bis zu 80 Prozent steigern könnten. Und die 80 Prozent sind deshalb niedriger als die 90 Prozent, die in dieser Tabelle ausgewiesen sind, weil wir eben berücksichtigen müssen, dass es auch Hotspotanschlüsse gibt und andere Informationen, sodass selbst eine IP-Adresse nicht zum Erfolg führt.

Die **Vorsitzende**: Vielen Dank. Dann hat als Nächster das Wort Dr. Krause. Sie hatten Fragen von Kollegen Fiedler und von mir.

SV **Dr. Benjamin Krause**: Ich möchte auf diese beiden Punkte eingehen, nämlich einerseits zur Frage: Gibt es Möglichkeiten zur Profilbildung für die Strafverfolgungsbehörden und zum anderen zur Frage: Welche Bedeutung für die Praxis hätte denn das Quick-Freeze-Verfahren? Zur ersten Frage, Profilbildung. Da kann ich mich Frau Link nur anschließen und ich möchte Ihnen gerne kurz schildern, wie das in der Praxis denn ablaufen würde. Wir würden mit einem Gerichtsbeschluss, den wir erwirken bei den Telekommunikationsdienstanbietern, also bei den Internetzugangsdiensten die Daten bekommen, welche IP-Adressen waren denn dieser jeweiligen Anschlussperson zugeordnet? Und diese Daten dieser IP-Adressen, die sind aus sich heraus erst mal zunächst nicht aussagekräftig. Das heißt wir müssten zu den jeweiligen IP-Adressen, die wir dann haben, weitere Ermittlungen machen und das ist teilweise faktisch überhaupt nicht möglich. Es ist angesprochen worden, zum Beispiel Suchbegriffe, die man bei Internetsuchmaschinen eingibt, nachzuvollziehen. Das ist faktisch nicht möglich, dass wir mit diesen IP-Adressen beispielsweise an Google herantreten und sagen: Google sagt uns mal, welcher Kunde von euch ist denn dann und dann mit der IP-Adresse gekommen? Welche Suchbegriffe hat er eingegeben? Das ist in der Praxis für uns nicht möglich und diese Profilbildung ist faktisch schlichtweg für uns nicht durchzuführen. Zweite Frage: Was bedeutet Quick Freeze für die Praxis und der Strafverfolgungsbehörden und für die Provider? Herr Fiedler, es ist richtig, 2011 hat es schon einen entsprechenden Entwurf gegeben. Damals war Quick Freeze für die Telefonie vorgesehen und eine begrenzte IP-Adressenspeicherung für den Bereich des Internetverkehrs, weil damals schon gesagt wurde, man muss das trennen, Telefonie und IP-Adressen, und das ist aus meiner Sicht heute genauso richtig wie damals. Für uns würde das bedeuten, Quick Freeze, dass es schon sehr viel mehr Aufwand ist, auch für die Provider im Übrigen diese zwei unterschiedlichen Regime einzurichten, nämlich für die Provider, diese müssten eine andere Datenhaltung bei sich einrichten, wenn diese Quick Freeze Sicherungsanordnungen kommen. Es müsste ein neuer Datentopf werden und das ist aus meiner Sicht natürlich ein Aufwand, der bei dieser ganzen Würdigung, die Sie zu treffen haben, natürlich auch zu berücksichtigen ist. Herzlichen Dank.

Die **Vorsitzende**: Vielen Dank. Dann hat Professor Kelber Gelegenheit zur Antwort auf Fragen von Frau Wegge und von Dr. Lieb.

SV **Prof. Ulrich Kelber**: Vielen Dank, Frau Vorsitzende. Das erste war die Frage: Warum sind IP-Adressen, insbesondere dynamische IP-Adressen nicht als Bestandsdaten, sondern als Verkehrsdaten zu werten? Der erste Blick lässt einem schon den Unterschied zwischen den sehr statischen Daten, Bestandsdaten, Name, Abrechnungsadresse und ähnlichem und der IP-Adresse, die ja nun wechseln kann, durch den ausgeschöpften IP-Adressenbereich gibt es ja im Regelfall keine statische Adresse mehr, sondern auch über die dynamische Adresse verbunden. Und ähnlich wie andere Verkehrsdaten, die Beziehungen zu zum Beispiel einem Angerufenen und hier eben zu einem etwas Aufgerufenen oder Abgerufenen darstellen lässt, ist es als Verkehrsdatum aus unserer Sicht anzusehen. Der Vergleich zum Kfz-Kennzeichen, auf der ersten Seite würde es den Datenschutzbeauftragten freuen. Wir haben lange genug gekämpft, dass Kfz-Kennzeichen und Fahrzeugidentifikationsnummern als Personen-

bezogene Daten auch angesehen werden müssen. Das wurde uns immer anders dargestellt lange, aber der Vergleich hinkt natürlich trotzdem beim Kfz-Kennzeichen, das auch wegen der Rolle des Autos selbst als Gefahrenstufe eingeführt wurde und damit einem Gegenstand zugeordnet wurde, ist ja diese Gefahr für sich nicht als Kennzeichnung des Einzelnen Geräts, sonst müssten wir statische, festzuführbare und immer zu übertragende Daten der einzelnen IP-fähigen Geräte haben. Zweitens wechselt es eben und das ist der entscheidende Unterschied. Wenn man das vergleicht, müsste man jedes Mal, wenn man losfährt und anhält, wird eigentlich ein anderes Kennzeichen zugeordnet. Das Kennzeichen kann Millisekunden vorher jemand anderes gehabt haben, vielleicht in der Nähe, vielleicht auch weiter entfernt. Je nachdem, mit welchem Fahrzeugtyp ich unterwegs bin, werden noch andere Dinge, da kommen wir gleich zu der Portnummer wieder zurück, von dem Anbieter dieses Dienstes des Kfz-Kennzeichen zuzuordnen mit gespeichert und zugeordnet und müssten dann auch aufgenommen werden. Das alles führte dazu, dass die Statistiken schwierig sind. Ich kenne keine Statistik, die mich überzeugt. Gegen die Vorratsdatenspeicherung, aber auch keine für, weil natürlich vor. Ich darf das mal ein Beispiel machen: Frau Hackenbuch hat jetzt von 200 IP-Adressen mit Deutschlandbezug gesprochen. Sind das deutsche Nutzerinnen und Nutzer gewesen? Sind 200 IP-Adressen wirklich 200 Täterinnen und Täter, die nicht ermittelt werden konnten? Oder war das ein Intensivtäter, der 200-mal zugegriffen hat? Oder war in den jüngeren Adressen einer, der auch vorher zugegriffen hat? Und die ältere IP-Adresse haben wir nicht mehr. Wir haben ihn bei den jüngeren Adressen zugeordnet. Die Statistiken sind durch diese Dynamik eigentlich alle wenig aussagefähig. Letzter Punkt, Portspeicherung. Was wird heute erst mal gespeichert? Die Bundesnetzagenturen und wir sind Regulierungsbehörde für Telekommunikation. Wir gestehen den Service-Providern zu, insbesondere zur Erkennung von Sicherheitsgefahren und Störungen, bis zu sieben Tage automatisch zu speichern. Einige speichern auch die Portnummern, andere nicht. Das ist bunt gemischt. Fallen Adressdaten auf, dürfen Sie auch über diese sieben Tage hinaus gespeichert werden. Das ist der aktuelle Stand. In den Portnummern können weitere Informationen mitgespeichert werden und deswegen entsteht daraus ein weiteres Missbrauchspotenzial. Das war der Grund, warum ich vorhin in meiner Stellungnahme gesagt habe, es bräuchte dann klare Regeln zur Speicherung, klare Regeln zum Schutz und auch klare Regeln zum Abruf dieser Daten, wenn man sich für weitere Daten entschiede.

Die **Vorsitzende**: Dann geht es weiter mit Tom Jennissen. Sie hatten Fragen von Herrn Jacobi und von Frau Domscheit-Berg.

SV **Tom Jennissen**: Ja, die haben sich ja teilweise ein bisschen überschnitten, die Fragen. Es waren verschiedene zur Speicherfrist, zu Portnummern und zu Alternativen. Zunächst zur Speicherfrist. Da wurde jetzt schon einiges zu gesagt. Noch mal, der EuGH sagt das für die Zielverfolgung auf den absolut notwendig beschränkten Zeitraum. Er macht an anderen Stellen auch klar, auch in den Urteilen, aber auch zum Beispiel im Urteil zu Digital-Rights-Island, was so eine zentrale Vorratsdatenspeicherungsentscheidung war, dass das Ganze anhand von objektiven Kriterien festzumachen ist, eine Speicherfrist. Dass sie, je länger sie ist, natürlich die Anforderung größer sind und dass das Ganze auch vollkommener Angemessenheitsprüfung unterliegt. Das bedeutet primär, dass es ganz offenkundig ein, aufgrund des vorliegenden Antrags, sechs Monate einfach mal in den Raum zu stellen, das geht gar nicht. Es kann nicht einfach willkürlich irgendeine Zahl genannt werden. Der Antrag selbst hat keine Zahlen. Es gibt Zahlen, die sind vom BKA bekannt. Die sind auch durchaus ein bisschen problematisch. Wie die zustande kommen, leider nicht ganz nachvollziehbar. Es gibt keine unabhängigen Untersuchungen. Allein dadurch, dass es erst mal willkürlich ist, würde der EuGH derzeit sagen, sechs Monate, wie kommt ihr da drauf? Was dann zeigt ist, die vom EuGH als okay erachtet werden würde, das hat auch Herr Wollschläger darauf hingewiesen, das ist ein Prozessrisiko und es ist nicht so ganz klar, was der EuGH jetzt sagt. Er hat nicht so eindeutige Ausnahmen gemacht, sondern, es kann durchaus bedeuten, dass wir dann weitere Jahre so einen legalen Limbo haben, in dem irgendwie unklar ist, wie jetzt die Rechtslage eigentlich ist. Da auf jeden Fall damit zu rechnen ist, dass das Ganze

vom Europäischen Gerichtshof vor den anderen Gerichten, Verfassungsgericht etc. landen wird. Das zu den Speicherfristen. Dazu noch eine kurze Anmerkung: Jetzt stehen nur die 2 bis 3 Wochen im Raum. Im Frühjahr gab es eine Anhörung zur Chatkontrolle, die auch schon mehrfach angesprochen wurde. Da hat zum Beispiel der Leiter der Zentralstelle Cybercrime bei der Generalstaatsanwaltschaft Düsseldorf darauf hingewiesen, dass ihnen durch, ich komme auch gleich zu den milderen Mitteln, durch tatsächlich strukturelle Änderungen in den Ermittlungsmethoden, durch eine Aufstockung von Personal etc. meinte er, dass zum Beispiel allein so sieben Tage einen deutlichen Unterschied machen würden. Das sind so die Zahlen, in denen wir uns hier befinden, die Zahlen, die wir kennen, dass es für irgendwelche anderen Ermittlungen auch aus anderen Deliktsbereichen, vielleicht eine längere Speicherung als nötig ist. Das ist alles noch offen, was da möglich ist. Auf jeden Fall besteht ein erhebliches Prozessrisiko mit dem großen Risiko der Rechtsunsicherheit auf Jahre hinweg. Zu den Portnummern. Es kam jetzt auch schon an. Portnummern sind tatsächlich deutlich Eingriffsintensiver. Mit Portnummern, auch eine dynamische IP-Adresse, wird in der Regel für einen längere Zeitraum, einige Stunden, eine Sitzung, bei einige Anbieter wechseln die im 24-Stunden-Takt, aber sie bleibt dann auch eine dynamische, bleibt erst mal für eine ganze Weile gleich. Deswegen aus der reinen Abfrage. Und daraus lassen sich auch keine Kommunikationsdaten direkt beziehen, wenn tatsächlich nur die Zuweisung gespeichert wird. Portnummern wechseln in Sekundenbruchteilen. Eine einzelne Website, die sind so aufgebaut, dass da verschiedene Menschen reinkommen. Eine dänische NGO hat mal errechnet, eine einfache Webseite, eine Nachrichtenwebseite war das, glaube ich, hat zwei *[unverständlich]* eröffnet mit jeweils unterschiedlichen Portnummern, ganz, ganz kurze Intervalle. Das ist ein Zeitstempelproblem. Das wird es dann problematisch, das rechtlicher zuzuordnen, wenn da einfach nur irgendwelche kleinen Fehler gemacht werden. Es bedeutet aber auch, dass massive Datenmenge gespeichert wird, die vielleicht nicht auf die Kommunikationsinhalte zurück Rückschlüsse erlauben, aber allein durch die Statistik, wann, wie wurden welche Portnummern gespeichert? Allein die Betrachtung, was da gespeichert wird, lässt wahnsinnig große Rückschlüsse darauf, wie Nutzungsverhalten ist, wie Lebensgewohnheiten sind, wann, wie oft. Ich sehe da einfach in der Statistik sehr, sehr detailliert, wann habe ich wie das Internet genutzt. Das führt dazu, dass tatsächlich die Portnummernspeicherung derart, also die Speicherung und nicht die Abfrage, das ist eine ganz andere Frage, aber allein die Speicherung eher zu vergleichen ist meiner Meinung nach zum Beispiel nach Standortdaten oder so was, eben weil sie Rückschlüsse auf Lebensgewohnheiten sehr detailliert möglich macht. So viel zu Portnummern, die sind keineswegs einfach nur so Anhängsel zur IP-Adresse oder so. Mildere Mittel, ja, da könnte man wahrscheinlich eine eigene Anhörung zu machen, zum Kinderschutz. Es ist evident, dass in der Prävention in dem, was da passiert, in der Aufklärung, im verantwortungsvollen Umgang mit Internet von Jugendlichen sehr viel im Argen liegt. Das kann man ewig ausführen, da muss man ansetzen. Man muss ansetzen daran, an ordentliche Prävention, dass Betroffene geschützt werden, dass eben diese Missbrauchsdarstellungen gar nicht erst entstehen, dass sie nicht kursieren. Es gibt immer einen Nahbereich, der da irgendwie involviert ist. Es gibt, die meisten Darstellungen entstehen im Nahbereich. Den muss man sich anschauen, nicht nur auf das Internet gucken, auf das Böse, sondern tatsächlich anzuschauen: Wo entstehen diese Darstellungen, wie werden sie verbreitet? Warum werden sie verbreitet, in Klassenchats, was oft die ganz große Masse ausmacht? Und da müssen wir draufschauen. Wir müssen Betroffene unterstützen, andere, mildere Mittel, andere Alternativen, Quick Freeze wurde hier schon eifrig diskutiert, das Löschen wurde angesprochen, derartigen Mittel und vor allem eine ordentliche Wissens- und Personalausstattung der Behörden und entsprechende Strukturen.

Die **Vorsitzende**: Vielen Dank, Herr Jennissen. Dann hat Herr Dr. Hiéramente das Wort.

SV **Dr. Mayeul Hiéramente**: Ja, vielen Dank für die Frage zur zeitlichen Einordnung. Wie immer, oder wie häufig, gibt es gewisse Mysterien, wenn der EuGH urteilt, und er lässt einen gewissen Spielraum zu. Allerdings, und das ist, glaube ich, das Wichtige, es kommt vielleicht nicht darauf an,

ob es sechs Monate sind oder fünfeinhalb Monate. Das ist willkürlich. Es kommt auf die Frage an, wie wir bestimmen können, was unbedingt notwendig ist. Und da scheint mir ein Ansatz zu sein, zu sagen, wir schauen uns den durchschnittlichen Bearbeitungsaufwand von Kenntniserlangung bis Antragsstellung an, das wird, bei einer hoffentlich gut ausgestatteten Polizei, vielleicht ein, zwei, drei Wochen sein, bei anderen, nicht so gut ausgestattet Polizeien und Staatsanwaltschaften leider länger. Der Ansatz, der längst gefahren wird und den halte ich für problematisch, ist, nicht auf den Zeitpunkt der Kenntniserlangung, sondern auf den Zeitpunkt der Entstehung des Datums abzustellen. Und da zeigen die Beispiele, die wir hier gehört haben, eigentlich eindeutig das Problem. Frau Link, auch Herr Dr. Krause sagte es, da ging es um die Frage der sieben Tage Speicherung durch die Provider, also die freiwillige Speicherung. Das ist weitgehend zufällig, wann man Kenntnis erlangt von einer Straftat, im Allgemeinen. Es gibt eine gewisse Wahrscheinlichkeit bei bestimmten Taten. Bei Mord erfährt man vielleicht schneller, dass jemand ermordet worden ist und dass man bestimmte Erkenntnisse braucht, aber im Allgemeinen ist es weitgehend zufällig, wann man Kenntnis von einer IP-Adresse erlangt und dementsprechend eine Regelung darauf abzustellen, wann Kenntnis erlangt wurde, zu sagen, wir brauchen eine IP-Speicherung so lange, dass wir sicher gehen können, dass in dem Zeitraum auch Kenntnis erlangt wird, ist eigentlich von vornherein zum Scheitern verurteilt. Also eine Orientierung eben an dem Zeitpunkt der Entstehung dieses Datums ist genauso zufällig, wie wir es nach derzeitiger Rechtslage haben. Nur, wir müssen es begründen vor dem EuGH und vor dem EuGH können wir nicht mit Zufälligkeiten agieren. Wir brauchen, wenn überhaupt, für den gesamten Bereich der schweren Kriminalität belastbare Statistiken, um eine Wahrscheinlichkeit zu ermitteln, wann im Durchschnitt Ermittlungsbehörden Kenntnis von einer IP-Adresse erlangen, die sie dann wiederum verproben wollen. Und ich glaube, diese belastbare Grundlage, die haben wir schlicht und ergreifend nicht. Das heißt, wenn wir das Entstehungsdatum der IP-Adresse zur Grundlage nehmen, können wir aus meiner Sicht keine Notwehr, keine Beschränkungen vornehmen, die die Voraussetzungen des EuGH erfüllt. Dementsprechend kann man nach derzeitigem Stand, aus meiner Sicht, nur auf die Bearbeitungszeit bei den Ermittlungsbehörden abstellen und dementsprechend nur eine äußerst kurze Frist rechtfertigen. Die Beispiele, die Sie genannt haben, dass ein Großteil der Erkenntnisse in den ersten Wochen zutage treten, das mag für die Entscheidungsfindung von Interesse sein, aber es sagt ja schon mal ausdrücklich, dass sechs Monate verfassungswidrig sind. Jedenfalls wenn man sich den Bereich der Kinderpornos anschaut.

Die **Vorsitzende**: Danke schön. Dann hat als Nächste das Wort Frau Marina Hackenbroch. Sie hatten Fragen von den Kollegen Jung und Fiedler und von mir.

SVe **Marina Hackenbroch**: Die Frage von Herrn Jung hat Frau Link ja schon weitestgehend beantwortet oder dazu ausgeführt. Ich würde es auch noch mal kurz einfach zusammenfassen, als dass einfach nicht alles davon abgedeckt ist, insbesondere, wenn es um Ermittlungen im Internet geht, weil wir eben die IP-Adresse brauchen, um sich daran anschließende Maßnahmen durchführen zu können, weil wir anders nicht den ja den Zugang bzw. den dahinterstehenden Anschluss finden können. Und ich würde es jetzt verquicken mit der Frage von Herrn Fiedler. Ist Quick Freeze eine Alternative? Meines Erachtens in diesem Bereich nicht. Insbesondere dann, wenn es um Ermittlungen im Internet geht. Es ist lediglich ein flankierendes Instrument, nämlich immer dann, wenn wir eine IP-Adresse haben. In dem Zeitraum, in dem noch gespeichert wurde, wird ja schnellstmöglich abgefragt. Es könnte sinnvoll sein in Fällen, in denen, aus welchen Gründen auch immer, nicht schnellstmöglich eine Abfrage gemacht werden kann, bei den Providern hinsichtlich der IP-Adresse, dass man dann sagt, okay, wir machen jetzt erst mal einen Quick Freeze, damit wir alle Daten erst mal haben und dann in Ruhe abfragen können. Andererseits, wenn wir wissen, welcher Zugang gemeint ist, könnte ja auch einfach direkt anfragen, dann müssen wir ja keinen Quick Freeze mehr machen. Das heißt, wir müssen ja dann nicht mehr einfrieren, wenn wir die Daten schon haben bzw. wissen, welche Daten das sind. Es geht also immer dann um die Sachverhalte, wenn wir eben

unbekannte Täter haben und wir IP-Adressen haben, aufgrund derer wir eben nicht mehr nachvollziehen können, welcher Anschluss genutzt wurde oder welcher Anschluss betroffen ist. Dementsprechend kann es ein flankierendes Instrument sein, insbesondere natürlich in Sachverhalten im Real Life, wie man so schön nennt, kann Quick Freeze eine Alternative sein. Das ist, glaube ich, auch unbenommen, innerhalb der Fachlichkeit hier im Bereich der Internetkriminalität eben nur in sehr eingeschränkten Fällen immer dann, wenn es schnell geht und immer dann, wenn man schnell die IP-Adresse zuordnen kann. Jetzt in Bezug auf die Frage von Herrn Fiedler zur Nachvollziehbarkeit des Surfverhalten, wurde ja schon ausgeführt: Nein, das können wir nicht. Meines Erachtens speichert oder ich hoffe, dass die Telekom die Inhalte auch nicht speichert, über die die Nutzerinnen und Nutzer zugreifen. Wenn das so wäre, würde ich mir darüber auch Gedanken machen, dass man bei der Telekom abfragen kann, wer hat denn wann wo welche Internetseite tatsächlich abgefragt? Wie dem auch sei, ich arbeite bei keinem Provider. Ich weiß aber, dass wir seitens der Strafverfolgungsbehörden diese Daten niemals abfragen würden über die IP Adresse. Herr Fiedler hat es auch schon angedeutet. Natürlich gibt es Ermittlungsinstrumente, die auch ein Surfverhalten rekonstruiert haben können oder über die wir Surfverhalten erheben können. Aber das ist nicht an eine Speicherung von IP-Adressen gekoppelt. Und jetzt Bezug nehmend auf Ihre Frage, Frau Vorsitzende. Die Abwägung von den Grundrechtseingriffen in Bezug auf den Schutz der Rechte von Betroffenen, welche Gefahren ich sehe bei der IP-Adressspeicherung. Ich glaube, das wurde deutlich, dass wir hier nicht Profile erstellen können, dass wir nicht sagen können, wer hat denn welche Internetseiten zu welchem Zeitpunkt aufgerufen, sondern dass es lediglich darum geht zu wissen, wer, wann, worauf im Internet zugegriffen hat. Dass sich daran dann Anschlussmaßnahmen anschließen, das ist ja klar. Ich würde gerne auf diesen Vergleich mit den Nummernschildern zurückgehen, denn Herr Dr. Kelber hat ja deutlich gemacht, es ist nicht nur so, wir haben ein Nummernschild, sondern dieses Nummernschild wechselt alle paar Sekunden. Das heißt, wir wissen überhaupt nicht, wer in dem Auto sitzt und selbst, wenn wir wissen, auf wen dieses Nummernschild zugelassen ist, wissen wir ja auch nicht, ob jetzt die Halterin tatsächlich auch diejenige war, die gefahren ist. Aber dafür müssen wir ja natürlich Anschlussmaßnahmen durchführen. Das heißt, wir werden dann Ermittlungsmaßnahmen durchführen, die dann natürlich wieder in Grundrechte von Menschen eingreifen kann, das ist ja klar. Aber auch das ist alles mit der Staatsanwaltschaft, mit Gerichten in der Art und Weise, wie es ja jetzt schon praktiziert wird, über die StPO in geregelten Bahnen. Letztendlich brauchen wir die Speicherung von IP-Adressen dafür, dass wir weiter ermitteln können. Das ist eigentlich die Grundlage dessen und ich sehe dort keine große Problematik hinsichtlich der Frage, wie Strafverfolgungsbehörden diese IP-Adressen, die dort gespeichert werden können, missbrauchen können. Danke schön.

Die **Vorsitzende**: Vielen Dank und dann hat Herr Danisch Gelegenheit, um auf die Frage von Herrn Jacobi zu antworten und dafür ungefähr zwei Minuten anzupeilen.

SV **Hadmut Danisch**: Ja, Danke schön. In den Antworten und den Stellungnahmen, auch den Fragen immer wieder aus russischer Seite kamen, war, dass viele technische Details.

Die **Vorsitzende**: Könnten Sie bitte das Bild wegschalten, damit die Verbindung besser zu hören ist?

SV **Hadmut Danisch**: Hören Sie mich jetzt besser?

Die **Vorsitzende**: Wir versuchen es, Sie haben das Wort.

SV **Hadmut Danisch**: Okay. Viele Details, technische Sachen, die ich heute gehört habe, sind schlicht nicht verstanden, missverstanden worden, waren einfach falsch. Und da hätte ich auch einen Kritikpunkt. Aus meiner Sicht ist das auch nicht vertretbar, Aussagen zu treffen über Dinge, die man eigentlich nie verstanden hat. Ich habe dazu ausführlich in meiner Stellungnahme geschrieben, weil jetzt hier zwei Minuten nicht ausreichen, das auszuleuchten, deswegen verweise ich auf meinen Text. Und nochmal zur direkten Antwort auf die Frage, der Hinweis, dass das Internet an sich nicht rechtssicher, auch grundsätzlich eine rechtssichere Speicherung von

IP-Adressen gar nicht möglich ist. Diese Rechtssicherheit ist ein rein juristisches Postulat, das keine Grundlage hat. Was man verstehen muss, ist, dass eine dynamisch zugewiesene IP-Adresse etwas anderes ist, als eine Network-Adress-Translation und diese Network-Adress-Translation im Wesentlichen eingesetzt wird, weil die IP-V4-Adressen knapp wurden. Und man hat vor vielen Jahren angefangen, den Endanschluss per NAT zu verschicken. Deswegen kann man also mit der IP-Adresse normalerweise nur den Anschlussinhaber, aber nicht den Täter identifizieren. Wenn es um ein Firmennetz geht oder eine WG oder so, was überhaupt nicht möglich ist, aus der IP-Adresse dann aus mehreren möglichen Verdächtigen, den Täter zu identifizieren. Und weil sich diese IP-V4-Knappheit in den letzten Jahren verschärft hat und der Vorwurf aufgebraucht ist, hat man dasselbe Verfahren, das man eigentlich nur für die Endanschlüsse, also die Wohnung oder die Firma verwendet, nochmal über die Provider gestülpt hat, also noch mal eine NAT-Schicht obendrauf. Und weil man dieses NAT nicht rechtssicher auflösen kann, ist das ganze Problem jetzt eben auf eine Etage höher, auf die Provider gestiegen. Da bitte ich aber nochmal meine Ausführung im Text. Nochmal der Hinweis: Es gibt keine rechtssichere Speicherung im Internet und ich bitte noch mal, sich drum zu kümmern, das zu verstehen.

Die **Vorsitzende**: Vielen Dank für diese Aussage.

SV **Hadmut Danisch**: Wenn man es nicht verstanden hat.

Die **Vorsitzende**: Trotz Probleme mit der Leitung, ist die Sorge, die Sie äußern wollen hier noch mal klar geworden. Und Sie verweisen auch noch mal auf Ihre schriftliche Stellungnahme. Vielen Dank dafür. Ich habe jetzt hier 1, 2, 3, 4, 5 Fragen noch mal angemeldet. Okay, sogar sechs, sieben. Wir überziehen. Jeder bitte innerhalb von 30 Sekunden eine Frage und dann gibt es auch nur noch eine Minute für die Antwort und es beginnt Carsten Müller.

Abg. **Carsten Müller (Braunschweig)** (CDU/CSU): Vielen Dank. Ich habe eine Frage an Herrn Professor Wollenschläger. Wir haben gelernt, dass die Speicherung von IP-Adressen heute im Rahmen des Betriebsablaufes bei den Providern ohnehin schon erfolgt und dann zu Abrechnungszwecken diese Adressen verwendet werden. Gibt es Besorgnisse, dass das Grundrechtseingriffe darstellen könnte, die nicht hinnehmbar sind? Ist Ihnen so etwas bekannt?

Die **Vorsitzende**: Volker Ullrich.

Abg. **Dr. Volker Ullrich** (CDU/CSU): Vielen Dank. Ich habe eine Frage an Frau Link. Gesetzt den Fall, wir würden die IP-Adressenspeicherung nicht einführen, mit welchen Zahlen an fortgesetzten, nicht aufgeklärten Fällen von sexuellem Missbrauch von Kindern müssten wir fortan leben und wie beurteilen Sie als Chefin einer großen Ermittlungsbehörde den Umstand, dass wesentliche Ermittlungsergebnisse nach wie vor vom Zufall abhängig bleiben?

Die **Vorsitzende**: Martin Plum.

Abg. **Dr. Martin Plum** (CDU/CSU): Vielen Dank. Ich habe eine Frage an Herrn Wollenschläger und sage direkt dazu, dass ich die Antwort nicht mehr hier im Saal, sondern gleich am Bildschirm weiterverfolgen werde. Sie haben gesagt, auf meine Frage, was die schwere Kriminalität angeht, dass das vermutlich unter Rückgriff auf die Rechtsprechung des Bundesverfassungsgerichts konkretisiert werden muss. Jetzt diskutieren wir gerade in der Rechtspolitik darüber, dass Paragraph 184 b Absatz 1 StGB, wo es um Verbreitung, Erwerb, Besitz kinderpornografischer Inhalte geht, reformiert werden muss. Das ist jetzt ein Verbrechenstatbestand. Es geht darum, ob das jedenfalls bei bestimmten Fallgruppen nicht mehr der Fall sein sollte. Hätte eine solche Reform, also eine Herabstufung vom Verbrechenstatbestand, Auswirkungen auf die Zulässigkeit einer IP-Adressenspeicherung in diesen Fällen?

Abg. **Elisabeth Winkelmeier-Becker** (CDU/CSU): Jetzt habe ich noch mal eine Frage an Dr. Piechaczek. Und zwar wurde verschiedentlich gesagt, dass die Informationen aus der Abfrage möglicherweise auch ein Risiko bergen, dass man hier auf eine falsche Spur kommt. Wie groß ist das Risiko, dass am Ende jemand Maßnahmen unterzogen wird, der tatsächlich gar nicht auf diesen Seiten war, sondern dass da die Ermittlungen fehlgehen? Und dann geht es weiter mit Kollegen Oellers.

Abg. **Wilfried Oellers** (CDU/CSU): Vielen Dank, Frau Vorsitzende. Meine Frage richtet sich ebenfalls an Herrn Dr. Piechaczek. Es kam in dieser Anhörung gelegentlich die Auffassung zu Tage, dass man doch vielleicht auch präventiv, gerade auch auf Opfersicht, Maßnahmen ergreifen sollte. Ist das in der Thematik, in der wir uns gerade befinden, wirklich der richtige Ansatz oder muss man nicht gerade eben auch auf Täterseite und Strafverfolgung doch den Schwerpunkt mehr legen? Danke schön.

Die **Vorsitzende**: Danke, Kollege Jacobi.

Abg. **Fabian Jacobi** (AfD): Danke schön. Ich habe noch mal eine kurze Nachfrage wiederum an Herrn Danisch und an Herrn Jennissen.

Die **Vorsitzende**: Bitte nur einen Sachverständigen.

Abg. **Fabian Jacobi** (AfD)**:** Gut, dann aufgrund der technischen Störung, beschränke ich mich dann auf Herrn Jennissen, hier im Saal. Es geht darum, eine Person zu identifizieren, die auf einen Inhalt im Internet zugegriffen hat. Das soll geschehen über die IP-Adresse, die diese Abrufe vor sich herträgt, gegebenenfalls erweitert um die Portnummer. Wie eindeutig, wie sicher, wenn hier gespeichert würde, diese Daten, wie sicher, wie zuverlässig ist feststellbar und belegbar, auch gerichtsfest nachweisbar, dass die IP-Adresse, die da gespeichert wird, auch tatsächlich echt ist, also nicht etwas ist, was sich jemand einfach nur vors Gesicht gehängt hat, wenn er da im Internet herumturnt? Könnte man beispielsweise auch den Adressraum, den hier der Deutsche Bundestag verwendet, bei einer solchen Abrufaktion verwenden und dadurch dort, wo gespeichert wird, den Eindruck erzeugen, dass also hier beispielsweise an einem bestimmten Tag 100 Abrufe von kinderpornographischen Inhalten von den Arbeitsplatzrechnern der Kollegen MdBs stattgefunden haben? Wie realistisch ist das technisch?

Die **Vorsitzende**: Danke. Dann hat Frau Domscheit-Berg noch eine Frage.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Ja, ich habe eine Frage an Sachverständigen Jennissen. Und zwar haben wir immer wieder darüber gesprochen, Evidenz hin oder her, was bringt eigentlich eine Vorratsdatenspeicherung? Da gehen offensichtlich die Meinungen auseinander. Ich wüsste gerne von Ihnen, was gibt es denn für eine Evidenz auch in der Vergangenheit, ob und wie viel eine Vorratsdatenspeicherung bringen würde an Nutzen und was sind die dem Gegenüberstellen den negativen Auswirkungen?

Die **Vorsitzende**: Und Dr. Lieb.

Abg. **Anke Domscheit-Berg** (DIE LNKE.): Ich werde auch raus müssen wegen Paralleltermine.

Die **Vorsitzende**: Das geht. Haben wir Verständnis für. Dr. Lieb.

Abg. **Dr. Thorsten Lieb** (FDP): Vielen Dank, Frau Vorsitzende. Ich habe eine Frage an Frau Link. Sie hatten mit Blick auf die, so habe ich das verstanden, da bitte ich nur um eine Bestätigung, auf die hier im Mittelpunkt stehenden Fragen von schrecklichem kinderpornographischem Material von zwei bis drei Wochen gesprochen, von einem Zeitraum. Wenn ich mal den Blick weiter auf andere schwere und schwerste Straftaten, die unterwegs sind, können Sie da aus dem Blickwinkel des BKA etwas sagen, was in anderen Terrorismus als Beispiel, vielleicht haben Sie noch andere Beispiele, was dort Zeiträume wären, über die man dann rein praktisch gesprochen diskutieren müsste?

Die **Vorsitzende**: Vielen Dank. Dann haben wir jetzt die Antworten möglichst im Stakkato. Ach, Helge Limburg, das stand noch nicht auf der Liste. Aber gut, aus Ausgewogenheitsgründen. Ja, bitte.

Abg. **Helge Limburg** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Eine zweite Frage an Frau Professor Dr. Witting. Sie gehen oder sind ja hier mehrfach eingegangen auf das Recht von Kindern auf Schutz vor sexualisierter Gewalt, ist ja zum Beispiel auch in Artikel 34 der UN-Kinderrechtskonvention normiert. Aber dort ist in Artikel 16 ja auch, das Recht von Kindern auf Schutz ihrer digitalen Privatsphäre und auf Schutz personenbezogener Daten normiert. Das wird oftmals gegeneinandergestellt, gegeneinander ausgespielt. Können Sie erläutern, warum Sie das aus kinder- oder menschenrechtlicher Sicht, wie Sie das bewerten, dieses gegeneinander ausspielen? Bzw. wie man bei einer entsprechenden Güterabwägung dann jeweils die Kinderrechte berücksichtigen müsste?

Die **Vorsitzende**: Vielen Dank. Jetzt brauchen wir die Antworten aber wirklich im Stakkato sozusagen. Und es beginnt Tom Jennissen.

SV **Tom Jennissen:** Eine echte IP-Adresse, repräsentiert einen immer, ich glaube, die Frage wurde auch schon beantwortet, weitgehend. Es gibt natürlich 1.000 Möglichkeiten, wenn ich mich hier ins WLAN des Bundestages einwähle, trotzdem habe ich eine IP-Adresse des Bundestages. Es gibt diverse Arten, das zu unterlaufen durch VPN, durch Thor, durch Proxys durch eben vor allen Dingen öffentliche WLANs. Ich glaube, die Frage wurde auch schon beantwortet und das auszuführen, ob man das dann noch mit krimineller Energie noch irgendwie anderweitig möglich ist, glaube ich, würde den Rahmen sprengen und vielleicht auch eher an das BSI zu richten sein. Eine Frage war, inwiefern Evidenz vorhanden ist. Ja, das wurde auch schon angesprochen. Es gab das Gutachten des Max-Planck-Instituts von 2011, dass sehr genau anschauen konnte, aus seiner Zeit wurde schon mal gesagt, wir brauchen unbedingt die Vorratsdatenspeicherung. Internet ist wahnsinnig wichtig und wir brauchen das. Es gibt keine, wurde seitens der Strafverfolgungsbehörden seinerzeit schon gesagt, eine Untersuchung, die sich genau anschauen konnte, Geltung von Vorratsdatenspeicherung, keine Geltung, hat gezeigt, es gibt keine belastbaren Hinweise darauf, dass die Vorratsdatenspeicherung so wahnsinnig wichtig ist. Andere Untersuchungen europaweit kommen zu ähnlichen Ergebnissen. Die vergleichen Staaten, wo es eine gibt und wo es keine gibt. Es gibt dazu tatsächlich einfach keine Gutachten. Es gibt große Zweifel daran, dass tatsächlich die Vorratsspeicherung von Daten so viel bringt, wie oft behauptet wird. Dem gegenüber steht ein massiver Grundrechtseingriff. Das wird auch vom EuGH anerkannt. Das betont das Bundesverfassungsgericht immer wieder. Auch IP-Datenspeicherung ist ein schwerwiegender Eingriff in die Grundrechte. Ich habe ausgeführt, dass das ein bisschen weitergehender ist. Das steht sich gegenüber, die Massenüberwachung der gesamten Bevölkerung versus zweifelhafte Ermittlungserfolge. Wir haben dazu keine Zahlen. Ich glaube, die werden, vielleicht warten wir mal auf die Überwachungsgesamtrechnung und anschließende Untersuchungen. Derzeit sehe ich die Voraussetzungen absolut nicht dabei. Und wir müssen mal betrachten, die Massenüberwachung der gesamten Bevölkerung hat auch politische Folgen, führt zu einer massiven Verunsicherung in der Bevölkerung, was gilt jetzt eigentlich, was nicht? Das würde so weiter gehen für eine ganze Weile, falls ein weiterer Anlauf geschehen sollte.

Die **Vorsitzende**: Danke. Dann hören wir noch mal Frau Link zu. Sie hatten Fragen von Dr. Ulrich und Dr. Lieb.

SVe **Martina Link**: Mit welchen Zahlen müssen wir leben ohne IP? Das ist davon abhängig, wie lange die Provider künftig dann aus anderen Gründen zu Geschäftszwecken ihre Daten speichern. Das können wir nicht abschätzen. Wir müssen aber davon ausgehen, dass sich die Zahlen entsprechend erhöhen. Das heißt, die Misserfolgsquote jetzt im NCMEC-Prozess deutlich über 25 Prozent liegen wird, wenn der Zeitraum der Verfügbarkeit sinkt. Das muss man dann in Bezug zu den Hinweisen, die wir bekommen, setzen. Wie gesagt, im Moment 180.000 vom NCMEC für den CSA-Prozess schätzt das statistische Bundesamt mit ungefähr 1,2 Millionen Hinweisen, die auf Deutschland zulaufen könnten. Das kann ich selbst nicht beurteilen, ob diese Zahlen kommen. Was die Speicherfrist noch mal angeht: Ja, zwei bis drei Wochen würden wir im fast automatisierten NCMEC-Prozess eine sehr hohe Erfolgsquote erzielen. In dem Zusammenhang auch noch mal zu den Aussagen von Herrn Dr. Hiéramente: Die Bearbeitungszeit bei uns dauert von der Kenntniserlangung der IP-Adresse bis zur Bestandsdatenanfrage nicht einmal einen Tag. Also, das ist der Zeitraum. Wir sind da sofort aktiv. In anderen Fällen komplexer Sachverhalte, ich möchte nur mal ein Beispiel einer sichergestellten Plattform aus dem Bereich Cybercrime bringen, wo wir dann entsprechend auch auswerten, und IP-Adressen versuchen zu generieren. Hier war es so, dass alle IP-Adressen älter als zwei Wochen waren. 15 Prozent waren 0 bis 6 Monate alt und alle anderen älter als sechs Monate. Und im Bereich komplexer Ermittlungen wissen wir tatsächlich nicht, wann wir auf solche relevanten IP-Adressen stoßen und je länger dann der Zeitraum ist, in dem man sie noch abfragen kann, umso größer ist die Erfolgschance. Aber anders als in diesem automatisierten Prozess

haben wir da natürlich keine Möglichkeit, Statistiken zu erheben.

Die **Vorsitzende**: Vielen Dank. Dann fragen wir Dr. Piechazcek, und zwar von mir kam eine Frage und von Kollegen Oellers.

SV **Dr. Oliver Piechaczek**: Ja, also zunächst mal zu Ihrer Frage, Frau Vorsitzende. Das Thema falsche Spuren, wie hoch das Risiko eine unrechtmäßige Verfolgung ist? Es ist ja nicht so, dass wir eine IP-Adresse geliefert bekommen, und dann sozusagen springt die Strafverfolgungsmaschinerie an und die ist nicht zu stoppen, sondern wir unterliegen dem Grundsatz der Verhältnismäßigkeit. Ich überlege mir bei jeder Akte ganz genau, wie ich mit diesem Fall umgehe und betrachte mir natürlich noch das Umfeld. Nicht nur die IP-Adresse zählt. Wo lebt jemand? Ich lasse ermitteln, wer, welche Personen in diesem Haus sind, kann es sich unter Umständen um eine Wohngemeinschaft handeln etc. Und erst dann, nach gründlicher Prüfung, überlege ich mir, ob ich einen Antrag stelle, ob ich in einem Vermerk niederlege, dass das dem Grundsatz der Verhältnismäßigkeit widerspricht, hier eine Durchsuchungsmaßnahme überhaupt durchzuführen. Das heißt also, um Ihre Frage auf den Punkt zu beantworten: Dieses Risiko ist moderat bis äußerst gering. Dann das Thema Prävention. Ja, das Thema Prävention kann dort gut funktionieren. Wir müssen das täterzentriert betrachten. Das Thema Prävention funktioniert dort möglicherweise gut, wo wir Täter davon abhalten, Täter zu werden. Da gibt es entsprechende Initiativen. Das kann man ausbauen, ja. Aber, was ebenso angeklungen ist, wir müssen die Kinder stärken, die Kinder, die missbraucht werden, die Kinder, die wir hier schützen müssen, und da sind wir wieder bei der Schutzpflicht. Das sind arme Kinder, das sind Kinder aus armen Familien. Da kann man in der Schule noch so viel an guten Ratschlägen geben, die Kinder verarbeiten das intellektuell möglicherweise gar nicht und vor allen Dingen treffen sie zu Hause auf eine Struktur, die das alles schlecht redet, was in der Schule passiert, und das sind unsere Missbrauchsopfer. Deswegen halte ich Prävention hier für ganz, ganz schwierig. Und auch der Zugang zu den Tätern gelingt meistens erst, wenn sie auf der Anklagebank sind, verurteilt werden und dann erst ihr Problem überhaupt realisieren. Erst dann gehe ich dazu über, da ist auch meistens das Gefängnis gar nicht die richtige Alternative, sondern dann eine Therapie zu bekommen, um diese Menschen überhaupt wieder in diese Gesellschaft zu integrieren. Aber, das ist täterzentriert und da brauchen wir effektive Strafverfolgung. Mit Softmaßnahmen in diesem Bereich kommen wir da nicht weiter.

Die **Vorsitzende**: Dann hat Frau Dr. Witting noch Gelegenheit zur Antwort auf eine Frage von Kollegen Limburg.

SV **Dr. Sabine Witting**: Vielen Dank. Es ging um die Frage, ob die Privatsphäre gegen den Kinderschutz ausgespielt wird. Und das ist natürlich sehen wir in diesen Narrativen in der heutigen Diskussion ja auch, das ist, was kinderrechtlicher Perspektive auf jeden Fall falsch. Der UN-Kinderrechtsausschuss hat klar gesagt, dass die Privatsphäre von Kindern eine Voraussetzung ist für deren Sicherheit. Also, es ist kein Gegeneinander, sondern, ohne Privatsphäre gibt es keine Sicherheit von Kindern und eben Ansätze, die eben nur auf den Kinderschutz abstellen, sind eben aus kinderrechtlicher Perspektive problematisch, weil sie Kinder als Schutzobjekte sehen und eben nicht als selbstständige Träger von Rechten. Und deswegen ist eben die Privatsphäre kein Recht, was man Kindern nicht einfach so wegwischen kann, sondern, das ist eine Voraussetzung für die Ausübung anderer Kinderrechte und auch für deren Sicherheit. Und ich möchte noch mal kurz anschließen, dass natürlich Opfer von sexualisierter Gewalt gegen Kinder aus allen Gesellschaftsschichten kommen und nicht nur aus armen Familien. Vielen Dank.

Die **Vorsitzende**: Dann hat abschließend das Wort Professor Wollenschläger. Sie hatten Fragen von Kollegen Müller und Dr. Plum.

SV **Prof. Dr. Ferdinand Wollenschläger**: Ja, vielen Dank. Herr Müller hat abgezielt auf die verschiedenen Speicherungsformen. Einmal die Speicherung aus eigenem Antrieb durch die Anbieter und dann die staatliche Speicherung. Natürlich ist es so, dass bereits die Anbieter, das hat ja Herr Kelber insbesondere ausgeführt aus Gründen der Betriebssicherheit oder sonstiger Belange, der Vertragsabwicklung, sozusagen

Vertragsdaten, IP-Adressen speichern. Das ist jetzt kein klassischer Grundrechtseingriff, weil es nicht vom Staat ausgeht, sondern von privaten Telekommunikationsunternehmen. Aber in Realisierung von Schutzpflichten hat der Staat oder die Europäische Union vielmehr hier einen Rechtsrahmen geschaffen, die eben hier auch entsprechende Speichermöglichkeiten begrenzt. Das hat der Herr Kelber ausgeführt, auch dass er eben hier das Ganze überwacht und telekommunikationsrechtlich reguliert. Das ist aber sozusagen die Speicherung durch die Betreiber. Davon zu unterscheiden ist das, worüber wir hier heute reden, sozusagen die aus repressiven und präventiven Gründen motivierte Pflicht, unabhängig vom Wollen und der Notwendigkeit zu Vertragszwecken, dass Betreiber eben staatlicherseits verpflichtet werden, diese Daten eben für einen begrenzten Zeitraum vorzuhalten. Wenn sie das tun, ohne dass es eine solche Pflicht besteht, vielleicht ein letzter Punkt, kann der Staat natürlich auf den vorhandenen Datenbestand zugreifen, wobei dann im Vergleich zur Vorratsdatenspeicherung eine geringere Eingriffsschwelle gilt.

Herr Dr. Plum hat es sich noch mal für den Begriff der schweren Kriminalität interessiert? Das ist ein europarechtlicher Begriff, dass ich da nicht missverstanden werde. Mein Verweis auf die Rechtsprechung des Bundesverfassungsgerichts hat eben dazu gedient, wenn man den jetzt ausfüllen möchte, ist eben der Befund, dass hier die Konkretisierung auf europäischer Ebene noch am Anfang steht, das Bundesverfassungsgericht hier deutlicher wurde, insbesondere unter Verweis auf das Erfordernis einer schweren Straftat, dass sich das maßgeblich nach dem Strafrahmen bestimmt und auch im Einzelfall eine hinreichende Schwere erforderlich ist. Und das beantwortet auch die Frage nach den Konsequenzen einer Änderung im Strafrahmen und einer Herabstufung eines Verbrechens zu einem Vergehen etc. Das hat Konsequenzen für die Einordnung einer Straftat. Und wenn eben der notwendige Strafrahmen, damit auch die schwere Straftat Schwere der Straftat unterschritten ist, wird eben das kein zulässiger Verwendungszweck mehr. Aber das muss man sich sozusagen fürs konkrete Delikt und den Strafrahmen dann anschauen. Vielen Dank.

Die **Vorsitzende**: Gut, dann sind so weit erst mal alle Fragen geklärt. Ich glaube, wir hatten eine sehr informative Anhörung heute. Ich danke Ihnen alle, dass Sie auch mit der Zeitüberziehung sich einverstanden erklärt haben, dass es für die meisten möglich war. Ich glaube, Ihre Argumente werden in unsere weiteren Beratungen sehr intensiv auch noch mal einfließen und von daher herzlichem Dank für Ihr Hiersein und unsere Beratung und ich wünsche Ihnen einen guten Heimweg.

Schluss der Sitzung: 14:39 Uhr

Elisabeth Winkelmeier-Becker, MdB
Vorsitzende