20. Wahlperiode

Deutscher Bundestag
Ausschuss für Digitales

Protokollauszug
der 44. Sitzung

Ausschuss für Digitales
Berlin, den 27. September 2023, 15:00 Uhr
10557 Berlin, Konrad-Adenauer-Str. 1
Sitzungssaal: PLH E.600

Vorsitz: Tabea Rößner, MdB

Tagesordnung

Tagesordnungspunkt 2 – öffentlich – Seite 03

Abschlussbericht des Untersuchungsausschusses des Europäischen Parlaments zum
Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware
Gast im Ausschuss: Sophie in ’t Veld
(Berichterstatterin des Untersuchungsausschusses)

Mitglieder des Ausschusses

	Ordentliche Mitglieder	Stellvertretende Mitglieder
SPD	Becker, Dr. Holger	Bartz, Alexander
	Kassautzki, Anna	Diedenhofen, Martin
	Klüssendorf, Tim	Esken, Saskia
	Marvi, Parsa	Hakverdi, Metin
	Mesarosch, Robin	Leiser, Kevin
	Mieves, Matthias David	Müller (Chemnitz), Detlef
	Schätzl, Johannes	Papendieck, Mathias
	Wagner, Dr. Carolin	Schneider, Daniel
	Zimmermann, Dr. Jens	Trăsnea, Ana-Maria
	Zorn, Armand	Werner, Lena
CDU/CSU	Biadacz, Marc	Bär, Dorothee
	Brandl, Dr. Reinhard	Hahn, Florian
	Durz, Hansjörg	Hauer, Matthias
	Hoppermann, Franziska	Heilmann, Thomas
	Jarzombek, Thomas	Henrichmann, Marc
	Kemmer, Ronja	Metzler, Jan
	Reichel, Dr. Markus	Müller, Florian
	Santos-Wintz, Catarina dos	Schön, Nadine
	Zippelius, Nicolas	Steiniger, Johannes
BÜNDNIS 90/DIE GRÜNEN	Außendorf, Maik	Bär, Karl
	Bacherle, Tobias B.	Christmann, Dr. Anna
	Grützmacher, Sabine	Gelbhaar, Stefan
	Khan, Misbah	Klein-Schmeink, Maria
	Rößner, Tabea	Notz, Dr. Konstantin von
FDP	Funke-Kaiser, Maximilian	Föst, Daniel
	Mordhorst, Maximilian	Höferlin, Manuel
	Redder, Dr. Volker	Konrad, Carina
	Schäffler, Frank	Kruse, Michael
AfD	Benkstein, Barbara	Höchst, Nicole
	Naujok, Edgar	Janich, Steffen
	Schmidt, Eugen	König, Jörn
	Storch, Beatrix von	Wiehle, Wolfgang
DIE LINKE.	Domscheit-Berg, Anke	Pau, Petra
	Sitte, Dr. Petra	Reichinnek, Heidi
fraktionslos	Cotar, Joana	

Tagesordnungspunkt 2 – öffentlich –

Abschlussbericht des Untersuchungsausschusses des Europäischen Parlaments zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware
Gast im Ausschuss: Sophie in 't Veld (Berichterstatterin des Untersuchungsausschusses)

Die **Vorsitzende**: Wir kommen jetzt zum öffentlichen Teil. Das ist der öffentliche Tagesordnungspunkt des Ausschusses für Digitales. Dieser Teil wird live im Internet übertragen und ist anschließend in der Mediathek des Deutschen Bundestages auf bundestag.de abrufbar. Die Besucherinnen und Besucher, die hier auf der Tribüne sitzen, möchte ich darauf hinweisen, dass auch wenn diese Sitzung öffentlich ist, das Fertigen von eigenen Ton- und Bildaufnahmen während der Sitzung nicht zulässig ist. Entsprechende Geräte sind deshalb abzuschalten. Zuwiderhandlungen gegen dieses Gebot können nach dem Hausrecht des Deutschen Bundestages nicht nur zu einem dauernden Ausschluss von den Sitzungen dieses Ausschusses sowie des ganzen Hauses führen, sondern auch strafrechtliche Konsequenzen nach sich ziehen. Wir beraten jetzt den Tagesordnungspunkt 2, Abschlussbericht des Untersuchungsausschusses des Europäischen Parlaments zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware öffentlich. Wir haben Sophie in t´ Veld als Gast im Ausschuss virtuell zugeschaltet. Sie ist die Berichterstatterin im Europaparlament des Untersuchungsausschusses. Das ist eine Selbstbefassung. Wir haben auch eine Debatte dazu. Wir haben auch weitere Gäste hier im Ausschuss, und zwar vom Bundesministerium des Innern und für Heimat (BMI). In Präsenz ist der Parlamentarische Staatssekretär Johann Saathoff hier. Herzlich willkommen. Neben ihm sitzt Andreas Könen. Er ist der Leiter der Abteilung Cyber- und Informationssicherheit. Virtuell ist uns von der Behörde des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) Christa Polfers zugeschaltet. Sie ist die Abteilungsleiterin Polizei und Nachrichtendienste beim BfDI. Herzlich willkommen an alle Gäste. Wir haben vereinbart, dass es ein Eingangsstatement gibt von fünf Minuten von Sophie in t´ Veld, der Berichterstatterin des Untersuchungsausschusses. Dann gibt es zwei Debattenrunden mit einer Redezeit von jeweils vier Minuten pro Fraktion. Wir haben hier die gute Praxis, dass wir Frage und Antworten direkt machen. Ich richte das auch an Sophie in t´ Veld und an Christa Polfers, Sie können direkt antworten, wenn Sie gefragt werden. Ich möchte noch darauf hinweisen, dass bei uns zehn Sekunden vor Ablauf der Zeit ein akustischer Gong zu hören ist. Damit wollen wir uns alle beim Zeitmanagement selbst disziplinieren. Ich übergebe das Wort an Sophie in t´ Veld. Herzlich willkommen.

Sophie in t´ Veld: Guten Tag. Sollte ich jetzt sofort anfangen?

Die **Vorsitzende**: Genau. Sie haben fünf Minuten, um einzuführen und zu berichten und dann kommen die Debattenrunden.

Sophie in t´ Veld: Es ist Ihnen wahrscheinlich bekannt, dass das Europäische Parlament zwischen März 2022 und Juni dieses Jahres einen Untersuchungsausschuss hatte. Wir haben Ende April über meinen Bericht abgestimmt, das heißt, über das, was wir herausgefunden haben. Wir haben im Juni im Plenum über die Maßnahmen abgestimmt. Seitdem ist eigentlich in den EU- Institutionen nichts passiert. Wir haben vom Europäischen Rat nichts gehört und von der Europäischen Kommission auch nicht. Man hat mir gestern gesagt, die Antwort der Europäischen Kommission ist bald zu erwarten, aber es ist eigentlich unfassbar, dass das vier Monate dauert. Das heißt, die Kommission macht eigentlich nichts und die Nationalregierung auch nicht, obwohl es doch gute Gründe für eine Reaktion, Antworten und Maßnahmen gibt. Das wurde auch mit einer sehr breiten Mehrheit im Europäischen Parlament abgestimmt. Das wurde von fast allen eigentlich mitgetragen. Ich finde es sehr besorgniserregend, dass der Missbrauch, also die Ausspähung ohne Gründe, einfach weiter geht. Seit wir im Juni abgestimmt haben, hat es immer wieder neue Enthüllungen gegeben. Ich weiß, dass es auch noch weitere Enthüllungen geben wird, und es passiert einfach nichts. Die einzige Antwort der Regierung ist Schweigen, das große Schweigen. Ich finde, das hat in einer Demokratie eigentlich keinen Platz. Das ist falsch. Es gibt auch von Nationalregierungen innerhalb der EU Missbrauch. Das wissen wir. Das wurde sowohl in Polen, Ungarn, Griechenland als teilweise auch Spanien – obwohl das eigentlich ein anderer Fall ist –

festgestellt. Das große Problem ist, dass es nicht in allen Ländern Missbrauch von Spyware gibt, aber alle Regierungen schweigen. Alle Regierungen. Ich finde das sehr besorgniserregend, denn das heißt, die Bürger können zwar zum Gerichtshof gehen, aber dort gibt es keine Auskünfte. In keinem der Hunderte von Fällen in der Europäischen Union hat es ein Urteil eines Gerichtshofs gegeben, nirgendwo in der Europäischen Union. Bürger haben keinen Zugang zu Informationen. Komischerweise haben die Hersteller von Spyware diese Informationen. Sie wissen eigentlich alles, sie haben Zugriff auf alles. In vielen Fällen hat die israelische Regierung, manchmal auch Regierungen der Drittländer, diese Informationen. Die Bürger der Europäischen Union haben eigentlich keine Informationen und auch keine Möglichkeit, etwas zu tun. Ich glaube, wenn es so ist, dass Regierungen ungestraft ihre Gegner und Kritiker ausspähen können, und wir – also Oppositionspolitiker, Journalisten, Rechtsanwälte, Zivilgesellschaft, aber sogar auch Politiker innerhalb der Europäischen Union – nichts dagegen tun können, dann ist das ein große Bedrohung für die Demokratie. Ich finde es sehr besorgniserregend, dass es eigentlich vonseiten der Regierungen und der Kommission keine Antwort gibt. Das ist jetzt also die Lage, was ich zu sagen habe.

Die **Vorsitzende**: Ganz herzlichen Dank. Sie haben sich tatsächlich daran gehalten, meistens sagen die Leute, ich brauche die Zeit nicht, und dann brauchen sie sie doch. Dann kommen wir jetzt in die Debattenrunde und als erstes für die SPD-Fraktion hat der Kollege Dr. Jens Zimmermann das Wort.

Abg. **Dr. Jens Zimmermann** (SPD): Herzlichen Dank, Frau Vorsitzende. Ich würde meine Fragen eher in Richtung derjenigen richten, die implizit zumindest angesprochen wurden, auch beim Eingangsstatement. Können wir davon ausgehen, dass in Deutschland Spyware, Pegasus im Speziellen, aber Spyware im Allgemeinen, nicht gegen politisch unliebsame Politikerinnen und Politiker eingesetzt wird?

PStS **Johann Saathoff** (BMI): Zunächst herzlichen Dank für die Einladung. Frau in t´ Veld, auch herzlichen Dank für Ihre Arbeit im Untersuchungsausschuss und den sehr, sehr umfänglichen Bericht, den wir gelesen haben. Wir haben ja nicht nicht geantwortet, sondern wir haben den Fragebogen PEGA beantwortet und auf die Rahmenbedingungen hingewiesen, unter denen bestimmte Dinge, die leider notwendig sind, gemacht werden können. Ich kann für Deutschland sagen, dass wir äußerst enge gesetzliche Rahmenbedingungen haben, zum Beispiel die grundsätzliche Erforderlichkeit von richterlichen Anordnungen für jede einzelne Maßnahme. Es gibt auch ein Erforderlichkeitsgebot, es gibt die Notwendigkeit einer anordnenden Stelle, etwa Untersuchungsrichter oder G10-Kommission. Es ist also nicht so, dass es das Ausspähen ohne Gründe in Deutschland gibt. Es gibt auch nicht Ausspähen mit Gründen, sondern wenn es Ermittlungsnotwendigkeiten gibt, dann erfolgen die aufgrund von Rechtsgrundlagen und dann anhand von extrem engen Rahmenbedingungen.

Abg. **Dr. Jens Zimmermann** (SPD): Herzlichen Dank. Wir haben auch eine enge parlamentarische Kontrolle, aber jetzt kommen wir zu den schwierigeren Sachen, nämlich den mittelbaren Auswirkungen. Presseberichten zufolge nutzt die Bundesrepublik auch diese Software dieses Herstellers, und wir wissen, dass dieser Hersteller offenbar keine Probleme damit hat, diese Software weiterzugeben an Staaten oder an andere Nutzer, die keine lange rechtsstaatliche Kontrolle haben. Da stellt sich für mich natürlich die Frage: Wie geht die Bundesregierung in der Güterabwägung am Ende damit um, dass man letztendlich Geschäftspartner eines solchen Unternehmens ist? Wie kann man das am Ende auflösen?

PStS **Johann Saathoff** (BMI): Wir haben in der Antwort auf den PEGA-Untersuchungsausschuss geschrieben, dass das Bundeskriminalamt (BKA), das in Deutschland über gesetzliche Befugnisse zur Quellen-TKÜ und Onlinedurchsuchung zur Gefahrenabwehr und zur Strafverfolgung verfügt, sowohl Eigenentwicklungen als auch kommerzielle Lösungen im Einsatz hat. Wir haben aber nicht davon gesprochen, welche kommerziellen Lösungen eventuell im Einsatz stehen könnten und wir haben auch nicht über die Arbeit der Nachrichtendienste gesprochen, schon allein deswegen, da wir dazu nicht befugt sind. Von daher kann ich auch über die möglichen Einsätze von bestimmten Produkten – Sie haben ja ein ganz bestimmtes Produkt im Auge – nichts sagen.

Abg. **Dr. Jens Zimmermann** (SPD): Das interessiert mich sehr, aber meine Frage ist unabhängig vom

konkreten Produkt, sondern eher, wie gehen wir als Bundesregierung mit dem Dilemma am Ende des Tages um, dass wir natürlich durch die Nutzung welcher Kaufsoftware auch immer die Weiterentwicklung ermöglichen und am Ende verkaufen sie es halt an irgendwen. Aber die Antwort dann vielleicht später.

Die **Vorsitzende**: Die Zeit ist um, und für die CDU/CSU-Fraktion hat der Kollege Marc Henrichmann das Wort.

Abg. **Marc Henrichmann** (CDU/CSU): Vielen Dank. Ich würde es gerne aufteilen.
Frau in t´ Veld, Sie haben sich sehr dezidiert mit der Thematik auseinandergesetzt. Sie haben vorgeschlagen, ein EU-Technologielabor auf die Reise zu bringen, das insbesondere bei den Themen illegale Überwachung untersuchen und unterstützen soll. Wie stellen Sie sich das konkret vor? Wie soll das arbeiten? Wie soll das besetzt sein?

Sophie in t´ Veld: Darf ich, bevor ich darauf antworte, noch etwas zu dem vorherigen Beitrag sagen?

Die **Vorsitzende**: Das ist die Redezeit der CDU/CSU-Fraktion, aber wir drücken ein Auge zu, wenn Sie sich kurz fassen.

Sophie in t´ Veld: Der Sprecher hat gesagt, die Regierung hat geantwortet. Fast alle Regierungen haben geantwortet, aber sie haben nichts Bedeutungsvolles geantwortet. Wirkliche Informationen haben wir nicht bekommen. Zweitens, wie der Abgeordnete auch gesagt hat, alle EU-Mitgliedstaaten machen auch Geschäfte mit der NSO Group und Intellexa. Das sind Unternehmen, die in den Vereinigten Staaten geblacklisted sind. Das ist doch irre, dass wir damit Geschäfte machen, obwohl die Amerikaner sagen, das ist eine Bedrohung für ihre Staatssicherheit.

Die **Vorsitzende**: Wenn Sie jetzt die Fragen des Abgeordneten beantworten, wäre das gut, denn sonst läuft seine Zeit weg.

Sophie in t´ Veld: Wir sind jetzt völlig abhängig von Citizen Lab und Amnesty International. Da gab es breiten Konsens. Wir brauchen eigentlich ein europäisches Zentrum, wo es Expertise und Sachkenntnisse gibt und wo man mit seinen Geräten hin kann und fragen, ob man Spyware in seinem Gerät hat. Ich glaube, das ist wichtig. Das könnten wir eigentlich innerhalb von einem Tag machen, denn die Sachkenntnis und die Experten haben wir in der Europäischen Union. Es ist mir nicht völlig klar, warum. Wir rufen schon seit anderthalb Jahren dazu auf und da wird wenig gemacht, eigentlich wird nichts von der Kommission gemacht. Wir brauchen das aber dringlich.

Abg. **Marc Henrichmann** (CDU/CSU): Dankeschön. Herr Staatssekretär Saathoff, Herr Könen, wer von Ihnen beiden sich da zuständig fühlt, kann gerne antworten. Es gibt einen Run auf die Software. So wie man hört, ist beispielsweise Saudi-Arabien auch mit einem erpresserischen Akt hinter Pegasus her gewesen. Ist es nur dieser eine Anbieter? Gibt es unter dem Radar auch weitere Entwicklungen in diesem Bereich? Wir kümmern uns um das Symptom, aber müsste man da generell noch viel weiter darauf schauen? Das zweite wäre der Begriff der nationalen Sicherheit: Glauben Sie, dass wir in Europa rechtlich eine Definition hinbekommen, hinter der sich die Mitgliedstaaten versammeln können?

Andreas Könen (BMI): Tatsächlich geht der Anbietermarkt für solche Tools weit über das jetzt benannte Unternehmen NSO hinaus. Es gibt eben verschiedenste Unternehmen, und wenn wir Tools für den Einsatz bei Online-Durchsuchungen und Quellen-TKÜ benötigen, dann gehört dazu natürlich eine Marktsichtung. Eine Marktsichtung, die heute bei dem Clinical Trials Information System (CTIS) im Wesentlichen zentral für die Sicherheitsbehörden durchgeführt wird, und die natürlich auch mit in Betracht zieht, wie sich das Unternehmen grundsätzlich auf dem Markt engagiert, ob es die Rechtsetzung des eigenen Heimatlandes dazu einhält. Israel hat Konsequenzen aus dem NSO-Vorfall gezogen, die völlig in unserem Sinne sind, da wir seit langem mit der standardisierenden Leistungsbeschreibung sehr enge Grenzen aus der Online-Durchsuchung und Quellen-TKÜ herauskommend jedem der Unternehmen hinlegen, die auch nur im Entferntesten betrachtet werden und infrage kämen. Das ist die Vorgehensweise, und wir schauen uns solche Ereignisse, wie Sie sie benannt haben, auch an. Der Fall Saudi-Arabien ist mir kein präziser Begriff, dazu kann ich mich nicht äußern. Aber ansonsten gilt das Gesagte.

Die **Vorsitzende**: Vielen Dank, und für BÜNDNIS 90/DIE GRÜNEN hat die Kollegin Misbah Khan das Wort.

Abg. **Misbah Khan** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Zum Beispiel Bitkom beziffert den jährlichen Schaden, auch durch Spysoftware, auf 203 Milliarden Euro. Das sind vor allem die Angriffe, das ist Spionage, das ist Sabotage. Das heißt, die Tragweite, die dieses Thema hat, kann man nicht unterschätzen. Von daher auch herzlichen Dank an Sie und an die Ausschussarbeit für das wertvolle Lagebild und Ihre Forderungen. Ich glaube, damit sind wir einen guten Schritt weiter in die Richtung, in die wir gehen müssen. Wir haben auch immer wieder Berichte von Reporter ohne Grenzen, die erzählen, dass auch in Deutschland Journalistinnen und Journalisten von Spysoftware infiziert werden und wurden. Zuletzt sah man das vorletzte Woche mit der russischen Exiljournalistin. Die Frage, die ich an der Stelle habe, ist: Welche Möglichkeiten sehen Sie denn bei den nationalen Behörden, diese Menschen besser zu schützen?

PStS **Johann Saathoff** (BMI): Ich hatte gerade schon einmal die Rahmenbedingungen, die wir haben, ausformuliert. Wie schützen wir die Bevölkerung davor, dass der Staat nicht willkürlich Menschen ausspäht? Dazu gibt es klare rahmenrechtliche Vorgaben. Die sind nicht diskutierbar, sondern gerichtlich überprüfbar. Zu dem wichtigsten Punkt der engen gesetzlichen Rahmenbedingungen gehört die richterliche Anordnung. Die ist nicht generalisiert für irgendeine Personengruppe, sondern für jede einzelne Maßnahme. Es muss im Rahmen der Strafverfolgung und der polizeilichen Gefahrenabwehr erfolgen. Selbst das reicht noch nicht. Es muss ein Erforderlichkeitsgebot da sein, das heißt, der anordnenden Stelle – zum Beispiel dem Untersuchungsrichter – muss gegenüber begründet werden, warum diese Maßnahme unbedingt erforderlich ist. Ich glaube, die rechtlichen Rahmenbedingungen, die wir in Deutschland haben, können sich sehen lassen. Damit ist sichergestellt, dass niemand willkürlich ausgespäht wird.

Abg. **Misbah Khan** (BÜNDNIS 90/DIE GRÜNEN): Dann habe ich noch eine weitere Frage an Frau in t´ Veld. Es geht um die Forderung Nummer 39 des Reports. Da geht es grob um hohe Compliance-Anforderungen an Unternehmen, insbesondere menschenrechtliche Standards, auf die geachtet werden soll. Wie ist Ihr Eindruck nach Ihren Sitzungen? Gibt es Unternehmen, die diesen Standard jetzt schon haben? Gibt es diesbezüglich gute Vorbilder? Wie kann so ein Überprüfungsprozess laufen?

Sophie in t´ Veld: Die Antwort ist ziemlich einfach: Nein, solche Unternehmen sind mir nicht bekannt. Leider ist dieser Markt der Anbieter sehr wenig transparent. Die sind auch in Bereichen, die teilweise sich im Schatten befinden. Leider gibt es nicht solche Anbieter. Es ist auch ziemlich leicht für Anbieter. Ich habe gerade gesagt, große Anbieter, so wie NSO und Intellexa, machen ihre Geschäfte in Europa ohne Schwierigkeiten, werden aber in den Vereinigten Staaten als Bedrohung für die Staatssicherheit betrachtet. Hier in Europa haben diese Unternehmen eigentlich alle Freiheiten, bekommen sogar Steuervorteile in ihrem Land und machen ihre Bankgeschäfte in Luxemburg. Wenn Spyware missbraucht wird, dann gibt es eigentlich keine Konsequenzen, so wie wir das auch im Bericht niedergeschrieben haben. Zum Fall mit der russischen Journalistin: Soweit bisher bekannt, wurde sie wahrscheinlich ausgespäht, als sie sich in Berlin befand. Am Anfang hat sie gemeint, da steckt der Kreml dahinter, aber jetzt ist es eher wahrscheinlich, dass es ein EU-Mitgliedstaat ist. Es kann sein, dass es rechtliche Rahmenbedingungen gibt, aber in der Praxis nützt ihr das nicht, denn wo sollte sie hin? Sie hat wahrscheinlich nie Zugang zu ihrem Dossier und kann nicht einmal zum Gerichtshof.

Die **Vorsitzende**: Kommen Sie bitte zum Ende. Ich weiß nicht, ob Sie die Zeit sehen und den Gong hören, denn wir müssen uns an das Zeitmanagement halten. Für die FDP-Fraktion hat der Kollege Dr. Volker Redder das Wort.

Abg. **Dr. Volker Redder** (FDP): Ich frage da aber gleich weiter, in Richtung BMI. Es geht um die Journalistin Galina Timtschenko, die während eines Aufenthalts mittels Pegasus hier überwacht worden ist. Betroffen waren auch Treffen mit deutschen Journalisten, Reporter ohne Grenzen und so weiter. Die Frage an das BMI wäre: Hatte das BMI Kenntnisse von der Überwachung und erfolgte die Überwachung durch eine deutsche Behörde?

PStS **Johann Saathoff** (BMI): Dazu kann ich antworten, dass dem BMI dazu keine Erkenntnisse vorliegen.

Abg. **Dr. Volker Redder** (FDP): Ich habe mir tatsächlich so etwas gedacht. Zurück zu Ihnen, Frau in t´ Veld. Sie haben eben gesagt, momentan gibt es im Europäischen Parlament keine richtigen Bewegungen. Das Europäische Parlament empfiehlt aber, dass Mitgliedstaaten für die Verwendung von Spysoftware bestimmte Bedingungen erfüllen sollen. Dazu soll eine Bewertung der Kommission bis Ende November entwickelt sein. Gibt es da einen Stand? Wie sind die aktuellen Bedingungen? Welche Bedingungen werden diskutiert?

Sophie in t´ Veld: Ich muss erklären, was ich am Anfang gesagt habe, bisher hat es von der Seite der Kommission nichts gegeben. Keine Antwort, nichts. Es ist seit dreieinhalb Monaten Schweigen. Man hat mir gestern gesagt, dass wir die Antwort innerhalb von ein bis zwei Wochen erwarten, also vier Monate, nachdem das Parlament sich geäußert hat. Es ist mir völlig klar, obwohl ich die Antwort noch nicht gesehen habe, dass die Kommission überhaupt keine Lust hat, sich mit dieser Frage zu beschäftigen, obwohl sogar Mitglieder und Mitarbeiter der Kommission selbst betroffen waren. Es waren Geräte infiziert mit Spyware, oder es hat wenigstens Versuche gegeben, das zu machen. Ich möchte noch einmal betonen, es wurde gesagt: Es gibt rechtliche Rahmenbedingungen und richterliche Anordnungen. In der Praxis ist das alles völlig bedeutungslos, denn diese Sachen passieren, es gibt Missbrauch und es gibt dann keine Möglichkeiten für Bürger oder für Leute, die betroffen sind, die Targets, irgendetwas zu machen. Die können sich nicht schützen, die können sich nicht verteidigen, die können nicht vor den Gerichtshof, denn die haben keine Beweise. Und sobald nationale Sicherheit gesagt wird, werden alle Fenster und Türen geschlossen und ist eigentlich auch fast alles erlaubt, und das macht es sehr, sehr schwierig, Rechtsschutz, den es auf dem Papier gibt, auch in der Praxis zu haben. Das gibt es einfach nicht, und ich finde das sehr besorgniserregend. Es gibt keine Konsequenzen, wenn innerhalb der EU Journalisten, Politiker und Oppositionspolitiker ausgespäht werden. Das ist wirklich eine Bedrohung für die Demokratie.

Abg. **Dr. Volker Redder** (FDP): Ich würde gerne noch eine zweite Frage stellen. Dadurch, dass sich jetzt die EU darum kümmert, aber am Ende es immer nationales Recht ist: Ist das für Sie das Problem? Was könnte man denn machen in der EU? Was ist denn Ihr konstruktiver Vorschlag, um so etwas in Zukunft zu verhindern?

Sophie in t´ Veld: Es gibt natürlich nicht eine einzige Lösung, wir haben ein ganzes Paket an Empfehlungen abgestimmt im Parlament. Und es ist eine sehr breite Mehrheit an Bedingungen für die Benutzung der Space Software und eine bessere Definition von nationaler Sicherheit. Ich sehe, dass ich keine Zeit mehr habe. Es steht alles in dem Bericht.

Die **Vorsitzende**: Es gibt noch eine zweite Runde. Für die AfD-Fraktion hat der Abgeordnete Janich das Wort.

Abg. **Steffen Janich** (AfD): Meine Fragen gehen an Frau in t´ Veld. Sie sprachen vorhin davon, dass es noch weitere Enthüllungen gegeben hätte nach den Abstimmungen, können Sie noch einmal genauer darauf eingehen? Was ist denn im Nachgang noch herausgekommen bei der ganzen Sache?

Sophie in t´ Veld: Es gibt mehrere Sachen. Fast jede Woche kommt etwas Neues. Es gab diese Geschichte, die wir schon erwähnt haben von der russischen Journalistin. Es hat sich schon herausgestellt vor zwei Monaten in Griechenland, dass fast 100 Leute ausgespäht wurden. Da gibt es auch Beweise für. Die haben noch nicht bewiesen, von wem, aber die sind sehr nah dran. Übrigens, die Behörde, die das herausgefunden hat und alles überwacht und kontrolliert, wird heute von der Regierung in ihren Kompetenzen beschränkt. Das ist dann die Antwort der Regierung. Auch zum Beispiel in Spanien hat es eine richterliche Untersuchung gegeben und der Richter, der hat vergeblich versucht, immer wieder mit den israelischen Behörden in Kontakt zu treten und Informationen zu bekommen. Die israelischen Behörden verneinen dies immer. Ich finde es unfassbar, dass wir abhängig sind von der israelischen Regierung, den israelischen Behörden, aber auch von großen Tech-Firmen wie Apple oder Citizen Lab für unseren Cyberschutz. Und dass die israelischen Behörden mehr Kenntnisse haben als wir Europäer, finde ich nicht in Ordnung.

Abg. **Steffen Janich** (AfD): Wie viele Abhörmaßnahmen hat es insgesamt gegeben? Sind Zahlen bekannt, in welchen Größenordnungen das stattgefunden hat?

Sophie in t´ Veld: Das ist schwierig zu sagen. Aber

die Fälle, die uns bekannt sind, sind in Ungarn, ich glaube, über 300 Fälle und in Polen auch wahrscheinlich Hunderte, in Spanien sind uns, ich glaube, 65 Fälle bekannt und in Griechenland mindestens 100, aber wahrscheinlich eher 200 oder mehr. Das sind alles Fälle von Ausspähungen, die eigentlich nicht gerechtfertigt waren, also Missbrauch. Es gibt auch Fälle, in denen die Polizei Spyware benutzt hat gegen Kriminelle, aber das sind andere Fälle, damit haben wir uns nicht beschäftigt. Wir haben uns jetzt wirklich beschäftigt mit Missbrauch von Spyware gegen Journalisten, Politiker und so weiter.

Abg. **Steffen Janich** (AfD): Sind Ihnen Fälle bekannt, in denen in irgendeiner Form eine deutsche Behörde involviert war?

Sophie in t´ Veld: Nein, aber so wie ich am Anfang gesagt habe, in vielen Ländern wird Spyware wahrscheinlich nicht von den Behörden missbraucht. Das ist aber nicht die Frage. Das Problem ist, wenn wir wissen, dass es in bestimmten Fällen missbraucht wird und auch tatsächlich politisch missbraucht wird, so wie in Polen, Ungarn und so weiter, dann ist es unglaublich, dass die anderen Regierungen einfach schweigen. Es ist nicht nur eine nationale Frage. Die europäischen Behörden sind unmittelbar davon betroffen, der Europäische Rat, die Kommission und das Parlament, es wurden auch europäische Abgeordnete ausgespäht. Durch das große Schweigen der Regierungen sind die alle mitverantwortlich und mitschuldig meiner Meinung nach.

Die **Vorsitzende**: Für die Fraktion DIE LINKE. hat Anke Domscheit-Berg das Wort.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Herzlichen Dank. Die Kollegin vom BfDI ist auch da, richtig? Die würde ich nämlich gerne fragen. Ende 2021 hat die Tagesschau berichtet, dass ein Prüfbericht des BKA zur Pegasus-Software dem BSI übermittelt worden ist zur Prüfung, inklusive Dokumente zur Leistungsbeschreibung, alle möglichen Informationen et cetera. Ich wüsste gerne: Hat der BfDI diese Dokumente auch erhalten? Haben Sie die aus Ihrer Sicht notwendigen Einblicke für eine datenschutzrechtliche Einschätzung des Einsatzes von Pegasus durch deutsche Behörden erhalten und haben Sie irgendwelche Empfehlungen abgegeben und sind die befolgt worden?

Christa Polfers (BfDI): Vielen Dank für die Frage, Frau Domscheit-Berg. Folgende Antwort: Es ist tatsächlich so, dass wir uns Quellen-TKÜ-Systeme anschauen, und dazu sind wir rechtlich auch verpflichtet, nach Paragraf 69 Absatz 1 BKA-Gesetz. Hiernach ist es so, dass wir alle zwei Jahre eine Pflichtkontrolle durchführen in Bezug auf verwandte Systeme. Unsere Befugnisse gehen dahin, tatsächlich Unterlagen zu bekommen, und zwar alle Unterlagen, die bestimmte Systeme betreffen. Wir schauen uns auch die Systeme vor Ort an, nehmen technische Sondierungen vor und prüfen, ob die Einhaltung mit den rechtlichen Vorgaben gegeben ist. Das ist der Rahmen, in dem wir uns bewegen, wenn es um Fragen geht, informationstechnische Systeme oder auch Quellen-TKÜ-Systeme zu überprüfen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Das heißt, Sie haben sich auch Pegasus angeschaut?

Christa Polfers (BfDI): Als Kontrollbehörde unterliegen auch wir der Geheimhaltung, auch wenn das sehr lästig sein mag und vielleicht auch nicht gerne gehört wird. Es ist aber Voraussetzung dafür, dass wir ganz effektiv und vernünftig umfassend kontrollieren können. Insofern würde ich mich zu konkreten Äußerungen an dieser Stelle nicht hinreißen lassen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Ich frage an einer anderen Stelle nach. Haben Sie Empfehlungen abgegeben und wurden diese befolgt, und welche waren das?

Christa Polfers (BfDI): Wir haben zu der Frage des Einsatzes von Quellen-TKÜ-Systemen grundsätzliche Empfehlungen abgegeben, die wir auch in einem Positionspapier des BfDI veröffentlicht haben. Nach diesen Empfehlungen gibt es einige Maßstäbe, die für uns ganz wesentlich sind bei dem Einsatz von Quellen-TKÜ-Systemen. Diese Maßstäbe betreffen insbesondere die Kontrolle. Aus unserer Sicht müssen sämtliche Systeme prüfbar und auch beherrschbar sein. Das halten wir für wesentlich, wenn eine Quellen-TKÜ genutzt wird. Ich verweise gerne insofern noch auf das veröffentlichte Positionspapier. Für uns weiter wichtig ist, dass wir uns bestimmte Systeme vor der Absicht einer Inbetriebnahme auch schon anschauen können. Da sind die Behörden verpflichtet, uns zu beteiligen im Wege einer

Anhörung. Wir haben dann die Gelegenheit, entsprechende Informationen einzuholen, uns die notwendigen Unterlagen vorlegen zu lassen und in die rechtliche und technische Betrachtung zu gehen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Kurz noch eine Frage an das BMI: Warum ist die zweimal eingeladene BKA-Vizepräsidentin nicht zum Untersuchungsausschuss im Parlament aufgetaucht?

Andreas Könen (BMI): Die Vizepräsidentin des BKA war aus Termingründen verhindert.

Die **Vorsitzende**: Vielen Dank. Dann kommen wir zu zwei Minuten für die fraktionslose Kollegin Cotar.

Abg. **Joana Cotar** (fraktionslos): Vielen Dank. Welche Rolle spielte Bernd Schmidbauer beim Einkauf von Spähsoftware? Spielte er eine Rolle? Wurde Software aufgrund von Empfehlungen von Herrn Schmidbauer eingekauft?

PStS **Johann Saathoff** (BMI): Da kann ich Ihnen gar nichts zu sagen. Dazu liegen mir keine Informationen vor.

Abg. **Joana Cotar** (fraktionslos): Frau in t´ Veld, wurde Herr Schmidtbauer eingeladen zum Untersuchungsausschuss? Wenn ja, was hat er gesagt? Und wenn nein, warum nicht? Als Lobbyist für Intellexa und ehemaliger Geheimdienstkoordinator.

Sophie in t´ Veld: Ob er eingeladen wurde, weiß ich nicht. Das müsste ich einmal nachschauen, aber ich bin mir ziemlich sicher, dass wir keinen Austausch mit ihm gehabt haben. Intellexa hat eigentlich überhaupt nicht geantwortet. Am Ende hat der Anwalt von Intellexa uns einen Brief geschrieben und sich mehr oder weniger beschwert. Aber das war eigentlich alles.

Abg. **Joana Cotar** (fraktionslos): Sie haben gesagt, dass die Regierungen zwar auf ihren Fragenkatalog geantwortet haben, auch die deutsche Regierung, aber die Antworten waren nicht so zufriedenstellend. Welche Antworten haben Ihnen von der deutschen Regierung gefehlt?

Sophie in t´ Veld: Wir haben nicht von 27 Regierungen, aber von mehreren, Antworten bekommen. Die meisten haben dann den Rechtsrahmen beschrieben. Aber wirklich Antworten auf Fragen über die Benutzung von Spyware, also Sachen, die uns wirklich etwas Neues gebracht haben, haben wir eigentlich von keinem Mitgliedstaat bekommen. Deswegen sind die Antworten an sich auch nicht so wichtig, denn wir haben da wenig Bedeutendes gefunden.

Die **Vorsitzende**: Vielen Dank. Wir kommen in die zweite Runde. Ich bitte noch einmal darum, nicht nach dem Gong noch eine zusätzliche Frage zu stellen. Für die SPD-Fraktion die Kollegin Kassautzki.

Abg. **Anna Kassautzki** (SPD): Vielen herzlichen Dank. Auch ich würde starten wollen mit einem Dank an die Kolleginnen und Kollegen aus dem Europäischen Parlament für die Arbeit im Untersuchungsausschuss und auch für den Abschlussbericht. Ich möchte aber mit meinen Fragen beginnen an die Bundesregierung. Aus dem Abschlussbericht geht hervor, dass die Spähsoftware von 14 europäischen Ländern eingesetzt wurde. In erschreckend vielen Fällen auch gegen die Zivilgesellschaft und die Opposition. In den vergangenen Wochen wurde bekannt, dass die russische Exil-Journalistin – die Kollegin Misbah Khan ist schon darauf eingegangen – auch in Deutschland ausgespäht wurde. Nicht durch Deutschland, aber in Deutschland. Ist bekannt, ob und in welchem Umfang weitere in Deutschland lebende Personen davon betroffen waren, von wem und aus welchen Gründen diese überwacht wurden? Was kann und muss gemacht werden, um missbräuchliche Ausspähungen zu verhindern? Damit meine ich nicht explizit von deutscher Seite, denn da sind Sie schon auf die Rahmbedingungen eingegangen, sondern von anderen Ländern. Was muss gemacht werden, um missbräuchliche Ausspähungen in Deutschland verhindern zu können?

PStS **Johann Saathoff** (BMI): Ich würde einmal anfangen. Vielleicht kann Herr Könen noch ergänzen. Das war Grund des Untersuchungsausschusses, das sicherzustellen. So verstehe ich Frau in t´ Veld auch mit der Frustration, dass Staaten nicht auf Staaten reagieren, die sich nicht an Regeln halten. Das nehme ich gerne mit als Auftrag, da genauer hinzuschauen. Wobei ich schon sagen möchte, dass wir natürlich geschaut haben, was die Empfehlungen aus dem Untersuchungsausschuss sind und schon geschaut haben, was müssen wir verändern, um den Empfehlungen zu entsprechen. Das Interessante ist, Frau in t´ Veld, Ihre

Empfehlungen sind, rechtliche Rahmenbedingungen zu schaffen. Aber hier in der Anhörung sagen Sie, es hilft nicht, wenn man rechtliche Rahmenbedingungen hat, denn es wird trotzdem gemacht. Wir haben schon die Einschätzungen und rechtlichen Mindeststandards grob überschätzt – und kommen zu dem Ergebnis, dass Deutschland die bereits jetzt erfüllt. Ich bin hier, um zu erklären, wie Deutschland damit umgeht. Wie das in einem internationalen Kontext gehandhabt wird, dazu muss die Bundesregierung sich abstimmen.

Abg. **Anna Kassautzki** (SPD): Ich hatte noch die Frage gestellt, wie viele Fälle bekannt sind, wo in Deutschland ausgespäht wurde.

Andreas Könen (BMI): Genauso wie in Bezug auf die betroffene Russin selber, sind keine deutschen Personen – weder Journalistinnen noch Menschenrechtsaktivisten, Politiker, Politikerinnen – bekannt, die betroffen sind. Wenn es Betroffene gibt, können wir nur empfehlen, das zur Anzeige zu bringen. Dann ist es durchaus technisch komplex, zunächst einmal nachzuweisen, dass eine solche Spyware im Einsatz war. Das können wir aber in entsprechend ausgerüsteten Polizeidienststellen beziehungsweise in den zentralen Staatsanwaltschaften gewährleisten. Dann wird einer solchen Anzeige nachgegangen. Das aktiv im Verkehr zu erkennen, ist eine große Herausforderung, wo zumeist die rechtliche Grundlage nicht existiert.

Abg. **Anna Kassautzki** (SPD): Vielen herzlichen Dank. Meine zweite Frage würde sich an Frau in t´ Veld richten. Auch vor dem Hintergrund zunehmend rechtsstaatsfeindlicher Bemühungen einiger Mitgliedstaaten, auch der Europäischen Union – der Kollege Redder hatte das schon angedeutet: Wie plant das Parlament sicherzustellen, dass es in Zukunft weniger und nicht mehr digitale Bespitzelung innerhalb der Europäischen Union gibt?

Sophie in t´ Veld: Dafür haben wir diese ganze Reihe von Empfehlungen vorgelegt. Es stimmt schon, dass in mehreren Mitgliedstaaten diese Rahmenbedingungen schon existieren. Aber nicht in allen Mitgliedstaaten funktioniert das. Aber das Problem ist, wenn wir diese Empfehlungen wirklich umsetzen, dann benötigen wir auch, dass die Nationalregierungen mitmachen. Aber die verweigern sich, die schweigen. Und auch die Kommission macht nichts. Dann wird es wirklich sehr schwierig, wenn die sich einfach nicht bewegen und schweigen.

Die **Vorsitzende**: Dankeschön. Und wir kommen wieder zur CDU/CSU-Fraktion. Das Wort hat wieder der Kollege Henrichmann.

Abg. **Marc Henrichmann** (CDU/CSU): Dankeschön. Ich würde noch einmal gerne aufsatteln auf die Antworten der ersten Runde. Die Attraktivität dieser Software, ganz nüchtern betrachtet, scheint relativ hoch zu sein. Bei Autokraten, Diktatoren und Co. wahrscheinlich noch viel größer als bei den Demokratien dieser Welt. Wenn wir das wissen, ist die Frage: Ist eine Regulierung an der Quelle sozusagen, ein Verbot, ein Steuern das Richtige? Oder guckt man hinten: Wie schützt man eigentlich die Menschen vor illegaler Überwachung in dem Zusammenhang? Ich würde einmal das Thema Schwachstellenmanagement in diesem Zusammenhang ansprechen. Frau Plattner als neue BSI-Präsidentin hat heute Morgen gesagt, das wäre die große Baustelle. Ich gehe jetzt einmal davon aus und würde dann Ihr Kopfnicken auch so werten, dass es keine aktive Zusammenarbeit mit solchen Unternehmen gibt. Dann hätte ich einmal die Bitte, ob Sie beschreiben können, wie hoch die rechtlichen Hürden für eine staatliche Überwachung in Deutschland mit dieser Software eigentlich sind. Über welche Tatbestände reden wir da? Ich glaube, das ist vielleicht noch einmal zur Verdeutlichung ganz gut.

Andreas Könen (BMI): Tatsächlich ist es so, dass man natürlich einiges unternehmen kann, um sicherzustellen, dass die Unternehmen, mit denen man etwa zusammenarbeitet, um eine entsprechende Quellen-TKÜ und Online-Durchsuchungssoftware zu kaufen, regulär arbeiten. Ich hatte das eben schon kurz geschildert. Da haben alle Sicherheitsbehörden eben einen sehr genauen Katalog, was erfüllt sein muss in der Umsetzung von Quellen-TKÜ und Online-Durchsuchung. Das ist dem Hersteller präzise mitzuteilen und er hat es präzise zu erfüllen. Und wenn er es nicht erfüllen kann, hat er nur dann die Chance, ein solches Tool überhaupt zu verkaufen, wenn er seine Software entsprechend anpasst an diese standardisierende Leistungsbeschreibung. Das ist ganz entscheidend. Denn der Einsatz selbst der Quellen-

TKÜ ist ausschließlich auf die laufende Kommunikation des Betroffenen beschränkt. Die Zulässigkeit richtet sich nach Paragraf 100a, Absatz 1 Satz 2 und 3 der StPO, beziehungsweise nach dem Paragrafen 5 und 51 Absatz 2 des BKA-Gesetzes, beziehungsweise für die Nachrichtendienste nach Paragraf 11 Absatz 1a G10. Da ist dann auch jeweils formuliert, welcher Straftatenkatalog überhaupt nur Grundlage für eine Maßnahme der Quellen-TKÜ sein kann. Im Rahmen der StPO ist dann auch definiert, wer die Anordnung erteilen kann. Eine richterliche Anordnung, eine staatsanwaltschaftliche Anordnung. Nur bei Gefahr in Verzug kann auch der Leiter der jeweiligen Polizeibehörde eine entsprechende Anordnung treffen, die aber sofort und schnellstmöglich durch einen Richter oder Staatsanwalt nachgezogen werden muss. Für die Onlinedurchsuchung gelten entsprechend härtere Bedingungen durch Einschränkung des entsprechenden Katalogs. In diesem Fall richtet sich die Zulässigkeit nach Paragraf 100b der Strafprozessordnung, beziehungsweise Paragraf 49 des BKA-Gesetzes. Die Onlinedurchsuchung greift auf gespeicherte Daten zu. Sie greift sehr tief in die jeweiligen IT-Systeme ein, sodass dabei zum Beispiel von vornherein ausgeschlossen wird, dass angeschlossene Kameras oder Mikrofone genutzt werden, um den Bereich wirklich einzuengen. Da gelten noch einmal besondere Bedingungen in der Betrachtung des gewonnenen Materials durch Richterband, sodass wirklich präzise herauszuschneiden ist, dass nur die Anteile, die der Anordnung der gewonnenen Daten entsprechen, verwendet werden.

Die **Vorsitzende**: Vielen Dank, und für BÜNDNIS 90/DIE GRÜNEN Tobias Bacherle.

Abg. **Tobias Bacherle** (BÜNDNIS 90/DIE GRÜNEN): Vielen herzlichen Dank. Ich habe eine kurze Nachfrage. Habe ich das richtig verstanden, dass es technisch, nicht rechtlich, möglich ist, die Spähsoftware ohne Richterbeschluss anzuwenden?

Andreas Könen (BMI): In ganz wenigen Fällen. Das ist im Rahmen der Gesamt-TKÜ-Regelungen so getroffen. Das gilt nicht nur für diese beiden.

Abg. **Tobias Bacherle** (BÜNDNIS 90/DIE GRÜNEN): Mir ging es auch tatsächlich um die technische Anwendung, wie gesagt, nicht um die rechtlichen Ausnahmen. Liebe Frau in t´ Veld, können Sie noch einmal die Auswirkungen beschreiben auf ausländische Akteure und Staaten, die die Europäische Union jetzt getroffen hat, beziehungsweise vor allem, die, die sie nicht getroffen hat, in Bezug auf Staaten, die Pegasus gegen europäische Staatsbürgerinnen und Staatsbürger eingesetzt haben, und was Sie sich da erhoffen würden, was noch folgt?

Sophie in t´ Veld: Wenn ich Sie richtig verstanden habe, dann meinen Sie, wenn Leute innerhalb der Europäischen Union ausgespäht wurden von außerhalb?

Abg. **Tobias Bacherle** (BÜNDNIS 90/DIE GRÜNEN): Ja, genau.

Sophie in t´ Veld: Ja, da gibt es eine Reihe von Fällen, die uns bekannt sind. Zum Beispiel, dass sogar Präsident Macron ausgespäht wurde aus Marokko, von den marokkanischen Behörden, beziehungsweise von wem, das wissen wir natürlich nicht genau. Aber es gibt zum Beispiel auch den Fall der Tochter eines Politikers aus Ruanda, die damals in Belgien lebte, dann nach Amerika umgezogen ist, und auch sie wurde ausgespäht, während sie in Belgien war und sogar, während sie sich mit Regierungsministern oder Europaabgeordneten traf. Es gibt bestimmt auch noch andere Fälle und es ist schwierig, sich davor zu schützen, denn technisch ist es durchaus möglich, das von außen zu machen. Deswegen haben wir auch vom Europäischen Parlament empfohlen, dass wir eine Art Allianz machen mit den Vereinigten Staaten und mit anderen Ländern und da Standards setzen, denn dann ist es technisch immer noch möglich und die Anbieter können dann immer noch ihre Ausspähsoftware verkaufen, aber es ist viel schwieriger, so etwas zu machen.

Abg. **Tobias Bacherle** (BÜNDNIS 90/DIE GRÜNEN): Daran anknüpfend: Welche Kriterien sollten denn aus der Sicht des Europäischen Parlaments bei Ausfuhrbestimmungen von Spähsoftware in Nicht-EU-Länder, aber vor allem auch Dual Use-Technologien oder möglichen Dual-Use-Technologien für Spähangriffe auf einzelne Individuen in Zukunft beachtet werden, vor allem in Hinsicht auf repressive Regime?

Sophie in t´ Veld: Da gibt es eigentlich schon eine Verordnung, Dual Use, Sie haben das schon erwähnt. Das Problem ist, es wird nicht eingehalten,

und die Europäische Kommission macht einfach nichts, sie verweigert sich. Wir wissen, dass zum Beispiel Spyware ausgeführt wurde mit einer Genehmigung von Griechenland, von den griechischen Behörden, wurde dann aus Zypern nach Sudan geflogen, aber es gibt auch andere Beispiele, und die Kommission sagt, wenn wir nachgefragt haben, sie könne nichts machen, das sei die Verantwortung der Nationalbehörden. Es sind aber die Nationalbehörden, die mitschuldig sind. Das ist ein bisschen schwierig, wenn die Nationalbehörden schuldig sind, aber sich selbst dann irgendwie kontrollieren sollen. Und wenn die Kommission ihre Aufgaben nicht macht, dann ist es sehr, sehr schwierig. Aber die Regeln, die gibt es.

Die **Vorsitzende**: Vielen Dank, und für die FDP-Fraktion noch einmal der Kollege Redder.

Abg. **Dr. Volker Redder** (FDP): Vielen Dank, Frau Vorsitzende. Ich habe noch zwei Fragen. Der Abschlussbericht kommt zu dem Schluss, dass es begründete Zweifel an der EU-rechtskonformen Anwendung von Spyware bei den nationalen Behörden der Mitgliedstaaten gibt. Wie positioniert sich das BMI zu diesem Ergebnis, und wie steht das BMI zu mehr Kontrolle seitens der EU in diesem Bereich? Das wäre auch eine Möglichkeit.

PStS **Johann Saathoff** (BMI): Ich glaube, ich habe mich gerade schon so ein bisschen hinreißen lassen, in diese Richtung zu antworten. Ich fange einmal damit an, dass ich mir gestern Abend noch zu später Stunde die Schlussfolgerungen des Untersuchungsausschusses angeschaut habe und natürlich die Bewertung des BMI dazu auch noch einmal. Erfüllen wir das eigentlich oder erfüllen wir das nicht? Die Schlussfolgerungen sind, dass innerhalb der EU bestimmte rechtliche Mindeststandards erreicht werden müssen in der Anwendung des Ganzen. Wir erleben das in anderen Themen, gerade in Digitalisierungsthemen, auch, dass wir uns durchaus unterhalten über bestimmte Mindeststandards, zum Beispiel über KI, biometrische Echtzeitfernidentifizierung und solche Sachen. Diese Mindeststandards wollen wir alle miteinander auf europäischem Rahmen festgelegt haben, und wir streiten gerade darüber, was die deutsche Position dazu sein könnte. Diese Mindeststandards werden gefordert in diesem Bericht, und wir haben uns damit auseinandergesetzt. Letzten Endes mit dem Hintergrund, wie viel Arbeit würde das für uns eigentlich bedeuten, wie viel Diskussion mit den Parlamentariern, um diese umzusetzen, kommen wir zu dem Ergebnis – das ist jetzt kein wissenschaftliches Gutachten – , dass wir diese Mindeststandards bereits erfüllen. Die zweite Frage war, was tun wir, um uns bei anderen Staaten dafür einzusetzen, dass sie das auch tun. Das habe ich gerade gesagt: Dann müsste die Bundesregierung sich abstimmen, ob sie im JI-Rat darauf eingehen würde. Aber ich würde empfehlen, das normale Verfahren ist, dass die Kommission sich zu dem Untersuchungsausschuss verhält und dann in den Mitgliedstaaten die Diskussion anstrengt.

Abg. **Dr. Volker Redder** (FDP): Vielen Dank. An Frau in t´ Veld noch eine letzte Frage: Aus dem Bericht über die Situation in Deutschland lassen sich Schwierigkeiten des PEGA-Ausschusses in der Zusammenarbeit mit dem BKA herauslesen. Würden Sie sagen, die Kooperation mit dem BKA war mangelhaft, oder kennen Sie noch eine schlechtere Note? Wie würden Sie die generelle Zusammenarbeit im Rahmen des PEGA-Ausschusses mit den deutschen Behörden bewerten?

Sophie in t´ Veld: Ganz ehrlich, Deutschland ist nicht das größte Problem. Ich stimme auch der Regierung zu, dass Deutschland zum größten Teil die Mindeststandards schon jetzt erfüllt, vielleicht nicht alle. Aber wir haben auch von Deutschland keine Informationen bekommen, die uns irgendwie weitergeholfen haben. Die Regierung hat gerade gesagt, wir werden das erst anregen im Rat, wenn die Kommission sich dazu geäußert hat. Aber die Kommission wartet dann wieder ab, was die Mitgliedstaaten machen. Inzwischen sind Deutschland, aber auch mein Heimatland, die Niederlande und auch alle anderen Mitgliedstaaten, noch nicht isoliert voneinander. Wir leben zusammen im europäischen Raum. Es gibt Polizeizusammenarbeit, Justizzusammenarbeit, die Geheimdienste arbeiten zusammen, tauschen Informationen aus. Man kann doch nicht so tun, als ob da nichts passiert. Ich glaube, da hat jede Regierung eine Verantwortung, nicht nur für das eigene Land, aber auch für die gesamte Europäische Union. Aber jeder versteckt sich hinter einem anderen. Inzwischen haben die Vereinigten Staaten mehr Maßnahmen unternommen als die Europäer.

Die **Vorsitzende**: Vielen Dank. Für die AfD-Fraktion Herr Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank. Herr Saathoff, Sie sagten vorhin, wenn Pegasus eingesetzt wird in Deutschland, dann würde das einer richterlichen Anordnung bedürfen. Wie oft wurde es denn im vergangenen Jahr eingesetzt?

PStS **Johann Saathoff** (BMI): Sie haben mich falsch verstanden. Ich habe nicht gesagt, dass wir Pegasus einsetzen. Ich habe auch nicht gesagt, dass es einer richterlichen Anordnung bedürfte, wenn wir Pegasus einsetzten, sondern ich habe gesagt, dass Quellen-TKÜ und Onlinedurchsuchungen generell – egal mit welchen Instrumenten, Eigenentwicklung oder Fremdkauf und ohne zu sagen, was wir denn hätten kaufen können oder wollen – äußerst engen gesetzlichen Rahmenbedingungen bedürfen.

Abg. **Steffen Janich** (AfD): Konnte ich jetzt daraus entnehmen, dass wir in Deutschland durch deutsche Behörden kein Pegasus einsetzen?

PStS **Johann Saathoff** (BMI): Auch im Umkehrschluss bekommen Sie mich nicht dazu, irgendetwas zu Produkten zu sagen. Ich sage Ihnen deutlich, ich bin nicht befugt, Ihnen zu irgendwelchen Produkten Auskunft zu geben.

Abg. **Steffen Janich** (AfD): Wie viele Mal wurden denn in Deutschland insgesamt im Rahmen einer Quellen-TKÜ solche Maßnahmen durchgeführt im vergangenen Jahr?

Andreas Könen (BMI): Die Zahlen habe ich jetzt hier nicht bei der Hand, aber das BfJ veröffentlicht für jedes Kalenderjahr eine entsprechende Statistik, die nicht nur die Einsätze der Bundesbehörden, sondern auch die der jeweils zuständigen Landesbehörden mitplottet. Diese Zahlen liegen auf jeden Fall für die Jahre 2020, 2021 und jetzt in Kürze für 2022 vor.

Abg. **Steffen Janich** (AfD): Setzen deutsche Behörden im Rahmen der Quellen-TKÜ auch solche Programme im Ausland ein?

Andreas Könen (BMI): Die Quellen-TKÜ und die Onlinedurchsuchung genauso ist eine Rechtsetzung für den deutschen Rechtsraum und betrifft die Polizei. Nachrichtendienstliche Einsätze werden eben unter G10 geregelt, und zu letzteren kann ich Ihnen keine Auskünfte geben.

Abg. **Steffen Janich** (AfD): Als letzte Frage noch: Nutzen deutsche Bundesbehörden die Privatanbieter, um mit solchen Programmen eventuell Informationen zu gewinnen oder kann man das ausschließen in Deutschland?

Andreas Könen (BMI): Nein, da gibt es eben – wie wir eben auch schon bemerkt haben– sowohl die Nutzung von eigenentwickelter Software als auch von kommerzieller zugekaufter Software. So viel konnten wir sagen.

Abg. **Steffen Janich** (AfD): Ja, ich meine das etwas anders. Die Frage ist: Nutzen deutsche Bundesbehörden das Angebot von Firmen, um über diese Firmen dann Ergebnisse aus Spähsoftware zu nutzen oder gibt es das grundsätzlich nicht?

Andreas Könen (BMI): Nein, das lässt die deutsche Rechtsetzung nicht zu.

Abg. **Steffen Janich** (AfD): Vielen Dank.

Die **Vorsitzende**: Vielen Dank, und für DIE LINKE. noch einmal Anke Domscheit-Berg.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Sehr geehrter Staatssekretär Saathoff, ich will Sie nicht so leicht von der Angel lassen. Im Koalitionsvertrag steht im Kapitel Staatstrojaner: Transparenz und effektive Kontrolle durch Parlamente stellen wir sicher. Ich erkenne das hier nicht. Warum genau dürfen Abgeordnete nicht erfahren, ob ein Produkt, für das es einen ganzen Untersuchungsausschuss im Europäischen Parlament gab, von deutschen Behörden eingesetzt worden ist, obwohl das auf Wikipedia steht, obwohl die Tagesschau darüber berichtet hat, obwohl das im Innenausschuss erzählt worden ist. Jeder weiß das, nur wir dürfen es offiziell nicht erfahren. Warum nicht? Wer verweigert die Befugnis, und wie passt das zum Koalitionsvertrag?

PStS **Johann Saathoff** (BMI): Generalisiert dürfen Abgeordnete das erfahren, dafür gibt es geeignete Gremien, zum Beispiel das Parlamentarische Kontrollgremium (PKGr), wo darüber berichtet wird.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Warum dürfen wir das nicht erfahren, nicht einmal in eingestufter Form? Was ist genau der Grund?

PStS **Johann Saathoff** (BMI): Das hat ein bisschen etwas mit der Einsatzfähigkeit der Ermittlungsinstrumente zu tun und ist auch nicht generalisiert zu beantworten, sondern im Einzelfall.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Der Einzelfall ist Pegasus.

PStS **Johann Saathoff** (BMI): Frau Domscheit-Berg, wir sind aber jetzt in einer öffentlichen Sitzung, von daher fabulieren wir darüber, ob es eventuell Auskunft geben könnte in einer geheimen Sitzung. Da müssen Sie die Sitzung geheim einstufen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Können Sie uns die Informationen eingestuft in der Geheimschutzstelle schriftlich zur Verfügung stellen?

PStS **Johann Saathoff** (BMI): Das können wir prüfen, inwieweit wir Ihnen das zur Verfügung stellen können. Da müsste ich noch einmal genau von Ihnen wissen, was genau Sie wissen wollen, und dann würden wir Ihnen das nachreichen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Das sage ich Ihnen gerne. Hat eine deutsche Behörde Pegasus irgendwann erworben und irgendwann eingesetzt? Wird es heute noch eingesetzt? Wenn es erworben worden ist: Ist das direkt von der NSO Group erfolgt oder über Dritte? Wir wissen von dem Untersuchungsausschuss, dass zum Beispiel die polnische Regierung über eine polnische Drittfirma dieses Produkt bezogen hat, die Firma Matic. Diese Frage wäre auch meine und eine, die Sie vielleicht auch hier beantworten können: Ich wüsste gerne, welche Konsequenzen es für die Geschäftsbeziehungen zwischen dem Bund und der Firma NSO hat, dass die Firma NSO auf die US-Sanktionsliste gesetzt worden ist. Welche Konsequenzen hat dies für die Geschäftsbeziehungen zu den USA?

PStS **Johann Saathoff** (BMI): Wir gucken uns die Fragen ganz genau an und prüfen, ob wir Ihnen das in eingestufter Form dann zur Verfügung stellen können.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Das heißt, Sie können zu den Konsequenzen, unabhängig von Pegasus, zur US-Sanktionsliste auch nichts sagen?

PStS **Johann Saathoff** (BMI): Ich vermute, dass, wenn ich darauf vorbereitet wäre, was ich im Moment nicht bin, es auf jeden Fall auch mindestens NfD eingestuft wäre. Und von daher schlage ich vor, wenn wir Ihnen sowieso etwas nachreichen, dann können wir das gleich mitnehmen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Dann nehmen wir das mit auf. Sie haben sich ja auch die Empfehlungen des Untersuchungsausschusses durchgelesen in Vorbereitung dieser Sitzung und sich gut vorbereitet. Teilen Sie die Einschätzung der europäischen Berichterstatterin, dass NSO eine Bedrohung für die nationale Sicherheit ist, auch für uns und auch in Europa?

PStS **Johann Saathoff** (BMI): Grundsätzlich äußert sich die Bundesregierung zu Einschätzungen hinsichtlich bestimmter Unternehmen und hinsichtlich bestimmter Produkte nicht.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Das stimmt nicht. Gegen Kaspersky gab es auch eine Sicherheitswarnung von einer Bundesbehörde.

PStS **Johann Saathoff** (BMI): Das ist ein ganz anderer Fall. Grundsätzlich stimmt das wohl. Grundsätzlich äußert sich die Bundesregierung nicht. Im Einzelfall dann eben schon.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Schade, dass das kein Einzelfall ist. Wenn Sie das eingestuft beantworten können, hätten wir das dann auch gerne nachgereicht.

Die **Vorsitzende**: Vielen Dank. Wir sind am Ende der Debattenrunde und der Beratung dieses Tagesordnungspunktes. Ich danke ganz herzlich den Gästen sowohl hier im Saal als natürlich ganz besonders auch noch einmal virtuell Frau in t´ Veld und Frau Polfers. Vielen Dank für die Diskussion, und damit ist dann der öffentliche Teil der Sitzung des Ausschusses für Digitales hiermit beendet, und damit endet auch die Übertragung im Internet.

Der Ausschuss beschließt Kenntnisnahme und erwartet einen ergänzenden Bericht des Bundesministeriums des Innern und für Heimat bis zur 43. KW.

Tabea Rößner, MdB
Vorsitzende