NIEDERSÄCHSISCHER LANDTAG
18. WAHLPERIODE

N i e d e r s c h r i f t

über die 24. - öffentliche - Sitzung
des Ausschusses für Inneres und Sport
am 16. August 2018
Hannover, Landtagsgebäude

Tagesordnung: Seite:

1. a) **Entwurf eines Reformgesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze**

   Gesetzentwurf der Fraktion der SPD und der Fraktion der CDU - Drs. 18/850

   b) **Für ein Niedersächsisches Gefahrenabwehrgesetz ohne Symbolpolitik und Generalverdacht**

   Antrag der Fraktion Bündnis 90/Die Grünen - Drs. 18/828

   Vor Eintritt in die Anhörung 7

   Anhörung

   - Rechtsanwalt Dr. Cornelius Held 8

   - Chaos Computer Club e. V. 11

   - Digitalcourage e. V. 18

   - Bündnis #noNPOG - Nein zum neuen niedersächsischen Polizeigesetz 21

   Weiteres Verfahren 24

2. **Beschlussfassung über Anträge auf Unterrichtung durch die Landesregierung**

   a) **Unterrichtung über eine Konzeption des Landeskriminalamtes zur Aufarbeitung sogenannter „cold cases“** 25

   b) **Ergänzende Unterrichtung über die Bedrohung von Bürgern in Eschede durch einen Asylbewerber aus dem Sudan** 25

3. **Aktenvorlage gemäß Artikel 24 Abs. 2 der Niedersächsischen Verfassung betreffend den Aufenthalt des ehemaligen Vorsitzenden der Justiz im Iran Ayatollah Shahroudi in Hannover (2. Tranche)**

Beschluss nach § 95 a GO LT über die Vertraulichkeit der mit Schreiben des Niedersächsischen Ministeriums für Inneres und Sport vom 3. Juli 2018 vorgelegten Unterlagen 27

4. a) **Zivilbevölkerung in Syrien schützen - niedersächsischer Verantwortung gerecht werden!**

Antrag der Fraktion Bündnis 90/Die Grünen - Drs. 18/830

b) **Familiennachzug dauerhaft aussetzen**

Antrag der Fraktion der AfD - Drs. 18/843

(abgesetzt) 29

5. **Altersfeststellung bei jugendlichen Flüchtlingen**

Antrag der Fraktion der FDP - Drs. 18/1064

Beginn der Beratung 31

Weiteres Verfahren 31

6. **Testphase zur Einführung einer Elektroschockwaffe (Taser) bei der niedersächsischen Polizei**

Antrag der Fraktion der AfD - Drs. 18/1086

Erörterung von Verfahrensfragen 33

7. **Beleidigungen, Drohungen, Hass und Gewalt gegen kommunale Amts- und Mandatsträger, Rettungskräfte und Ehrenamtliche sind nicht hinnehmbar - Land und Kommunen müssen gemeinsam aktiv werden**

Antrag der Fraktion der SPD und der Fraktion der CDU - Drs. 18/1175 neu

Beginn der Beratung 35

Anwesend:

Ausschussmitglieder:

1. Abg. Thomas Adasch (CDU), Vorsitzender
2. Abg. Karsten Becker (SPD)
3. Abg. Dunja Kreiser (SPD)
4. Abg. Deniz Kurku (SPD)
5. Abg. Bernd Lynack (SPD)
6. Abg. Doris Schröder-Köpf (SPD)
7. Abg. Ulrich Watermann (SPD)
8. Abg. André Bock (CDU)
9. Abg. Rainer Fredermann (CDU)
10. Abg. Bernd-Carsten Hiebing (CDU)
11. Abg. Sebastian Lechner (CDU)
12. Abg. Uwe Schünemann (CDU)
13. Abg. Belit Onay (GRÜNE)
14. Abg. Jan-Christoph Oetjen (FDP)
15. Abg. Jens Ahrends (AfD)

Als Zuhörer nahm teil:

Abg. Sebastian Zinke (SPD).

Sitzungsdauer: 10.15 Uhr bis 12.17 Uhr.

Außerhalb der Tagesordnung

Parlamentarische Informationsreise

Der **Ausschuss** sprach über das Programm seiner für den 29. August bis zum 1. September 2018 geplanten Informationsreise nach Bayern. Er beschloss, zwei Plätze für Vertreter der LPK zur Verfügung zu stellen.

Tagesordnungspunkt 1:

a) **Entwurf eines Reformgesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze**

Gesetzentwurf der Fraktion der SPD und der Fraktion der CDU - Drs. 18/850

b) **Für ein Niedersächsisches Gefahrenabwehrgesetz ohne Symbolpolitik und Generalverdacht**

Antrag der Fraktion Bündnis 90/Die Grünen - Drs. 18/828

Zu a) erste Beratung: 15. Plenarsitzung am 17.05.2018
federführend: AfluS
mitberatend: AfRuV
mitberatend gem. § 27 Abs. 4 Satz 1 GO LT: AfHuF

Zu b) erste Beratung: 15. Plenarsitzung am 17.05.2018)
AfluS

beide zuletzt beraten: 23. Sitzung am 10.08.2018 (Anhörung)

Abg. **Ulrich Watermann** (SPD) und Abg. **Jan-Christoph Oetjen** (FDP) hatten im Vorfeld der Sitzung um die Gelegenheit gebeten, Erklärungen zu diesem Tagesordnungspunkt abzugeben. Im Einzelnen ergab sich folgende Aussprache:

Vor Eintritt in die Anhörung

Abg. **Ulrich Watermann** (SPD): Nachweislich des Vorabauszuges der Niederschrift über die 22. Sitzung am 9. August 2018 hat die Landesbeauftragte für den Datenschutz im ersten Teil der Anhörung zu diesem Gesetzentwurf gesagt:

> „Unter dem Deckmantel der Bekämpfung des internationalen Terrorismus beschneiden die vorgeschlagenen Regelungen die Freiheitsrechte der Bürgerinnen und Bürger bis zur Unkenntlichkeit.“

An anderer Stelle wird das noch einmal verschärft, nämlich wenn Frau Thiel sagt, dass versucht werde, „alle verfassungsrechtlichen Möglichkeiten zur Stärkung der inneren Sicherheit auf Biegen und Brechen“ auszuschöpfen.

Die Regierungsfraktionen - die Fraktion der SPD, deren Mitglied ich bin, und die Fraktion der CDU - haben diesen Gesetzentwurf eingebracht. Ich respektiere und akzeptiere Einschätzungen rechtlicher Art. Ich weise es aber aufs Schärfste zurück, wenn mir unterstellt wird, dass ich auf Biegen und Brechen und wegen einer vermeintlichen Terrorgefahr die Freiheitsrechte der Bürgerinnen und Bürger Niedersachsens einschränken will. Ich würde es genauso wenig zulassen, wenn im Umkehrschluss behauptet würde, dass man aus vermeintlichen Datenschutzgründen Terroropfer in Kauf nehme. Ich weise diese Unterstellungen aufs Schärfste zurück, und ich erwarte, dass die Landesdatenschutzbeauftragte klarstellt, dass solche Motive für die Regierungs- bzw. Fraktionsmitglieder nicht in Betracht kommen.

In den weiteren Ausführungen wurde auch angemerkt, dass es für das Pilotprojekt „Bodycams“ in Niedersachsen keine Rechtsgrundlage gegeben habe. Nachweislich der Beratungen zu dieser Frage in der vergangenen Wahlperiode und insbesondere der Stellungnahme des Gesetzgebungs- und Beratungsdienstes im Innenausschuss ist diese Behauptung ebenfalls falsch.

Ich will ganz deutlich sagen: Ich habe Vertrauen, dass sowohl die Polizeikräfte als auch die Justiz angemessen mit dem Werkzeug, das man ihnen durch Gesetze an die Hand gibt, umgehen. Insofern hat mich das wirklich schwer getroffen und auch schwer enttäuscht. Die Debatte war sonst sehr von gegenseitigem Respekt geprägt. An dieser Stelle war das nicht der Fall. Deshalb fordere ich die Landesdatenschutzbeauftragte hiermit auf, das klarzustellen.

Abg. **Jan-Christoph Oetjen** (FDP): Herr Watermann hat gerade von Respekt gesprochen, und ich möchte daran anschließen. Der Ministerpräsident hat gestern im NDR-Sommerinterview gesagt, dass er keinen Änderungsbedarf am Entwurf für das niedersächsische Polizeigesetz sieht und dass er so, wie er ist, beschlossen werden sollte.

Der Gesetzentwurf wurde von den Fraktionen von CDU und SPD eingebracht. Er liegt hier im Innenausschuss zur Beratung vor. Wir haben nicht

einmal die Anhörung dazu abgeschlossen, und wir haben noch keine Stellungnahme des GBD. Es sind schwerwiegende verfassungsrechtliche Fragen aufgeworfen worden. Ich halte es für eine Frage des Respekts, dass der Ministerpräsident sich nicht vor Abschluss eines solchen Verfahrens in die Angelegenheiten des Parlaments einmischt und Ansagen von vorne macht. Sonst könnten wir uns die Anhörung sparen, und auch dem GBD könnten wir - mit Blick auf die Erstellung von Vorlagen - viel Arbeit ersparen. Ich finde, das ist eine unangemessene Art und Weise, mit dem Parlament umzugehen.

Der **Ausschuss** folgte der Bitte der Abgeordneten, der Landesbeauftragten für den Datenschutz sowie Ministerpräsident Weil einen Auszug aus der Niederschrift zu der heutigen Sitzung zu übermitteln, der die beiden Erklärungen enthält.

Anhörung

Rechtsanwalt Dr. Cornelius Held

Schriftliche Stellungnahme: Vorlage 19 (zu Drs. 18/850), Vorlage 15 (zu Drs. 18/828)

Dr. Cornelius Held: Ich bin Rechtsanwalt und habe mich in den vergangenen Jahren intensiv mit dem Verfassungsrecht beschäftigt, insbesondere mit Blick auf das Thema Videoüberwachung. Das ist wahrscheinlich auch der Grund, weshalb Sie mich eingeladen haben. Dementsprechend werde ich meine Ausführungen auf das Thema Videoüberwachung fokussieren. Das betrifft insbesondere § 32 des Gesetzentwurfs. Ein inhaltliches Statement zu allen geplanten Änderungen sehe ich in der kurzen Zeit auch als nicht möglich an.

Die Perspektive, aus der ich mich dem Thema nähere, ist eine rein juristische, d. h. ich betrachte die geplanten Änderungen und den Gesetzentwurf aus rein verfassungsrechtlicher Perspektive. Es geht mir nicht um Politik, und es geht mir auch nicht um Kritik jenseits des Verfassungsrechts, sondern ich möchte einfach meine Gedanken dazu äußern, was das Grundgesetz zu der geplanten Novelle sagt.

Ich werde auch nicht an Kritik sparen - bitte, sehen Sie es mir nach. Das soll aber keine Fundamentalkritik sein, die mit irgendeinem Vorwurf verbunden ist. Ich werde verfassungsrechtliche Bedenken erheben. Die ließen sich aber bezüglich der Videoüberwachung auch auf viele andere Landespolizeigesetze übertragen. Aus meiner Sicht handelt es sich hierbei also nicht um ein singuläres Verschulden des Landes Niedersachsen, sondern es handelt sich um den momentanen Stand in der Gesetzgebung, und den möchte ich kritisch beleuchten.

Ihnen liegt bereits eine ausführliche schriftliche Stellungnahme von mir vor. Ich möchte mich im Folgenden auf die in meinen Augen ganz zentralen Punkte beschränken und Ihnen keine juristische Vorlesung halten, um möglichst schnell zum Punkt zu kommen.

Eingangs gebe ich einen kurzen Überblick über die verfassungsrechtlichen Grundlagen, die hier in meinen Augen eine Rolle spielen. Danach werde ich mich mit drei Einzelproblemen befassen. Sehen Sie es mir nach, wenn ich Positives nicht lobe oder einen Fortschritt nicht hervorhebe. Ich beschäftige mich tatsächlich nur mit dem, was aus meiner Sicht konstruktive Kritik verdient.

Zu den Grundlagen: Ein ganz wichtiger Ausgangspunkt ist der Vorbehalt des Gesetzes. Dieser besagt letztlich nichts anderes, als dass staatliches Handeln, das geeignet ist, in Grundrechte einzugreifen, einer gesetzlichen Grundlage bedarf. Das ist Ausfluss des Demokratieprinzips. Der Landtag bzw. der Bundestag soll vorher ein Gesetz erlassen, in dem steht, was der Staat darf, wenn er in Grundrechte eingreifen möchte. Daneben gibt es die aus dem Rechtsstaatsgebot folgenden Vorgaben von Normenbestimmtheit und Normenklarheit. Das bedeutet nichts anderes, als dass in einem Gesetz die Voraussetzungen und die Grenzen eines Eingriffs klar und deutlich beschrieben werden sollen. Das ist ein rechtsstaatliches Gebot, das natürlich dem Schutz der Grundrechtsträger, aber auch dem Schutz der Rechtsanwender dient - also in diesem Fall der Polizei, die ja ein ganz legitimes Interesse daran hat, nachlesen zu können, was sie darf und was nicht und unter welchen Voraussetzungen.

In der Eingriffsdogmatik ist heute eigentlich anerkannt, dass auch bei zusammenhängenden Komplexen - und als solche verstehe ich das große Thema Videoüberwachung - in die einzelnen Maßnahmen zerlegt werden muss. Jede Maßnahme eines zusammenhängenden Komplexes ist potenziell ein eigener Grundrechtseingriff. Das bedeutet, dass man auch Maßnahmen, die sich aus vielen Einzelmaßnahmen zusammensetzen,

in die einzelnen Bestandteile zerlegen muss und dann diese eben als eigenen Eingriff behandeln muss. Das heißt, die Voraussetzungen und die Grenzen müssen in einem Gesetz geregelt sein. Hierbei gilt die Regel: Je schwerwiegender der Eingriff, desto präziser müssen die Regelungen sein.

Bezogen auf die Videoüberwachung muss man, meine ich, zwischen drei Einzelmaßnahmen differenzieren, zumindest vor dem Hintergrund des novellierten § 32. Da ist zum einen die bloße Beobachtung, also wenn ein Polizist oder ein Mitarbeiter einer Verwaltungsbehörde in Echtzeit auf einem Bildschirm verfolgt, was eine Videokamera aufnimmt. Da hat sich einiges getan. Das ist in § 32 Abs. 3 Satz 1 des Gesetzentwurfs, um jetzt doch einmal etwas Positives zu sagen, klar verbessert worden. Bislang hieß es: Wenn die Polizei ihre Aufgaben wahrnimmt, darf sie auch Videoüberwachungen vornehmen. - Das ist nicht mehr zeitgemäß, und vollkommen zu Recht enthält die Novelle verschärfte Voraussetzungen, dass nämlich die Voraussetzungen und die Grenzen des Eingriffs detailliert geregelt werden.

Der zweite Einzeleingriff ist die Aufzeichnung, im Gesetzentwurf geregelt in § 32 Abs. 3 Satz 3. Das heißt, wenn die Bilder nicht nur gesehen und dann sozusagen wieder spurenlos vergessen werden, sondern aufgezeichnet werden, dann ist auch diese Aufzeichnung ein eigener Eingriff. Im Datenschutzrecht wäre das die Speicherung von Daten.

Drittens - und das ist der vielleicht neuralgischste Punkt - muss man auch die Auswertung von aufgezeichneten Daten wiederum als eigenen Eingriff verstehen. Im Datenschutzrecht wäre das die Nutzung von Daten. Aus polizeirechtlicher und verfassungsrechtlicher Perspektive muss auch hier klar unterschieden werden; denn die Auswertung, also die gezielte Durchsicht des gespeicherten Materials, ist nun einmal etwas anderes als die Beobachtung ohne Aufzeichnung oder die Aufzeichnung an sich.

Zu meiner Kritik: Zunächst möchte ich kritisieren, dass der Gesetzentwurf keine Differenzierung zwischen Aufzeichnung und Auswertung vorsieht. Es taucht keine begriffliche Differenzierung auf, sondern es ist immer nur von der Aufzeichnung die Rede. Die Aufzeichnung verstehe ich als eine Vorratsdatenspeicherung, also als eine Speicherung zu abstrakten Zwecken; d. h. man weiß noch nicht, wozu man die Daten eines Tages brauchen wird, aber sie werden gespeichert, um sie bei Bedarf parat zu haben.

Dieser abstrakte Zweck ist aber kein Selbstzweck, sondern dadurch wird eine weitere Maßnahme vorbereitet: Wenn man einen Anlass hat, sich das Bildmaterial noch einmal anzusehen, möchte man darauf zurückgreifen können. Insofern hat die Aufzeichnung einen dienenden Charakter, um die spätere Auswertung vorzubereiten und überhaupt erst diese Möglichkeit zu schaffen.

Die Auswertung ist aber - ähnlich wie die erste Beobachtung - eine visuelle Wahrnehmung. Das ist etwas ganz anderes als die Aufzeichnung. Man muss das deutlich auseinanderhalten. Gegenüber der herkömmlichen Beobachtung, also der visuellen Wahrnehmung ohne Aufzeichnung, hat - so meine ich - die Auswertung sogar eine höhere Grundrechtsintensität. Es gibt diverse Untersuchungen, die zu dem Ergebnis kommen, dass die Echtzeitbeobachtung des Bildes einer Videokamera auf Dauer so anstrengend und ermüdend für den Beobachter ist, dass er relativ wenig Details wahrnimmt und die Vergessensquote natürlich sehr hoch ist.

Demgegenüber ist die Auswertung von aufgezeichnetem Bildmaterial auf Grundlage eines konkreten Anlasses natürlich viel wacher, konzentrierter und fokussierter, und Personen, die mit dem Anlass der Auswertung überhaupt nichts zu tun haben, werden ebenfalls stärker und konzentrierter in den Fokus gerückt. Insofern ist die Auswertung ein eigener Eingriff, und sie muss auch legislatorisch als solcher behandelt werden. Dies geht momentan aus dem mir vorliegenden Gesetzentwurf nicht hervor.

Mein zweiter Kritikpunkt ist die aus meiner Sicht unzureichende Ausgestaltung des Eingriffs Aufzeichnung. Die Aufzeichnung ist eine Vorratsdatenspeicherung. Es ist geregelt, wann diese Vorratsdatenspeicherung erlaubt ist. Es ist aber beispielsweise nicht geregelt, wie lange die Daten gespeichert werden dürfen. In meinen Augen ist das eine Lücke. Die zeitlichen Grenzen sind auf Grundlage des Gesetzentwurfs weder für den Bürger noch für die Polizei zu erkennen.

Es gibt allgemeine Vorschriften - §§ 38 und 39 a -, die sich mit der Löschung von Daten beschäftigen. Daraus könnte man ja eine Pflicht zur Löschung auch für die Videodaten ableiten. Nur erkennbar sind die Vorschriften der §§ 38 und 39 a nicht auf die Videoüberwachung abge-

stimmt. Denn wenn man § 38 Abs. 1 und § 39 a Abs. 1 zusammen liest, dann ist die Speicherung der Daten letztlich so lange zulässig, wie sie für den Zweck der Erhebung erforderlich ist. Das ist ein Zirkelschluss. Zweck der Erhebung ist, dass man sie später ansehen kann, und ob es nicht doch irgendwann einen Grund gibt, sie vielleicht noch einmal anzusehen, ist nicht im Voraus zu entscheiden. Nach dieser Vorschrift darf man die Videodaten letztlich unbegrenzt speichern, was sicherlich nicht richtig sein kann. Auch hier muss es natürlich eine Frist geben, wie lange die Daten gespeichert werden dürfen, und wenn es in der Zwischenzeit keinen Anlass gibt, um sie anzusehen, dann muss man sie löschen. Das muss man in meinen Augen auch so deutlich in das Gesetz hineinschreiben.

Dass der Entwurfsverfasser die Problematik durchaus auch gesehen hat und sie letztlich genauso sieht wie ich, kann man aus dem neuen Absatz 5 erkennen, Stichwort „Bodycams“. Wenn Polizisten mit kleinen Videokameras ausgerüstet werden, ist genau geregelt, wann die Aufzeichnung beginnen darf und wann sie zu löschen ist. Das ist auch völlig richtig. So hätte man das mit den aufgezeichneten Daten aber ebenfalls regeln müssen. Oder man müsste bei den §§ 38 und 39 a Bezug nehmen auf die Videoüberwachung und es dort konkreter fassen. Man muss die Frage beantworten: Wenn es keinen Anlass gibt, die Daten später auszuwerten, wie lange dürfen sie dann maximal gespeichert werden? Ein Rückgriff auf die Erforderlichkeit reicht in meinen Augen nicht aus.

Mein dritter und letzter Kritikpunkt - dieser wiegt vielleicht am schwersten -: Der eigene Eingriff Auswertung ist in meinen Augen derzeit überhaupt nicht geregelt. Es fehlt in § 32 eine Vorschrift darüber, was passieren muss, damit die Polizei die auf Vorrat gespeicherten Bild- und Tondateien auch auswerten darf. Also: Was muss passieren, damit die Polizei im Nachhinein die Bilder ansehen darf? Reicht dafür jede Bagatelle, bedarf es dafür einer Ordnungswidrigkeit oder des Verdachts einer Straftat? Das ist aus dem Gesetzentwurf nicht ersichtlich und müsste meiner Meinung nach geregelt werden.

Letztlich ist das aus der datenschutzrechtlichen Nomenklatur gesehen - die ja auch Eingang in das Polizeigesetz gefunden hat -, in den §§ 38 und 39 geregelt. Dort steht, wann man gespeicherte Daten nutzen darf. Aber auch diese Vorschriften sind wieder nicht auf die Videoüberwachung abgestimmt, sondern sie sind so unscharf und haben einen Auffangcharakter, dass man zu keinen präzisen Ergebnissen kommt. Subsummiert man die Vorschriften auf die Videoüberwachung, dann darf man die aufgezeichneten Bilder nutzen - also auswerten -, wenn es zum Zweck der Erhebung erforderlich ist. Das erinnert mich ganz stark an die alte Formulierung, wann die Polizei überhaupt beobachten darf - nämlich einfach dann, wenn es zur Aufgabenwahrnehmung erforderlich ist.

Der Zweck der Erhebung kann nur die spätere Auswertung sein, und damit ist der Zirkel geschlossen. In meinen Augen müsste für die Auswertung genauso eine Eingriffsschwelle definiert werden, wie sie präzise für die Beobachtung und für die Aufzeichnung geregelt ist. Das ist der dritte Eingriff bzw. die dritte Ebene, und da gehört eine eigene Eingriffsschwelle ins Gesetz geschrieben.

Dass der Entwurfsverfasser meine Ansicht im Grundsatz teilt, kann man an den Regelungen zum automatisierten Abgleich von Kraftfahrzeugkennzeichen erkennen. In § 32 Abs. 6 Sätze 1 und 3 ist präzise geregelt, wie die Auswertung der visuell erhobenen Daten erfolgt. So ist es auch richtig, und so hätte man bei der Auswertung von Bildern von Videokameras ebenfalls vorgehen müssen.

Hintergrund der Regelung für die Kfz-Mustererkennung ist eine zu einem anderen Landesgesetz ergangene Entscheidung des Bundesverfassungsgerichts. Dort wurde der Transfer in das Gesetz auf Basis dieser Entscheidung vollzogen. Das ist auch richtig und zu begrüßen. Nur der Transfer, was das generell für die Videoüberwachung bedeutet, der fehlt. Insofern habe ich aus verfassungsrechtlicher Sicht derzeit ernsthafte größere Bedenken, ob die Auswertung der Daten, die Videokameras erheben, im Moment verfassungsgemäß wäre.

Wenn Sie abschließend eine anwaltliche Empfehlung hören möchten: Der § 32 des Gesetzentwurfs müsste noch einmal revidiert werden. Da müssen klare Grenzen und Voraussetzungen für alle Eingriffe hinein. Die für die Auswertung fehlen vollständig. Es ist auch nicht ersichtlich, wie lange die Daten gespeichert werden dürfen, wenn sie aufgezeichnet wurden. Redaktionell scheint mir auch nicht alles geglückt. Dazu habe ich mich schriftlich ausführlicher geäußert.

Chaos Computer Club e. V.

Schriftliche Stellungnahme: Vorlage 22 (zu Drs. 18/850), Vorlage 17 (zu Drs. 18/828)

Anwesend:

- Dr. Constanze Kurz

Dr. Constanze Kurz: Unsere umfassende schriftliche Stellungnahme liegt Ihnen vor. Ich werde im Folgenden deshalb nur auf einige Aspekte eingehen, die mir wichtig erscheinen. Ich werde nichts zur Videoüberwachung sagen, die wir vor allen Dingen im Bereich der verdeckten Videoüberwachung kritisch sehen. Das Kriminologische Forschungsinstitut Niedersachsen hat dazu schon vieles gesagt, ich will das nicht wiederholen. Ich werde auch nichts weiter zur Fußfessel sagen, weil ich weiß, dass auch das im Rahmen der Anhörung bereits intensiv besprochen wurde.

Ich werde mich vielmehr dem widmen, wo wir vom Chaos Computer Club eine andere Perspektive haben, - nämlich dem Staatstrojaner, den Sie in zwei Varianten in dieses Polizeigesetz aufnehmen wollen - in Form einer Quellen-TKÜ, die sich auf laufende Kommunikation beziehen soll, und in Form der Online-Durchsuchung, also die Durchsuchung des gesamten informationstechnischen Geräts. Dabei gibt es verschiedene Risiken technischer und rechtlicher Natur.

Im Rahmen der Stellungnahme haben wir auf Seite 2 darauf verwiesen, dass wir sowohl beim Bundesverfassungsgericht wie auch bei anderen Landtagen und im Bundestag dazu Stellungnahmen abgegeben haben, insbesondere zu der Frage, welche Risiken für die innere Sicherheit mit dem Kauf von Sicherheitslücken oder generell mit der Benutzung von Schadsoftware zur Spionage einhergehen. Ich würde auf diese längeren Stellungnahmen, die wir dazu geschrieben haben - auch im Rahmen des Beschwerdeverfahrens gegen das BKA-Gesetz - verweisen, in denen wir auf diese Problematiken intensiver eingehen.

Ganz klar ist, dass im niedersächsischen Polizeigesetzentwurf ein großer Rückgriff auf die Entscheidungen, die zum BKA-Gesetz gefallen sind, erfolgt. Faktisch haben Sie im Wesentlichen aus dem Urteil kopiert - ich kann es nicht anders sagen. Der Bundesgesetzgeber hat das auch so gemacht. Das bedeutet aber auch, dass Sie die alleräußersten Grenzen, die Karlsruhe gesetzt hat, jetzt quasi als Grenzen in Ihrem Gesetzentwurf haben, und damit stehen Sie vor einem Problem. Denn wie Sie wissen, hat sich man sich bei der StPO-Novellierung auch sehr stark an dem Urteil orientiert, und hierzu gibt es bereits vier rechtlich und technisch sehr gut begründete Verfassungsbeschwerden, die in einigen Jahren sicherlich zu einem weiteren Urteil aus Karlsruhe führen werden, wonach die Landtage, die sich jetzt für die Trojaner entscheiden, sicherlich noch einmal nacharbeiten müssen. Mir sind keine Verfassungsjuristen bekannt, die nicht schon schwerwiegende Mängel in der StPO-Novelle, aber auch in verschiedenen anderen Landesgesetzen bezüglich dieser Staatstrojaner gefunden haben.

Wie auch andere Länder und der Bund haben Sie sich für zwei verschiedene Varianten von Trojanern - Quellen-TKÜ und Online-Durchsuchung - entschieden. Technisch gesehen, ist natürlich - so steht es auch in beiden Urteilen zum Staatstrojaner - die eigentliche Infiltration des informationstechnischen Systems der tatsächliche Übersprung und damit auch der Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Die Beschränkung besteht quasi immer nur im Nachhinein in technischer Art, dass man nämlich, wenn man das Gerät gehackt hat, bestimmte Funktionen des Trojaners nicht ausführen kann.

So ist es auch bei dem Trojaner gewesen, den der Chaos Computer Club analysiert hat. Wir haben diese Analyse 2011 öffentlich gemacht. Wie Sie wissen, war dieser Staatstrojaner rechtswidrig, aber er war vor allen Dingen auch handwerklich eine große Peinlichkeit. Keiner derjenigen, die ihn eingesetzt haben - und auch nicht die Richter, die das geprüft haben, oder die Strafverteidiger, die diesen Trojaner später gefunden haben, weil er nicht einmal korrekt gelöscht war -, hätte dies prüfen können; denn niemand - auch nicht der Bundesdatenschutzbeauftragte oder die betroffenen Landesdatenschutzbeauftragten - hatte den Quellcode dafür vorliegen. Das heißt, die desaströsen handwerklichen Mängel dieser Spionagesoftware hätten gar nicht aufgedeckt werden können.

Vor diesem Problem stehen Sie natürlich auch. Sie laufen heute sogar noch stärker als damals darauf zu. Das geht ganz klar aus den Problemen, die sich beim Staatstrojaner im Bund ergeben, hervor. In der schriftlichen Stellungnahme haben wir darauf hingewiesen, dass die Firmen,

mit denen im Bund zusammengearbeitet wird, sich weigern, eine Zusammenarbeit so zu gestalten, dass sie eine Prüfungsmöglichkeit etwa von einem unabhängigen Sachverständigen oder z. B. bei Landesdatenschutzbeauftragten zulassen. Tatsächlich muss man sagen, dass das eine Form von Erpressung ist - das finden Sie auch zitiert -, weil die Hersteller dann sagen: Wir arbeiten nicht mit jemandem zusammen, wenn wir solche Bedingungen diktiert bekommen. - Ich glaube, in diese Falle sollte der Gesetzgeber nicht tappen.

Wie Sie wissen, gibt es auch einen anderen Weg. Seit vielen Jahren wird eine Eigenentwicklung, für die es auch eine Standardleistungsbeschreibung gibt, entworfen - die sogenannte RCIS, in der zweiten Version auch für mobile Geräte. Soweit wir wissen - zumindest aus den Unterlagen, die im Bund bekannt sind -, ist bisher keine rechtmäßige Variante davon tatsächlich im Einsatz. Das ist noch ein praktisches Problem, vor dem Sie stehen.

Dazu gehört noch ein anderer Bereich, der mir auch schon im Bund, aber auch bei anderen Landespolizeigesetzen aufgefallen ist. Offenbar gibt es in Niedersachsen - wie auch im Bund - keinerlei Zahlen, wie viele Geräte eigentlich betroffen sind und wo tatsächlich die Notwendigkeit besteht. Es werden keine Zahlen erhoben, in wie vielen Fällen tatsächlich nur mithilfe eines Trojaners ein Zugriff auf eine Kommunikation erfolgen kann. Als Parlamentarier würde ich mir diese Zahlen doch einmal geben lassen und nicht sozusagen ins Blaue hinein annehmen, dass es ein größeres Problem gibt, das man mit einem Trojaner lösen kann, mit dem man sich ohne Zweifel auch wieder neue Probleme schafft.

Mir fällt zudem auch hier - wie beim Bund - wieder auf, dass andere Möglichkeiten, an die gewünschte Kommunikation, die nach einer richterlichen Genehmigung für die Polizeibehörden ja auch abzuhören wäre, heranzukommen, überhaupt nicht exploriert werden. Sie haben überhaupt nicht erwogen, das Hacken der Geräte sein zu lassen und mit anderen technischen Mitteln an diese Kommunikation zu kommen.

Eine letzte Bemerkung zur Quellen-TKÜ: Sie haben auch hier eine Regelung übernommen, die ich für sehr fragwürdig halte, sowohl technisch als auch rechtlich gesehen. Die Quellen-TKÜ soll sich ausschließlich auf die laufende Kommunikation beziehen. Im Landesgesetzentwurf ist aber eine Regelung enthalten, die ganz klar macht, dass man das, wenn man schon ein Gerät gehackt hat, neben der laufenden Kommunikation auch auf Daten ausweiten darf, die das Programm, mit dem kommuniziert wird, betreffen, also auf zurückliegende oder gespeicherte Daten. Das halte ich für sehr problematisch; denn letztlich ist eine Kommunikation erst dann geschehen, wenn sie den Rechner verlässt. Wenn man gespeicherte Daten - etwa E-Mail-Entwürfe oder Entwürfe für eine WhatsApp-Nachricht - mitspeichert, ist das keine laufende Kommunikation, und auch Metadaten, die man etwa aus dem Programm erlangen könnte, sind aus meiner Sicht von der Quellen-TKÜ eigentlich nicht abgedeckt. Denn dann wäre es eine Online-Durchsuchung und mit deutlich höheren Grenzen überhaupt nur umsetzbar. Das ist ja gerade der Unterschied zwischen der Quellen-TKÜ und der Online-Durchsuchung.

Ein weiterer Bereich, der mir sehr wichtig erscheint, der aber sowohl in der Diskussion in den Landesparlamenten als auch im Bund aus meiner Sicht leider viel zu kurz kommt, ist die Frage des Kernbereichsschutzes. Der Kernbereichsschutz hat, wie Sie wissen, nichts mit der Privatsphäre zu tun, sondern er beschäftigt sich mit dem Höchstpersönlichen, mit der Intimsphäre von Menschen. Wir reden hier etwa von Telefonaten zwischen Partnern, von Bildern und Filmen, die Höchstpersönliches betreffen wie z. B. die Geburt der Kinder etc.

Mit dem Staatstrojaner, den ich bereits erwähnt hatte und der nicht nur handwerklich mangelhaft, sondern auch rechtswidrig war, wurde ebenfalls in diesen Kernbereich eingegriffen - ein Sex-Telefonat wurde aufgezeichnet und auch noch transkribiert -, der eigentlich nach mehreren Entscheidungen des Bundesverfassungsgerichts absolut geschützt ist. Egal, was man jemandem vorwirft: In diesen höchstpersönlichen Bereich darf nicht eingegriffen werden.

Aus meiner Sicht sind die Regelungen sowohl bei der Quellen-TKÜ als auch bei der Online-Durchsuchung für den Bereich des Schutzes des Höchstpersönlichen von Menschen nicht ausreichend. Ich denke, an dieser Stelle müsste auf jeden Fall nachgearbeitet werden. Es sollte zumindest versucht werden - wie es etwa beim „Großen Lauschangriff“ der Fall ist -, eine ordentliche Kernbereichsprognose zu machen und abzuschätzen, ob man nach dem Hacken des Gerätes nicht tatsächlich Gefahr läuft, in diesen höchstpersönlichen Bereich einzugreifen.

Noch ein paar Anmerkungen zur Evaluation: Den im Polizeigesetzentwurf vorgesehenen Evaluationszeitraum halte ich für exorbitant lang, vor allen Dingen was die Spionagesoftware angeht. Im IT-Bereich bewegt sich jede Form von technischer Innovation mit einer sehr schnellen Veränderungsrate. Ich halte diese vielen Jahre definitiv für nicht adäquat. Man müsste sehr viel früher gucken und einen Blick darauf werfen und gerade bei den technischen Maßnahmen versuchen, schneller zu evaluieren. Ich würde ein oder zwei Jahre vorschlagen.

Zudem würde ich in Anlehnung an das, was ich eben schon sagte, vorschlagen, die Anforderungen an etwaige kommerzielle Partner, mit denen man hier vermutlich zusammenarbeiten müssen wird, ganz klar zu fassen und zu stellen, sodass man solche Peinlichkeiten wie beim Staatstrojaner, der aufgedeckt wurde, vermeidet. Insbesondere sollte man auch eine Regelung für den Quellcode finden und überlegen, ob es eine unabhängige Stelle geben kann, die den Quellcode dieser Spionagesoftware einsehen kann.

Es gibt noch einen Bereich, der aus meiner Sicht sowohl in diesem Polizeigesetzentwurf als auch im Bund eine problematische Entwicklung darstellt. In den beiden Verfassungsgerichtsentscheidungen, bei denen der Chaos Computer Club als sachverständig anwesend war, wurde dieser Bereich sehr wenig besprochen. Ich sehe aus rechtlicher Sicht auch eine gewisse Begründung dafür; denn der Gesetzgeber muss eine gewisse technische Offenheit in seine Gesetze schreiben.

Die Frage ist, inwieweit man mit einer Spionagesoftware Leben und Gesundheit von Menschen gefährden kann. Der niedersächsische Polizeigesetzentwurf enthält keine Regelung dahin gehend, welche Arten von informationstechnischen Geräten gehackt werden dürfen, also wo solch eine Spionagesoftware eingebracht werden kann. Mein Vorschlag wäre, dass man versucht, die Arten der informationstechnischen Geräte, die infiltriert werden dürfen, zu benennen, insbesondere bei der Quellen-TKÜ. Dort ist ja ohnehin schon die Beschränkung auf die laufende Kommunikation vorgesehen.

Ich würde mit so einer Regelung ausschließen wollen, dass man über diese Geräte unabsichtlich oder auch durch Fehlfunktionen, die durch so eine Spionagesoftware entstehen können, Leben oder Gesundheit von Menschen in Gefahr bringt. Das wäre in gewisser Form rechtliches Neuland; denn das ist bisher weder auf Landes- noch auf Bundesebene versucht worden. Aber aus meiner Sicht muss man auch die Tatsache bedenken, dass wir Computer letztlich nicht mehr nur bei uns tragen, sondern z. B. auch darin sitzen. Im Rahmen der Schadsoftware-Wellen im vergangenen Jahr und im Jahr davor haben wir erstmals gesehen, was Spionagesoftware, die aus staatlichem Besitz entkommen ist, anrichten kann. Der WannaCry-Vorfall hat sozusagen die freie Umwelt und auch das Leben und die Gesundheit von Menschen betroffen.

Ich darf daran erinnern, dass diese Schadsoftware, die die Welt in der Summe 4,5 Milliarden Euro gekostet hat, aus den Arsenalen staatlicher Spionagesoftware gekommen ist. Wie wir wissen, haben manchmal auch staatliche Behörden Schwierigkeiten, ihre digitalen Waffen sozusagen für sich zu behalten. In diesem Fall sind sie gestohlen worden, und dabei hat man ganz deutlich gemerkt, dass durch diese Schadsoftware auch das Leben von Menschen gefährdet wurde. Ich würde vorschlagen, dass man zumindest bei der Quellen-TKÜ die Art der informationstechnischen Geräte, die damit infiltriert werden können, benennt. Hier ist auch an alle Arten von Medizinalgeräten zu denken, die Betriebssysteme haben, die heute vollwertige informationstechnische Systeme sind und die immer mehr vernetzt sind.

Ich verweise im Weiteren auf unsere schriftliche Stellungnahme sowie auf die Stellungnahmen, die wir darüber hinaus bereits zu diesem Thema verfasst haben. Um ganz ehrlich zu sein: Ich halte die Gefahren, die von den Regelungen, die Sie im Wesentlichen übernommen haben - so wie es auch in der StPO geregelt wurde -, ausgehen, letztlich für größer als den Nutzen, den diese für die Polizei haben. Sie bekommen damit einfach sehr viele Probleme, und Sie schaffen sich ein Sicherheitsproblem.

Zum anderen möchte ich als letzten Gedanken an einen Begriff, der auch in Karlsruhe geprägt wurde, erinnern, nämlich an die sogenannte Gesamtüberwachungsrechnung. Man muss sich schon klarmachen, dass in den Fällen, in denen solche Staatstrojaner eingesetzt werden können, man heute eine ganze Reihe an anderen technischen Möglichkeiten hat. Insofern stellt sich die Frage, ob man sich zusätzlich noch daran machen will, die Geräte zu hacken und dafür irgendwie in diesen Graumarkt der Sicherheitslücken einzusteigen und staatliche Gelder zu investieren,

um Sicherheitslücken aufzukaufen, die dann gleichzeitig auch die eigenen Verwaltungsbehörden und deren Computer oder auch die Wirtschaft betreffen.

Ich würde sagen, dass man sich im Ergebnis eher einen Unsicherheitsfaktor schafft, den man sicherlich mit einer guten technischen Beratung und der Überlegung, wie man anders an diese Kommunikationsdaten kommen kann, leicht vermeiden könnte. Man hätte dann im Übrigen auch nicht das Problem, dass man immer nach Karlsruhe und auf diese vier Verfassungsbeschwerden schielen muss, die aus meiner Sicht ohne Zweifel zumindest in Teilen erfolgreich sein werden.

Abg. **Belit Onay** (GRÜNE): Ich habe eine kurze Anmerkung zu Ihrem Hinweis zur Zahl der Fälle. Das haben wir bereits thematisiert, als die Vertreter der Polizei angehört worden sind und ich die Frage gestellt habe, wie denn dieses Verhältnis sei. Zahlen dazu liegen offenbar tatsächlich nicht vor - auch der Polizei nicht. Man ist uns da zumindest eine schlüssige Antwort schuldig geblieben.

Ich habe eine Frage zu Ihrem Vorschlag, die Art der Endgeräte zu definieren, sowohl technisch als auch rechtlich. Es gibt, glaube ich, bisher keine vergleichbaren Formulierungen in Gesetzestexten.

(Dr. Constanze Kurz: Nicht in Deutschland!)

- Aber vielleicht woanders. Vielleicht können Sie uns dazu etwas sagen.

Die Frage ist aber auch, ob das überhaupt sinnvoll ist. Die WannaCry-Software war beispielsweise eine Windows-Schadsoftware. Dann ist es doch im Grunde letztlich egal, auf welchem Gerät sie läuft, oder? Lässt sich das tatsächlich an den Endgeräten definieren, damit eine Schadsoftware eben keine anderen Computer und Systeme infizieren kann, so wie es bei WannaCry der Fall war?

Dr. Constanze Kurz: Das ist ein komplexes Thema. Aus der Erfahrung mit anderen Landespolizeien - aber auch mit den Sicherheitsbehörden im Bund - bin ich der Meinung, dass der Fokus ganz stark auf dem Betriebssystem Windows liegt.

Anders, als man es vielleicht in der Zeitung liest, sind die Vertreter der Polizeibehörden und auch die der deutschen Geheimdienste keine Magier, sondern sie beschränken sich in der Regel auf die Möglichkeiten, die diese Polizeien haben. Das ist in der Regel eine Fokussierung auf Windows. Das liegt auch daran, was der Markt hergibt, sprich daran, was von den wenigen Firmen, mit denen im Bund und in den Ländern kooperiert wird, angeboten wird. Aufgrund der Tatsache, dass die meisten informationstechnischen Geräte mit diesem Betriebssystem arbeiten, ist der Markt dort am größten.

Sie müssen sich schon klarmachen, dass, wenn Sie eine Sicherheitslücke etwa für einen Windows-PC kaufen wollen, es ein Preistag gibt. Der Markt wird von staatlichen Geldern aus vielen Ländern - mittlerweile auch aus Deutschland - befeuert. So entscheidet sich, wo man Sicherheitslücken kaufen kann. Bei dem Hersteller Microsoft ist es so - das war gerade die Problematik bei dem WannaCry-Vorfall und der Grund, aus dem so viele tausende Rechner betroffen waren -, dass er sich jeweils nach einigen Jahren entschließt, keine Sicherheitsupdates für ein Betriebssystem mehr zu geben. Das Betriebssystem gilt dann als veraltet, und man kann keine Patches mehr herunterladen.

Das heißt, diejenigen, die dieses Betriebssystem einsetzen - wie z. B. Großbritannien, wo eine ganze Reihe von Krankenhäusern betroffen war -, haben ältere Versionen, bei denen sie gar nicht mehr die Möglichkeit haben, ein Update einzuspielen. In vielen Systemen kann man das ohnehin nicht, weil man z. B. anschließende Softwaresysteme - das ist insbesondere in Krankenhäusern so - ebenfalls updaten müsste. Deshalb vermeidet man ein Update.

Zudem haben die staatlichen Behörden, die diese Schadsoftware besessen haben, sechs, sieben Jahre von dieser Sicherheitslücke gewusst und sie nicht gemeldet. Auch in Niedersachsen gibt es keinerlei Regelung, wie man damit umgehen will, wenn man z. B. eine bestimmte Sicherheitslücke mit einer staatlichen Spionagesoftware ausnutzt. Wie lange will man das eigentlich tun? Findet man irgendwann eine Regelung, wie man - z. B. nach einer bestimmten Zeit - die Hersteller informiert?

Habe ich jetzt alle Fragen, die Sie hatten, beantwortet?

Abg. **Belit Onay** (GRÜNE): Sie meinten, dass es in Deutschland keine Regelung gibt, die die Art der Endgeräte definiert. Gibt es sie international?

Dr. Constanze Kurz: Es wäre ein gewisses Neuland, wenn man aufgrund einer möglichen Gefährdung von Leben oder Gesundheit von Menschen die Art der Geräte beschränken würde. Bei der Quellen-TKÜ halte ich es für nicht allzu schwer, weil man dort ohnehin auf Kommunikation abstellt. Man könnte es dort z. B. auf Kommunikationsgeräte einschränken. Damit würde man ausschließen, dass z. B. Medizinalgeräte oder Computer, in denen wir sitzen - die wir heute Autos nennen -, betroffen sind.

Sicherlich ist das nicht einfach; denn wenn Sie z. B. als Gesetzgeber ein Kommunikationsgerät für die Quellen-TKÜ definieren, dann könnte man sagen: Na ja, ein Auto ist auch ein Kommunikationsgerät - das ist es auch faktisch, weil es gleich drei Mobiltelefonmodule enthält.

Ich finde die Regelung schwierig. Letztlich muss ich sagen, ich würde auf die staatliche Infiltration aus vielen Gründen verzichten. Mir ist aber klar, dass das jetzt gerade nicht dem Zeitgeist entspricht.

Für mich ist das ein Vorschlag, bei dem ich auf die Expertise im juristischen Bereich, die jetzt erstellt wird, setzen würde. Ich finde es ausgesprochen schade, dass in diesem schwierigen Bereich immer nur das Verfassungsgericht eine Rechtsfortentwicklung vornimmt und sich die Landtage und der Bund immer nur darauf beschränken, aus den Urteilen zu kopieren. Ich halte das für eine fatale Fehlentwicklung. Ich denke, auch ein Landesgesetzgeber könnte sich darüber Gedanken machen und bezüglich der Frage, wie man dort Schranken setzen könnte, die Expertise von Juristen hinzuziehen.

Beispielsweise ist auch an Implantate zu denken. Ich trage vier informationstechnische Geräte mit mir herum. Laut dem Gesetzentwurf könnten Sie sie alle hacken. Ich denke, diese Regelung ist nicht mehr zeitgemäß, erst recht nicht für die volldigitale Zukunft, in die wir gehen. Aber ich bin leider kein Jurist, sondern Technikerin.

Abg. **Jan-Christoph Oetjen** (FDP): Sie haben gesagt, Sie würden auf die Nutzung von Trojanern verzichten, weil die Risiken größer sind als der Nutzen. Sie haben zudem gesagt, es gebe noch andere technische Mittel als Hacking. Ich verstehe das Bedürfnis der Polizei, die sagt, sie dürfe zwar die Telefone abhören, aber heute werde nicht mehr telefoniert, sondern auf anderem Wege kommuniziert, und darauf habe sie letztlich keinen Zugriff. Welche Alternativen können Sie aufzeigen, die nicht diese Risiken mit sich bringen wie das Hacken?

Dr. Constanze Kurz: Solche Alternativen hätten zunächst den Vorteil, dass keine Risiken bezüglich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eröffnet würden. Man würde darin nicht eingreifen. Tatsächlich gibt es einige bekannt gewordene Fälle - insbesondere vom BKA -, in denen man andere Techniken benutzt hat. Dabei nutzt man in der Regel aus, dass Menschen Fehler machen, dass sie z. B. eine Software installieren, die nur so tut, als sei sie ein Messanger. Man hat also versucht, diejenigen, deren Gespräche man abhören will, zu überlisten. Es gibt da eine ganze Reihe von Möglichkeiten.

Wir wissen sogar ein wenig mehr darüber. Aus den Snowden-Dokumenten haben wir eine ganze Menge darüber erfahren, was die amerikanischen Behörden seit vielen Jahren machen, wenn sie die Geräte nicht hacken, also welche Möglichkeiten noch bestehen. Ich finde es interessant, dass kein Landtag diese Möglichkeiten überhaupt einmal exploriert, obwohl man schwierige rechtliche Fragen damit umgehen könnte.

Man vermeidet im Prinzip, dass man eine Spionagesoftware einschleust, indem man z. B. Softwareprodukte wie Messenger nachbaut und sie dem Verdächtigen unterschiebt. Solche Möglichkeiten sind auch in Deutschland schon bekannt geworden, und es gibt noch mehr davon. Das amerikanische FBI hat eine ganze Abteilung dafür, wie wir heute wissen. Ich denke, das zu explorieren, wäre durchaus eine Möglichkeit, wenn man sich dazu entschließen könnte, vom Hacken der Geräte, vom Eindringen und damit vom Kauf und vom Offenlassen von Sicherheitslücken abzusehen.

Abg. **Jan-Christoph Oetjen** (FDP): Ganz konkret meinen Sie beispielsweise das Aufspielen einer Software über einen E-Mail-Anhang und Ähnliches, womit man ja keine Sicherheitslücke ausnutzt, sondern die Dummheit des Menschen. Eine Möglichkeit wäre auch sozusagen der physische Kontakt, indem man an das Gerät, auf dem man gern etwas installieren möchte, selbst heran-

kommt und die Software aufspielt. Habe ich das richtig verstanden?

Dr. Constanze Kurz: Teilweise. Ob Sie eine Spionagesoftware aufspielen, wenn Sie das Gerät physisch in die Hand nehmen, spielt hier keine Rolle. Mir ging es darum, dass man das Hacken, also den tatsächlichen Eingriff in das Betriebssystem, vermeidet. Beim BKA hat man etwa einen Messenger genutzt. Man hat sozusagen diejenigen, die glaubten, über diesen Messanger zu kommunizieren, ausgetrickst, indem man ihnen eine Software unterjubelte, die das Mithören erlaubte. - Ich finde, es ist es wert, solche Möglichkeiten zu explorieren.

Abg. **Doris Schröder-Köpf** (SPD): Ich persönlich habe Sie so verstanden, dass ein großes Problem darin besteht, dass wir gar nicht wissen, was wir da kaufen, wenn wir Spionagesoftware kaufen, und dass deswegen der Quellcode irgendwo deponiert werden müsste. Wäre es eine Möglichkeit, dies bei der Landesbeauftragten für den Datenschutz oder bei einer anderen Institution zu hinterlegen? Wie wird das anderswo geregelt?

Dr. Constanze Kurz: Nicht einmal bei dem Staatstrojaner, den wir aufgedeckt haben, ist der Quellcode jemals offengelegt worden. Das ist später sowohl von Landesdatenschutzbeauftragten wie auch vom damaligen Bundesdatenschutzbeauftragten versucht worden. Unsere Analyse war ein Reverse Engeneering. Das heißt, wir haben uns die Binaries dieses Trojaners angesehen und daraus Schlüsse gezogen.

Tatsächlich weigern sich - zumindest im Bund - die kommerziellen Partner, bei denen man die Spionagesoftware kaufen möchte, diesen Quellcode herauszugeben - aus gutem Grund. Denn das ist deren Geschäft, und wenn er herausgegeben wird, ist er kopierbar. Diese Anbieter agieren ja in der Regel nicht nur im deutschen Raum, und sie haben nicht nur deutsche staatliche Behörden als Kunden. Das ist ein weiteres Problem; denn einige - zumindest die kommerziellen Anbieter, die im Bund in Erwägung gezogen werden - haben überhaupt keine Skrupel, mit irgendwelchen Diktatoren auf der Welt zusammenzuarbeiten. Davon würde ich mich als deutscher Staatsbürger sehr abgrenzen.

Tatsächlich ist das problematisch. Man müsste eine Stelle finden - ich denke, die Landesdatenschutzbeauftragte wäre eine Variante -, die diesen Quellcode prüfen kann. Das dient auch dem Manipulationsschutz; denn wir reden ja hier nicht von Geheimdiensten, sondern von der Polizei. Das heißt, im Regelfall werden die Daten, die erlangt werden, später in Gerichtsprozessen verwendet - sowohl von der Strafverteidigerseite als auch von der staatsanwaltlichen Seite -, und da möchte man schon belegen können, dass diese Daten tatsächlich von dem Gerät stammen und nicht manipuliert wurden. Denn wenn Sie ein Gerät hacken, können Sie natürlich auch Daten platzieren oder manipulieren. Entsprechend muss man zum einen ein gutes Protokoll haben: Was hat die Spionagesoftware tatsächlich zu welchem Zeitpunkt getan? Zum anderen muss man ausschließen können, dass es zu einer Manipulation gekommen ist.

Ich halte den Weg, den Quellcode zumindest zu hinterlegen, für unabdingbar. Schließlich eröffnet dieses Hacken der Geräte alle Möglichkeiten: Sie können Daten löschen, Sie können Daten platzieren, Sie können Daten manipulieren. Wenn Sie jemanden bestrafen wollen, müssen Sie in einem Strafprozess schon belegen, dass die Daten genau die Daten von dem Rechner sind. So wird es auch sonst in der digitalen Forensik gemacht.

Abg. **Doris Schröder-Köpf** (SPD): Das hat bisher keiner geschafft?

Dr. Constanze Kurz: Der Quellcode liegt vor für die Variante, die das BKA selbst entwickelt hat, also RCIS. Ich kann zu der Eigenentwicklung wenig sagen. Wie Sie wissen, hat das ungefähr 6 Millionen Euro gekostet. Ich weiß nicht, was das BKA da macht und warum es trotzdem noch kommerzielle Partner hinzuzieht.

Natürlich haben kommerzielle Partner kein Interesse daran, den Quellcode herauszugeben. Sie sollten es aber festschreiben. Sicherlich müsste der Staat bzw. in diesem Fall das Land Niedersachsen dann auch zusichern, den Quellcode nicht weiterzuverwenden, d. h. man müsste da einen Vertrag eingehen.

Abg. **Doris Schröder-Köpf** (SPD): Sie sagen, dass man bestimmte Geräte, die Leib und Leben gefährden könnten, ausschließen sollte. Wenn man das in den Gesetzestext schreiben würde, könnte das meiner Ansicht nach wie eine Einladung wirken, genau für diese ausgeschlossenen Geräte Möglichkeiten zu deren Nutzung zu entwickeln. Gäbe es eine Möglichkeit, genau das zu verhindern?

Dr. Constanze Kurz: Ich muss an dieser Stelle vielleicht mit einem Mythos aufräumen. Selbstverständlich gibt es auch heute sehr viele informationstechnische Geräte, die nicht von der Polizei oder von den Geheimdiensten gehackt werden können. Sie können das immer umgehen, wenn Sie das Geld haben, jemanden dafür zu bezahlen, oder wenn Sie selbst die technische Expertise haben. Im Regelfall bezieht sich diese Spionagesoftware auf bestimmte Betriebssysteme. Und es gibt sehr viel mehr Betriebssysteme als Windows.

Selbstverständlich können Sie wirksam verhindern - das tun übrigens auch viele staatliche Behörden und auch Wirtschaftsunternehmen -, dass Sie gehackt werden. Das ist nicht wie in einer amerikanischen Vorabendserie, in der man immer in zwei Minuten auf einem Gerät ist. Im Gegenteil: Es gibt nur eine bestimmte Art von Geräten, die typischerweise mit solch einer staatlichen Spionagesoftware überhaupt zugänglich sind. Selbstverständlich können Sie auch verhindern - Sie haben ja die Hoheit über das Gerät -, dass jemand einen Trojaner bei Ihnen platziert.

Insofern halte ich eine Einschränkung eher deshalb für wichtig, um auszuschließen, dass Sie nicht zufällig auch ein vernetztes Auto hacken oder Implantate, die man trägt, oder auch ein Gerät, was eine Gesundheitskomponente hat und z. B. die Körperfunktionen überwacht. Es geht ja nur darum, auszuschließen, dass Sie das informationstechnische Gerät, indem Sie es hacken, auch manipulieren. Das kann ja passieren. Das kann auch eine Fehlfunktion sein. Es geht nicht darum, ob Sie möglicherweise jemanden daran hindern. Das kann man sowieso mit technischer Expertise, oder wenn man jemanden bezahlt, der diese Expertise hat.

Abg. **Sebastian Lechner** (CDU): Sie sagten, es könnte zufällig passieren, dass man Medizinalgeräte hackt. Ich habe es so verstanden, dass man bei der TKÜ oder einer Online-Untersuchung immer sehr auf IP-Adressen fokussiert ist und man eine Untersuchung wahrscheinlich auch nur für ein bestimmtes Gerät beantragen kann, weil man ja auch dem Übermaßverbot unterliegt und dem Richter, der das anordnet, nachweisen muss, dass die Maßnahme geeignet ist. Mir fehlt ein bisschen die Fantasie, wann es geeignet sein könnte, Medizinalgeräte einzubeziehen. Können Sie erklären, wie das technisch durch Zufall passieren kann, wenn eine Geräteadresse vorliegt?

Dr. Constanze Kurz: Natürlich müssen Sie eine ordentliche Analyse machen, um das Zielsystem zu analysieren, damit Sie wissen, welche Art von Spionagesoftware Sie dort überhaupt platzieren können. Sie müssen vorher wissen, was das für ein Gerät ist, was es für ein Betriebssystem hat und wo überhaupt Schwachstellen sind, an die Sie andocken können. Diese Analyse passiert.

Die Erfahrung aus den vergangenen Jahren zeigt - deswegen gab es beim WannaCry-Vorfall so viele Probleme -, dass die Tatsache, dass solche Schadsoftware sozusagen aus den digitalen Waffenschränken des Staates entkommen kann, einen hohen Gefährdungsgrad darstellt. Und dass in diesem Fall so viele Krankenhäuser betroffen waren, lag schlicht an der Art der Sicherheitslücke und an dem Betriebssystem.

Wenn Sie derjenige sind, der den Command-and-Control-Server hat, und Sie die Quellen-TKÜ aufspielen, werden Sie sich natürlich Mühe geben, tatsächlich auch das richtige Gerät zu finden.

Ein informationstechnisches Gerät kann natürlich auch gleichzeitig Medizinalgerät sein, wenn es z. B. den Gesundheitsstatus monitort. Die Geräte wachsen ja sehr stark zusammen. Ich würde auch nicht vermuten, dass morgen zufällig so ein Staatstrojaner in meinem Auto landet, obwohl das Auto auch ein Betriebssystem hat. Aber Sie machen dieses Gesetz ja auch nicht nur für heute, sondern Sie machen es für die nächsten Jahre. Insofern wäre ich da schon vorsichtig. Wir haben gesehen, dass Ihr Gesetzentwurf die Möglichkeit enthält, sozusagen auf Drittrechner zuzugreifen. Da sehe ich schon eine gewisse Gefahr.

Abg. **Sebastian Lechner** (CDU): Sie sprachen von der Gesamtüberwachungsrechnung. Man hat mir erklärt, dass Sicherheitslücken beim Android System für Handys oder beim iOS System für Apple nicht unbedingt gleich eine Sicherheitslücke für VW oder eine staatlichen Behörde darstellen müssen; denn das seien oft geschlossene Systeme - so, wie Sie es sagten - mit besonderem Schutz. Insofern muss man nicht zu der Einschätzung kommen, dass es, wenn man diese Sicherheitslücke aufkauft oder benutzt, gleich zu massiven Gefahren für die eigenen Behörden oder größere Wirtschaftsunternehmen kommt.

Dr. Constanze Kurz: Dazu müsste man ein bisschen ausholen, aber dafür habe ich hier nicht die Zeit. Es gibt natürlich sehr unterschiedliche Arten von Sicherheitslücken. Sie können z. B. Software

angreifen, die es auf verschiedenen informationstechnischen Systemen verschiedener Betriebssysteme gibt. Dann hätten Sie einen sehr potenten Trojaner, der über verschiedene Betriebssysteme hinweg funktioniert.

Üblicherweise dockt man aber beim Betriebssystem oder aber bei den Browsern an, die auf sehr vielen Geräten installiert sind. Die Problematik besteht aus meiner Sicht vor allen Dingen darin, dass Sie, wenn Sie die teure Spionagesoftware kaufen, kein Interesse daran haben, diese Sicherheitslücke zu verraten, sondern Sie müssen ein Interesse daran haben, dass die Sicherheitslücke geöffnet bleibt. Das betrifft leider dieselben Geräte, die auch in der Wirtschaft, in den Behörden und bei Privatpersonen benutzt werden - da Sie nicht die ganz speziellen teuren Trojaner kriegen werden, sondern sozusagen nur den Standard. Mehr Geld wird Niedersachsen nicht ausgeben.

Abg. **Sebastian Lechner** (CDU): Diese „normalen“ Trojaner sind aber nicht unbedingt geeignet, um damit bei VW einzudringen. Dort hat man nämlich ganz besondere, spezielle Vorkehrungen, um genau dies abzuwehren. Das war ja mein Punkt. Genauso ist es auch bei den Behörden. Sie hatten vorhin selbst gesagt, dass die Behörden - nicht jede Behörde, aber einige Behörden - besondere Anstrengungen unternehmen, um gerade die üblichen Trojaner, die wir vielleicht benutzen würden, um an Handys heranzukommen, nicht auf ihre Informationssysteme zugreifen zu lassen. Da gibt es ja auch unterschiedliche Schutzniveaus, die kein normaler Bürger auf seinem Handy realisieren kann usw. Hier greift auch wieder das Kostenargument.

Dr. Constanze Kurz: Dem würde ich tendenziell zustimmen. Ich komme aber aus Berlin, wo es einen Bundestags-Hack gab. Ich hoffe, das hat zur Sensibilisierung beigetragen. Auch staatliche Behörden sind - was ich für einen großen Fehler halte - nach wie vor oft Microsoft-Nutzer und damit in einem hohen Maß betroffen.

Abg. **Bernd Lynack** (SPD): Die Hinweise zu den medizinischen Geräten, Autos etc. und Ihren Blick in die Zukunft finde ich sehr spannend. Wir machen das Gesetz nicht für heute und morgen, sondern auch noch für übermorgen. Wäre es aus Ihrer Sicht in Ordnung, wenn wir das auf Computer, Laptops usw. begrenzen und eine Formulierung finden würden, wonach Autos, Fahrzeuge, Implantate usw. davon ausgenommen sind?

Dr. Constanze Kurz: Wie ich vorhin schon sagte: Bei der Quellen-TKÜ halte ich es für durchaus machbar, weil es dort ja ohnehin sehr auf die Kommunikation bezogen ist. Bei der Online-Durchsuchung sehe ich größere Probleme, auch weil Sie als Gesetzgeber eine gewisse Offenheit in der Formulierung und damit eine gewisse Technikoffenheit für die Zukunft behalten wollen.

Ich würde eine Negativliste besser finden als eine Positivliste. Ich glaube, es ist auch jetzt schon zu sehen, dass informationstechnische Geräte konvergieren. Meine Medizinalgeräte sind auch gleichzeitig normale informationstechnische Geräte. Ich glaube, dass viele Techniken konvergieren. Medizinalgeräte sind heute oft auch Kommunikationsgeräte, weil das bequem bzw. „convenient“ ist. Ich glaube, diese Entwicklung wird zunehmen.

Versteifen Sie sich nicht auf die Autos. Natürlich sind auch schon Autos gehackt worden. Aber ich glaube, dass die Autohersteller noch diejenigen sind, die es am besten hinkriegen, sich gegen Schadsoftware zu wehren, weil sie nämlich als Einzige haften müssen. Die Autos sind ein Beispiel, weil ich das für eine besondere Gefahr halte, aber da sehe ich rein praktisch noch die geringsten Probleme.

Ich glaube, eine Negativliste wäre wahrscheinlich sinnvoll. Aber Sie könnten auch immer noch auf das staatliche Hacken verzichten.

Digitalcourage e. V.

Schriftliche Stellungnahme: Vorlage 9 (zu Drs. 18/850)

Anwesend:

- Friedemann Ebelt

- Uli Fouquet

Friedemann Ebelt: Vielen Dank für die Möglichkeit der Stellungnahme und für die sehr umfangreiche Anhörung. Aber ich muss offen und ehrlich sagen: Das reicht uns noch nicht. Denn wir sehen erheblichen Überarbeitungsbedarf. Das ist auch durch die beiden vorangegangenen Stellungnahmen deutlich geworden.

Ich habe noch zwei Anmerkungen zu der Debatte über das Thema Staatstrojaner.

Erstens: Wir alle hinterlassen im Alltag unglaublich viele Datenspuren, ob wir wollen oder nicht. Und wir sehen das an dieser Stelle genauso wie Dr. Kurz: Es muss Expertise her, um die Daten, die ohne Hacking ohnehin schon anfallen, nutzen zu können. Wir würden uns über Studien und eine parlamentarische Debatte an dieser Stelle sehr freuen.

Der zweite Punkt ist der Rechtsschutz bei der sogenannten Online-Durchsuchung. Der Einsatz eines sogenannten Staatstrojaners wäre in der Geschichte der BRD der erste Fall, in dem es eine Durchsuchung gäbe, bei der man nicht die Möglichkeit hätte, ein Protokoll zu führen, Zeugen heranzuziehen oder auch einen Rechtsbeistand hinzuzuziehen. Das sehen wir sehr, sehr kritisch.

Unsere schriftliche Stellungnahme möchte ich hier nicht wiederholen, die Zeit ist knapp. Aber grundsätzlich stellt sich für mich die Situation folgendermaßen dar: Ich konnte ca. 150 Seiten vorwiegend sehr kritischer Stellungnahmen lesen mit mehr als 200 Kritikpunkten, Ergänzungen, Fragen und Hinweisen auf Klarstellungsbedarf. Das waren noch nicht einmal alle Stellungnahmen. Seit gestern gibt es auch noch eine Stellungnahme des Vereins Hannover IT. Vor diesem Hintergrund schlage ich vor bzw. ich würde es gern mit Nachdruck einfordern, dass die Landesregierung diese Punkte aus den schriftlichen Stellungnahmen schriftlich zusammenfasst, eine Synopse erstellt und darauf öffentlich antwortet. Die Punkte sind sehr breit gefächert, sie müssen und können zusammengefasst werden. Wir erachten das für absolut notwendig, allein aus der Sorgfaltspflicht heraus, die sich mit Blick auf die Grundrechte ergibt, die hier betroffen sind. Das sind die Grundrechte Freiheit und Sicherheit und peripher auch noch andere. Das ist ein Punkt, den ich nicht stark genug betonen kann. Wir wünschen uns das und glauben, dass das absolut angemessen ist.

Ich möchte unsere Grundhaltung zum gesamten Gesetzentwurf einmal zum Ausdruck bringen. Wir halten den Gesetzentwurf aus den vielen, bereits genannten Gründen für nicht verhältnismäßig. Es gibt mildere Maßnahmen, die nicht in dem Umfang diskutiert wurden wie die schärferen Maßnahmen. Wir sehen große Probleme bezüglich der Normenklarheit. Das hat Herr Dr. Held beispielsweise mit Blick auf die Videoüberwachung ausgeführt. Die Verhältnismäßigkeit bezieht sich u. a. auf die sehr gute Sicherheitslage im Lande. Da muss man auch einmal sagen: Die Polizei macht im Großen und Ganzen - obwohl es auch berechtigte Kritik gibt - eine sehr gute Arbeit im Land. Niedersachsen ist ein sicheres Bundesland. Das ist eine Sache, die man vielleicht auch einmal zurückmelden muss. Wir stehen nicht an der Schwelle einer großen Unsicherheit.

Sicherheit ist der Dreh- und Angelpunkt. Darum geht es bei der Gesetzesreform. Wir sehen Unsicherheitsfaktoren und haben auch Bedenken, ob die Reform wirklich die Wirkung in Bezug auf mehr Sicherheit hat, die vom Gesetzgeber erwünscht ist.

Der erste Punkt dabei ist: Viele Stellungnahmen kritisieren und bezweifeln die Wirksamkeit der Maßnahmen. Das betrifft die Videoüberwachung, den Einsatz von Staatstrojanern - dort wird sogar von Gefahrenpotenzial gesprochen -, die Fußfessel und andere Maßnahmen. Das muss ich nicht weiter ausführen. Wie gesagt, wir wünschen uns eine schriftliche Zusammenfassung und eine Neubewertung nach dieser Anhörung.

Zweiter Punkt zum Thema Sicherheit: Obwohl es in der Begründung des Gesetzentwurfs sehr stark betont wird, legen die Maßnahmen eben keinen zugespitzten Fokus auf Terrorismus und organisierte Kriminalität, sondern es geht durch die weiten Straftatbestände um Alltagskriminalität. Wir wissen, wen das betreffen wird: Fußballfans und gegebenenfalls auch politische Aktivistinnen und Aktivisten. Insofern verfehlt die Gesetzesreform in Punkten ihr Ziel.

Der nächste Punkt ist: Nach unserer Einschätzung entstehen durch den Fokus der geplanten Gesetzesreform sogar gravierende Lücken. Der Leiter der Kriminalpolizei Braunschweig, Ulf Küch, hat betont, dass die Polizei ein Kapazitätsproblem hat. In Braunschweig ist es wohl so, dass in den nächsten Jahren ein Drittel der Polizeibeamtinnen und -beamten in den Ruhestand geht. Und die Frage nach Ersatz und Aufstockung des Personals ist nicht gelöst und nicht adressiert. Während wir die ganze Zeit über staatliches Hacking usw. diskutieren, verpassen wir es, uns gerade um diese Stellschrauben zu kümmern.

Eine weitere gravierende Lücke: Die Gesetzesreform adressiert zwei sehr wichtige Punkte in der jüngsten Vergangenheit der Sicherheitsdebatte in der Bundesrepublik nicht. Das eine ist der NSU-Komplex. Wir hatten es dabei mit Aktenvernichtung, Verhinderung von Aufklärung und der Involvierung des Bundesamtes für Verfassungsschutz

in NSU-Tätigkeiten zu tun. Der andere Fall ist Anis Amri. Man kann nicht behaupten, dass Anis Amri zu wenig oder ungenügend überwacht wurde. Sondern auch in diesem Fall gab es, soweit bisher bekannt - die Untersuchungen sind ja noch nicht abgeschlossen -, eher Probleme beim Nachgehen der Indizien. Bevor man den Fall Amri in die Gesetzesbegründung aufnimmt, muss man aus unserer Sicht die Untersuchungsergebnisse abwarten.

Hinzu kommt, dass die Ursachenbehebung, also die klassische Präventionsarbeit, aus dem Fokus des Gesetzentwurfs herausrutscht. Wir sehen eine Verschiebung des Begriffs. So wie ich die Polizeiarbeit kennengelernt habe, auch damals in der Schule, geht es darum, Menschen aufzuklären und dafür Sorge zu tragen, dass Menschen Wissen erlangen. Jetzt wird ein anderer Präventionsbegriff eingeführt, und es geht eher um eine Art Vermutungspolizeiarbeit. Das sehen wir grundsätzlich sehr kritisch.

Ein letzter Punkt zum Thema Unsicherheitsfaktoren sind die angesprochenen sogenannten Staatstrojaner, deren Anwendung aus den genannten Gründen sehr schnell aus dem Ruder laufen kann. An dieser Stelle ist die Verhältnismäßigkeit gegenüber der Betroffenheit von potenziell allen Menschen, die Kommunikationsgeräte und andere technische Geräte nutzen, zu betrachten.

Unter dem Strich ist für uns die Abwägung der geplanten Maßnahmen noch nicht abgeschlossen, weshalb wir um diese schriftliche Zusammenfassung bitten. Wir stellen uns zu diesem Gesetzentwurf weitere Fragen, die aus unserer Sicht dringend behandelt werden müssen.

Uli Fouquet: Uns ist beim Sichten dieses Gesetzentwurfs der Hauch dieses Zeitgeistes, den Frau Kurz erwähnt hatte, nicht verborgen geblieben. Wir machen uns hauptsächlich deswegen Sorgen. Als wir den Gesetzentwurf durchgearbeitet haben, haben sich uns viele Fragen gestellt, von denen wir einige aufgeschrieben haben. Sie stehen exemplarisch für die Probleme, die wir im Moment mit dem Gesetzentwurf haben.

Eine Frage lautet etwa: Warum geht die Reform des Polizeigesetzes, ein großer juristischer Akt, auf die bekannten Probleme der Polizei wie Überstunden, Aktenberge, Verfahrensstau etc. so wenig ein? Dazu haben wir im Gesetzentwurf bisher wenig gefunden.

Wir haben ganz gravierende Probleme mit dem Staatstrojaner. Das wurde bereits ausführlich gewürdigt. Aber ein Problem möchte ich noch einmal ansprechen. Ich habe mir auch den zweiten Teil der Anhörung am vergangenen Freitag angehört, und es gibt da eine Unterscheidung, von der ich mir nicht sicher bin, ob sie bei allen Abgeordneten angekommen ist. Sie definieren im Gesetzentwurf zwei Staatstrojaner, quasi den großen und den kleinen. Im Angriffssektor unterscheiden sie sich zunächst - Frau Kurz hat das wunderbar und technisch sehr korrekt erklärt - kaum. Sie tun zunächst dasselbe mit dem Gerät, sie installieren eine Software und tun dann Dinge. Welche Dinge das sind, ist im Gesetzentwurf überhaupt gar nicht geregelt. Wie wird es kontrolliert, wie wird es evaluiert, wie wird es im Nachhinein betrachtet? - Darüber wissen wir nichts. Schon der kleine Staatstrojaner, die Quellen-TKÜ, die nur eine ganz geringe Schwelle hat - sie kann bereits von der Polizei ohne richterliche Anordnung veranlasst werden -, hat das Potenzial, großen Schaden auf Geräten anzurichten. Wir wissen nicht, was die Software dort macht. Wir haben keinen Quellcode, wir haben noch nicht einmal eine parlamentarische Überprüfung, in deren Rahmen die Parlamentarier letztlich gebeten würden: Guckt einmal drüber, ob das so okay ist. - Das macht uns große Sorgen.

Dieser kleine Staatstrojaner, die Quellen-TKÜ, kann das Gleiche wie der große, man hat nur eine freiwillige Selbstverpflichtung unterschrieben, dass er das nicht ausschöpft. Das ist, technisch gesehen, der einzige Unterschied. Und wenn man nun den gesamten Inhalt eines Handys abspeichert, dann tut man das eben. Das ist zwar nicht legal, aber es gibt im Gesetzentwurf keinen Hebel, um die Schadsoftware bzw. die Stellen, die sie einsetzen, daran zu hindern. Das ist für uns ein erheblicher Mangel, der vielleicht einfach aus Unkenntnis über die technische Ähnlichkeit resultiert.

Wir haben ein wenig das Gefühl - das ist ein Grund, warum uns die Lektüre des Gesetzentwurfs nicht zur reinen Freude gediehen ist -, dass der Zeitgeist ein großes Problem ist und dass viele Ansätze, die es früher gab, in ihr Gegenteil verkehrt werden. Prävention heißt jetzt Überwachung, und viele Maßnahmen, die früher als milde Mittel gedacht waren, werden anders angewandt. Beispielsweise sollte früher über die elektronische Fußfessel eine Haftverschonung gewährleistet werden, und jetzt soll sie im Vorfeld einer Straftat, bei einem bloßen Verdacht, auf polizeiliche An-

ordnung eingesetzt werden, weil eine Haft nicht möglich ist. Wir haben mindestens vier verschiedene Formen dieser Verkehrung in diesem Gesetzentwurf entdeckt, die uns große Sorgen bereiten.

Das ist neben dem Staatstrojaner der andere große Bereich, bei dem wir uns fragen: Warum muss das so sein? Ist das wirklich der Zeitgeist nach dem Motto „Wir müssen jetzt einmal mit harter Hand durchgreifen und etwas gegen die Kriminalität tun, weil der Bürger es erwartet“? Ich fühle mich in Niedersachsen sehr sicher, und ich finde auch, dass die Polizei gute Arbeit macht. Ich kann die Notwendigkeit so nicht erkennen.

Vors. Abg. **Thomas Adasch** (CDU): Vielen Dank für Ihre Ausführungen. Ich habe noch einen kurzen Hinweis: Der Gesetzentwurf kommt nicht von der Landesregierung, sondern von den Koalitionsfraktionen. Der Innenausschuss wird als federführender Ausschuss im Rahmen des weiteren Verfahrens darüber beraten, wie er mit diesem Gesetzentwurf und mit dieser Anhörung umgehen wird. Er wird der Landesregierung keine Anweisung erteilen, irgendetwas zusammenfassen.

Bündnis #noNPOG - Nein zum neuen niedersächsischen Polizeigesetz

***Anwesend**:*

- Juana Zimmermann

- Thomas Ganskow

Juana Zimmermann: Zunächst möchte ich mich im Namen des Bündnisses bedanken, dass wir zu dieser Anhörung eingeladen worden sind, das ist keine Selbstverständlichkeit, wie wir am Vorgehen anderer Landesinnenausschüsse sehen konnten. Unsere Freude hält sich aber in Grenzen, denn lieber hätten wir, dass es keine Anhörung gebe, weil es keinen Gesetzentwurf gibt.

Ich bin die Sprecherin des Bündnisses „#noNPOG - Nein zum neuen niedersächsischen Polizeigesetz“. Wir sind ein breites Bündnis aus der Gesellschaft, d. h. wir setzen uns zusammen aus Gewerkschaften, Jugendorganisationen von Parteien wie die Jusos, Migrantenorganisationen, Gruppen aus der Flüchtlingshilfe, Vertreterinnen und Vertreter der Jurisprudenz etc. Wenn wir auch nicht immer einer Meinung sind, uns alle eint die strikte Ablehnung dieses Gesetzentwurfs, und wir fordern dazu auf, diesen Gesetzentwurf nicht zu verabschieden.

Wir sind am dritten Tag dieser Anhörung. Ich muss die bereits geäußerte Kritik nicht weiter ausführen. Wir schließen uns den Stellungnahmen von freiheitsfoo und Digitalcourage, die auch Teil unseres Bündnisses sind, an. Wir sind heute hier, um deutlich zu machen, dass das Inkrafttreten dieses Gesetzentwurfs alle Menschen in Niedersachsen betreffen würde. Ich möchte Ihnen die zivilgesellschaftlichen Folgen deutlich machen. Wenn dieser Gesetzentwurf verabschiedet werden sollte, würde die Polizei in Zukunft, ohne dass eine Straftat vollzogen wurde, Menschen ausspähen, überwachen, verfolgen und in Gewahrsam nehmen dürfen, und zwar bereits schon, wenn sie vermutet, dass diese Menschen eine Straftat begehen könnten. Damit ändert sich die Rolle der Polizei grundsätzlich. Es ist eine Verwischung der Grenzen der Gewaltenteilung, wenn die Exekutive mehr Befugnisse bekommt, ohne dass wir eine Kontrolle durch die Judikative haben. Dann ist die Gewaltenteilung aufgelöst. Ich denke, das ist ein grundsätzliches Infragestellen unseres Rechtssystems. Ich möchte Ihnen dies an einigen Beispielen verdeutlichen, die uns als Bündnis besonders kritisch erscheinen.

1. Fehlender Richterinnen- und Richtervorbehalt bei Regelungen zu Meldeauflagen, Kontaktverboten, Aufenthaltsvorgaben, Fußfesseln etc.

Wir konnten bei dem Mordfall in Nordfrankreich vor zwei Jahren sehen, dass solche Maßnahmen nicht die Wirkung haben, die man sich vielleicht erhofft. Zudem stehen sie nicht unter Richterinnen- und Richtervorbehalt, sodass hier aufs Massivste in die Grundrechte der Menschen eingegriffen wird.

2. Freiheitsentzug bis zu 74 Tagen

Bei Nichtbefolgung eben genannter Anordnungen bzw. wenn die Polizei die bevorstehende Begehung einer sogenannten terroristischen Straftat sieht, sind diese, immer noch als unschuldig zu betrachtenden Menschen - zwar mit richterlicher Bestätigung, aber dennoch - lediglich unter der Begründung einer hohen abstrakten Gefährdungslage aufgrund der Unterstellung einer gemeinwohlgefährdenden Gesinnung bis zu 74 Tage in Präventivgewahrsam zu nehmen. Zu Straftaten des Terrorismus zählen nach diesem neuen Katalog bereits einfache Körperverletzungen mit

vor Tatbegehung bereits prognostizierten bleibenden Schäden. Wir bleiben also die ganze Zeit in einem vagen Bereich von Vermutungen und Prognosen.

Auch wenn die zuständige Ministerin laut ihrer bisherigen Einlassungen davon ausgeht, dass dieses Instrument nur selten zum Einsatz käme, so sehen wir doch, dass jeder einzelne Fall ein Skandal wäre. Denn wenn man jemanden bis zu 74 Tage in Gewahrsam nimmt, kann man davon ausgehen, dass der Arbeitsplatz der betroffenen Person weg ist, dass die Wohnung unter Umständen gekündigt ist und dass dieser Makel, dass man als vermeintlicher Terrorist in Gewahrsam genommen worden ist, nur nach unglaublich großen Bemühungen wieder loszuwerden ist, auch wenn der Verdacht unbegründet war. Die Folgen dieser präventiven Maßnahmen sind für den Einzelnen, für das Individuum, für jeden Menschen einfach unbegreiflich.

3. Unverhältnismäßige Grundrechtseingriffe

Diese Maßnahmen, die sich auf vage Mutmaßungen stützen, sehen wir nach unserem Verständnis von Verfassung und Grundrechten als unverhältnismäßig an. Sie verletzen rechtsstaatliche Prinzipien, wie auch schon Constanze Kurz anmerkte: Privatsphäre und Persönlichkeitsrechte der Betroffenen, die ja letztlich unschuldig sind. Denn solange sie nicht verurteilt sind, gilt für sie die Unschuldsvermutung. Sie wird durch solche Maßnahmen de facto aufgehoben.

4. Vergeheimdienstlichung der Polizei

Die Polizei soll aufgrund von nicht definierten Gefahrenprognosen für die zukünftige Begehung von Straftaten die Telekommunikation Unschuldiger sowie die ihrer Kontaktpersonen überwachen, Computersysteme mittels des Niedersachsentrojaners hacken und ausspähen, observieren, Aktivitäten in Bild und Ton festhalten, aufzeichnen und speichern. Unschuldige sollen unter zweifelhaften Eingriffsbefugnissen durch verdeckte Ermittlerinnen und Ermittler bespitzelt werden dürfen. Letztlich können die Sicherheitslücken, die Sie ausnutzen, auch Sie und Ihre Familien betreffen. Wir sehen es als Aufgabe des Staates, die Bürgerinnen und Bürger, die Menschen in Niedersachsen zu schützen und solche Sicherheitslücken nicht auszunutzen. Letztlich machen Sie sich damit selbst zu Cyberkriminellen.

Vors. Abg. **Thomas Adasch** (CDU): Entschuldigung, aber dass Sie uns hier zu Kriminellen machen, geht ein wenig zu weit. Ich bitte Sie, das zurückzunehmen.

Juana Zimmermann: Ich nehme das zurück und sage, Sie verhalten sich ähnlich.

Vors. Abg. **Thomas Adasch** (CDU): Auch das akzeptiere ich nicht. Ich darf Sie bitten, solche Einlassungen zu unterlassen, sonst muss ich die Anhörung abbrechen. Das nimmt eine Form an, die ich nicht tolerieren kann.

Juana Zimmermann: Okay.

5. Bei Demo unter Generalverdacht

Der Straftatbestand des besonders schweren Falls des Landfriedensbruchs, der schon jetzt häufig bei Demonstrationen als Joker zur harten Strafverfolgung gezogen wird, wird zur Straftat von erheblicher Bedeutung. Damit verbunden wird auch die Befugnis der Polizei zur Observation von Demonstrierenden. Damit wird die Erlaubnis erlassen, dass bereits im Vorfeld Aktivitäten ausgespäht werden können. Es kann zu einer Verhinderung der Teilnahme an der Versammlung kommen, indem die betroffene Person in Gewahrsam genommen wird. Das konnten wir jetzt auch schon in Bayern im Vorfeld der Demonstration zum AfD-Parteitag in Augsburg sehen. Auch die angedachte Veränderung, dass Vermummung als ein Straftatbestand statt einer Ordnungswidrigkeit aufgenommen werden soll, sehen wir als sehr kritisch an. Denn letztlich würde schon der Schal im Winter und das Basecap und die Sonnenbrille im Sommer unter Umständen darunter fallen. Damit werden eine Einschränkung und eine Kriminalisierung der Demonstrierenden für uns deutlich.

6. Die Bevölkerung als Sicherheitsrisiko

Die künftige Anfertigung und Speicherung der polizeilichen Bild- und Tonaufzeichnungen in öffentlichen oder öffentlich zugänglichen Räumen bei bloßer Annahme von zukünftigen Begehungen von Ordnungswidrigkeiten oder Straftaten unterstellt letztlich der breiten Bevölkerung, dass jeder jederzeit straffällig werden könnte. Das ist ein Generalverdacht gegen jeden, der sich im öffentlichen oder öffentlich zugänglichen Raum aufhält. Letztlich ist das eine Aushebelung der Unschuldsvermutung, und das ist eine Entwicklung, die wir ablehnen. Wir stellen die Verhältnismäßigkeit infrage, und wir stellen infrage, ob der Nutzen, den

wir als Gesellschaft daraus gewinnen, wirklich so groß ist, dass wir dies so ausführen wollen.

7. Elektroschocker im Einsatz

Geplant ist, dass der Einsatz von Elektroimpulsgeräten in der Reihenfolge der Mittel zur Ausübung des unmittelbaren Zwangs vor dem Einsatz des Schlagstockes aufgenommen werden soll. Wir sehen keine Notwendigkeit bzw. zwingende Gründe, warum das so sein sollte. Wir leben, wie gesagt, in einem sicheren Land. Demonstrationen verlaufen in der Regel friedlich. Deshalb lehnen wir auch das ab.

Zum Gesetzentwurf allgemein

Wenn Sie tatsächlich etwas zum Wohl der Bürger tun möchten, sollten Sie anderweitig ansetzen. Es ist letztlich nicht die Aufgabe der Polizei, den Rechtsstaat und die Bürgerrechte einzuschränken und zu beschneiden, sondern diese Rechte zu schützen und zu garantieren. Mit diesem Gesetzentwurf wird eine grundsätzliche Richtung eingeschlagen, die unter Umständen nicht abschätzbare Folgen haben wird. Die Frage ist: Werden wir die Geister, die wir damit rufen, im Zaum halten können? Wir konnten in Österreich sehen, dass mit dem Erstarken der FPÖ, die auch in der Regierung ist, die Instrumente der Polizei bereits zweckentfremdet wurden. Wir sind uns nicht sicher, ob dies nicht auch hier passieren könnte. Wir sehen grundsätzliche Einschnitte in das Leben aller Menschen, nicht nur in das potenzieller Straftäter. Denn was ist, wenn man unschuldig in das Fadenkreuz der Ermittler kommt und die Ermittler alle ihnen rechtlich gegebenen Instrumente nutzen? - Die Folgen wären unbegreiflich. Letztlich ist es schon schlimm, wenn man unbegründet nicht zur Demo gehen kann, um sich gegen seinen Arbeitgeber zur Wehr zu setzen, oder nicht ins Fußballstadion gehen kann. Das sind alles Einschränkungen. Wir werden unserer Grundrechte beraubt.

Wir hoffen, dass wir Ihnen mithilfe dieser Beispiele deutlich machen konnten, dass Sie mit diesem Gesetzentwurf die Rechte aller Menschen in Niedersachsen einschränken, und wir zu einer argumentgeleiteten Debatte kommen. Wir glauben, dass die Polizei nicht mehr Rechte braucht, sondern gut ausgebildetes, qualifiziertes Personal.

Abg. **Dunja Kreiser** (SPD): Gerade, was das Thema Taser anbelangt: Es wäre sinnvoll, den Gesetzentwurf richtig zu lesen, dann wüssten Sie auch, wofür er eingesetzt wird.

Thomas Ganskow: Beim Taser gibt es ja noch ein ganz bestimmtes anderes Problem. In den USA gab es entsprechende Untersuchungen, laut denen dadurch Todesfälle verursacht worden sind. Insofern muss überlegt werden, in welchen Fällen ein Taser tatsächlich eingesetzt werden kann. Das ist ein wesentlich schärferes Mittel, um unmittelbare Gewalt auszuüben, als beispielsweise ein Schlagstock. Selbst ein Schuss ins Bein ist letztlich weniger gefährlich als der Einsatz eines Tasers.

Abg. **Karsten Becker** (SPD): Es ist ja eigentlich nicht die Aufgabe eines Abgeordneten, im Rahmen einer Anhörung eine Stellungnahme abzugeben. Das möchte ich eigentlich auch nicht tun, aber eines möchte ich dennoch sagen: Es hilft, sich mit den Inhalten eines Gesetzentwurfs zu beschäftigen, wenn man dazu Stellung nimmt. Ich möchte das am Thema Taser deutlich machen.

Erstens: Der Gesetzentwurf deklariert den Taser als Waffe und ordnet ihn damit deutlich ein im Hinblick auf die Abwägung, wann er eingesetzt werden darf, nämlich in Relation zu den Einsatzbedingungen für eine Schusswaffe und nicht zu denen eines Schlagstockes oder eines Reizstoffsprühgeräts.

Zweitens: In Niedersachsen ist der Einsatz des Tasers eindeutig geregelt. Er ist ausschließlich Spezialeinsatzkommandos vorbehalten und sonst niemandem. Daran wird sich auch überhaupt nichts ändern.

Das ist ein schönes Beispiel dafür, dass das, was Sie teilweise vorgetragen haben, mit der Realität dieses Gesetzentwurfs überhaupt gar nichts zu tun hat. Gestatten Sie mir, dass ich das als kurze Erwiderung zurückgebe.

Abg. **Jens Ahrends** (AfD): Sie sprachen von Todesfällen im Zusammenhang mit dem Einsatz von Tasern. Es gibt eine Erhebung - ebenfalls aus den USA -, nach der bei 1 000 Einsätzen des Tasers lediglich drei Menschen zur medizinischen Versorgung ins Krankenhaus mussten. Bei dieser Untersuchung wurden gar keine Todesfälle festgestellt. Ich bin sicher, dass bei tausendfachem Einsatz einer Schusswaffe wesentlich mehr Verletzungen entstanden wären.

Weiteres Verfahren

Die **Ausschussmitglieder** kamen mit Blick auf die weitere Beratung überein, sie im Sinne eines effizienten Vorgehens schrittweise fortzusetzen, sobald beratungsreife Vorlagen zu Teilkomplexen des Gesetzentwurfs übermittelt worden sind.

***

Tagesordnungspunkt 2:

Beschlussfassung über Anträge auf Unterrichtung durch die Landesregierung

a) **Unterrichtung über eine Konzeption des Landeskriminalamtes zur Aufarbeitung sogenannter „cold cases“**

Der **Ausschuss** beschloss einstimmig, dem Unterrichtungswunsch zu entsprechen, und bat die Landesregierung um eine mündliche Unterrichtung in einer der nächsten Sitzungen.

b) **Ergänzende Unterrichtung über die Bedrohung von Bürgern in Eschede durch einen Asylbewerber aus dem Sudan**

Der **Ausschuss** beschloss einstimmig, dem Unterrichtungswunsch zu entsprechen, und bat die Landesregierung um eine mündliche Unterrichtung. Die Unterrichtung soll in einem vertraulichen Sitzungsteil entgegengenommen werden. Zudem beschloss der Ausschuss auf Antrag der AfD-Fraktion, dass Abg. Stephan Bothe (AfD) gemäß § 94 Abs. 2 GO LT mit beratender Stimmung zu diesem Sitzungsteil hinzugezogen werden soll.

***

Tagesordnungspunkt 3:

Aktenvorlage gemäß Artikel 24 Abs. 2 der Niedersächsischen Verfassung betreffend den Aufenthalt des ehemaligen Vorsitzenden der Justiz im Iran Ayatollah Shahroudi in Hannover (2. Tranche)

Der **Ausschuss** beschloss gemäß § 95 a GO LT die Vertraulichkeit der mit Schreiben des Niedersächsischen Ministeriums für Inneres und Sport vom 3. Juli 2018 vorgelegten Unterlagen.

***

Tagesordnungspunkt 4:

a) **Zivilbevölkerung in Syrien schützen - niedersächsischer Verantwortung gerecht werden!**

Antrag der Fraktion Bündnis 90/Die Grünen - Drs. 18/830

b) **Familiennachzug dauerhaft aussetzen**

Antrag der Fraktion der AfD - Drs. 18/843

Zu a) erste Beratung: 15. Plenarsitzung am 17.05.2018
federführend: AfluS
mitberatend gem. § 27 Abs. 4 Satz 1 i. V. m. § 39 Abs. 3 Satz 1 GO LT: AfHuF

Zu b) erste Beratung: 15. Plenarsitzung am 17.05.2018
AfluS

Der **Ausschuss** setzte diesen Punkt von der Tagesordnung ab.

***

Tagesordnungspunkt 5:

Altersfeststellung bei jugendlichen Flüchtlingen

Antrag der Fraktion der FDP - Drs. 18/1064

direkt überwiesen am 14.06.2018
federführend: AfluS
mitberatend gem. § 27 Abs. 4 Satz 1 i. V. m. § 39 Abs. 2 Satz 2 GO LT: AfHuF

Beginn der Beratung

Abg. **Jan-Christoph Oetjen** (FDP) stellte die Grundzüge des Antrages kurz vor und erinnerte daran, dass der Innenausschuss im Rahmen der Beratung des Antrages der AfD-Fraktion zu diesem Thema bereits gemeinsam mit dem Sozialausschuss über Möglichkeiten zur medizinischen Altersfeststellung unterrichtet worden sei (7. Sitzung am 8. Februar 2018).

Die FDP-Fraktion sehe die Notwendigkeit eines bundesweit einheitlichen Vorgehens in dieser Frage. Deshalb beinhalte der Antrag die Forderung, eine Bund-Länder-Expertenkommission einzurichten, die eben dies festlege.

Zum weiteren Verfahren schlug der Abgeordnete vor, den Antrag gemeinsam mit dem Antrag der AfD-Fraktion zum gleichen Thema zu beraten.

Abg. **Sebastian Lechner** (CDU) sagte, die Koalitionsfraktionen ständen in regem Austausch zu diesem Thema und würden in absehbarer Zeit zu einem Ergebnis kommen.

Weiteres Verfahren

Der **Ausschuss** verständigte sich darauf, den Antrag gemeinsam mit dem Antrag der AfD-Fraktion „Medizinische Altersfeststellung unbegleiteter minderjähriger Flüchtlinge“ (Drs. 18/147) zu beraten.

***

Tagesordnungspunkt 6:

Testphase zur Einführung einer Elektroschockwaffe (Taser) bei der niedersächsischen Polizei

Antrag der Fraktion der AfD - Drs. 18/1086

erste Beratung: 19. Plenarsitzung am 21.06.2018
AfluS

Erörterung von Verfahrensfragen

Abg. **Jens Ahrends** (AfD) sagte, die AfD-Fraktion verfolge mit dem Antrag das Ziel, eine Testphase für den Einsatz von Tasern im Polizeidienst einzurichten. Er schlug vor, eine Anhörung durchzuführen, damit sich der Ausschuss ein Bild davon machen könne, welche Erfahrungen in anderen Bundesländern wie etwa Rheinland-Pfalz und Bremen mit dem Einsatz von Tasern gemacht worden seien.

Abg. **Bernd Lynack** (SPD) wies darauf hin, dass das Thema Einsatz von Tasern auch eine große Rolle im Rahmen der Anhörung zur Novelle des Nds. SOG gespielt habe. Er schlug vor, den Antrag in die Beratungen dazu einfließen zu lassen. Weiter regte er an, alternativ zu einer Anhörung zunächst die Landesregierung um eine Unterrichtung zu bitten, da diese voraussichtlich über Kenntnisse zu Erfahrungen in anderen Bundesländern verfüge.

Abg. **Jens Ahrends** (AfD) zeigte sich mit den Vorschlägen einverstanden und merkte an, dass der Antrag ohnehin obsolet werde, sollte der Einsatz von Tasern im Polizeidienst Eingang in die Novelle des Nds. SOG finden.

*

Der **Ausschuss** verständigte sich darauf, den Antrag in die Beratung zum Entwurf eines Reformgesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze (Drs. 18/850) miteinfließen zu lassen. Zudem bat er die Landesregierung, in diesem Rahmen darüber zu unterrichten, welche Erfahrungen mit dem Einsatz von Tasern in anderen Bundesländern gemacht worden sind.

***

Tagesordnungspunkt 7:

Beleidigungen, Drohungen, Hass und Gewalt gegen kommunale Amts- und Mandatsträger, Rettungskräfte und Ehrenamtliche sind nicht hinnehmbar - Land und Kommunen müssen gemeinsam aktiv werden

Antrag der Fraktion der SPD und der Fraktion der CDU - Drs. 18/1175 neu

direkt überwiesen am 26.06.2018
AfluS

Beginn der Beratung

Abg. **Uwe Schünemann** (CDU) stellte die Grundzüge des Antrages kurz dar und schlug vor, eine Anhörung vorzusehen und von diesem Thema Betroffene zu hören.

*

Der **Ausschuss** folgte dem Vorschlag und beschloss, eine Anhörung durchzuführen. Die Fraktionen wurden gebeten, bis zum 22. August 2018 den Kreis der Anzuhörenden zu benennen.

***