Missing Link: Eingefleischte Geheimniskrämer gegen moderne Geheimdienstaufsicht

Originalartikel

Backup

<html> <p class=„printversionback-to-article printversion–hide“>zurück zum Artikel <figure class=„printversionlogo“></figure><figure class=„aufmacherbild“><figcaption class=„akwa-caption“><p class=„source akwa-captionsource“>(Bild: nitpicker/Shutterstock.com) </figcaption></figure> Deutschland hinkt bei der Aufsicht der Nachrichtendienste hinterher. Wird das Bundesverfassungsgericht dem Gesetzgeber auf die Sprünge helfen? Beim Bundesnachrichtendienst hat man sich nach eigener Aussage gefreut, als die Bundesregierung das Unabhängige Gremium (UGr) 2016 ins BND-Gesetz geschrieben hat. Mit der neuen, zusätzlichen Aufsicht werde endlich deutlich werden, wie weiß die Weste des BND sei. Mit solchen Erwartungen begrüßte der damalige BND-Chef Klaus-Dieter Fritsche die ersten drei richterlichen Teilzeit-Kontrolleure am Bundesgerichtshof in Karlsruhe, berichtete BGH-Richterin Gabriele Cirener, Mitglied des 1. UGr im Verfahren gegen das BND-Gesetz, Mitte Januar dem 1. Senat des Verfassungsgerichts vor wenigen Wochen. <div class=„collapse-boxtarget collapse-boxcontent a-inline-textboxcontent a-inline-textboxcontent–horizontal-layout“ data-collapse-target=„“> <figure class=„a-inline-textboximage-container“></figure> Was fehlt: In der rapiden Technikwelt häufig die Zeit, die vielen News und Hintergründe neu zu sortieren. Am Wochenende wollen wir sie uns nehmen, die Seitenwege abseits des Aktuellen verfolgen, andere Blickwinkel probieren und Zwischentöne hörbar machen. <ul class=„a-inline-textboxlist“><li class=„a-inline-textboxitem“>Mehr zum Feuilleton „Missing Link“ [1] mehr anzeigen Zwei Tage lang

sezierten die Karlsruher Richter die erstmals überhaupt rechtlich gefasste Massenüberwachung ausländischer Datenverkehre. Davor hatte der deutsche Auslandsnachrichtendienst das einfach ohne Rechtsgrundlage, also illegal und praktisch unbeaufsichtigt, gemacht. In der Verhandlung nahmen sich die Richter nicht nur die von der Bundesregierung hartnäckig verteidigte Beschränkung des Grundrechts auf vertrauliche Kommunikation allein auf Deutsche kritisch vor, auch die novellierten Aufsichtsstrukturen stellten sie ganz öffentlich auf den Prüfstand. Vorbereitet hatten sich die obersten Richter mit einem rund 600 Seiten starken Papier, behaupteten Eingeweihte. Das zeigt wohl, dass es rechtlichen Klärungsbedarf gibt. <h3 class=„subheading“ id=„nav_neue0“>Neue Kontrolleure</h3> Das Gremium mit dem unauffälligen Namen UGr soll laut BND-Gesetz stichprobenartig prüfen, ob der Dienst bei der „Ausland-Ausland-Überwachung“ im Rahmen der gesetzlichen Schranken aktiv ist. Werden aus den unter anderem vom deutschen Decix abgelauschten Terabytes die Daten deutscher Bürger ausreichend ausgefiltert? Das UGr kann die Anträge des BND und die daraufhin vom Bundeskanzleramt erlassenen Anordnungen für breitbandig überwachte Telekommunikationstrecken prüfen und versucht, so Cirener, auf die Einhaltung des Kernbereichsschutzes zu achten. Die BGH-Richterin sagte in Karlsruhe, der BND habe die Idee von der richterlichen „Reinwaschung“ inzwischen revidiert. Als sie kürzlich aus dem UGr ausschied, vertraute man ihr an, man habe nach dem Austausch mit den BGH-Richtern eine andere Auffassung von „Genauigkeit“ bekommen. In der Anfangsphase habe man beispielsweise auch darauf gepocht, dass der Geheimdienst Formalien einhält, also etwa ob Anordnungen von Suchbegriffen auch die korrekten Unterschriften tragen. Nicht damit es hinterher wieder keiner gewesen sein will. In der Anfangszeit hat das neue Gremium viel Zeit darauf verwendet, sich selbst eine Geschäftsordnung zu geben und ganz praktische Dinge zu klären. Beispielsweise boten die Räumlichkeiten des BGH in Karlsruhe gar nicht die notwendigen Voraussetzungen für den Umgang mit Verschlusssachen. Zudem mussten sich drei eingesetzten Richter (und die drei Stellvertreter), die für ihre UGr-Aufgaben zu 50 Prozent von ihren klassischen richterlichen Tätigkeiten freigestellt wurden, damit auseinandersetzen, dass das Justizministerium ihre Aufsichtsrolle offenbar als „Ehrenamt“ betrachtete, sagt Cirener. <h3 class=„subheading“ id=„nav_kontrollverzicht1“>Kontrollverzicht, Kinderkrankheiten, böse Briefe</h3> Ungewöhnlich war für die Richterin aber vor allem, „erstmals in einem Bereich zu arbeiten, der keinerlei Kontrolle unterliegt“, sagte Cirener den Verfassungsrichtern. Weder die Öffentlichkeit, noch der Dienstherr oder das Parlament könne wegen der Geheimhaltung nachvollziehen, ob man wirklich gründlich geprüft habe oder vielleicht nur durch „Handauflegen“. Letztlich hänge viel vom Engagement der drei Mitglieder ab. Mehr als solche organisatorische Kinderkrankheiten stellten die eingeschränkten Kompetenzen die Richter vor Herausforderungen. „Wir kontrollieren nicht insgesamt die Arbeit des BND, sondern haben sehr eng umrissene Stichprobenbefugnisse“, berichtete Cirener. Und nicht immer war klar, welche Stichproben die Richter ziehen durften. Bei der Prüfung der BND-internen Nachkontrollen von Kernbereichsschutz und anderen Grenzen in Daten, die der Dienst an andere Nachrichtendienste weitergibt, kann das UGr ohnehin nur auf das schauen, was der BND selbst als problematisch betrachtet hat. Bei einer Prüfung, inwieweit die Bespitzelung eines Berufsgeheimnisträgers außerhalb der EU auch dessen Kollegen innerhalb der EU betroffen habe, bekam Cirener so auch anschließend einen „bösen Brief“ des Amtes. Sie habe damit ihre Kompetenzen überschritten. Die UGr-Mitglieder dürfen nach Ansicht des BND also etwa nicht prüfen, ob ein Anwalt oder Journalist beobachtet wird. Diese Frage steht mit im Zentrum der in Karlsruhe verhandelten Beschwerde. Die Beschwerdeführer sind Journalisten aus verschiedenen Ländern, die von Reporter ohne Grenzen beziehungsweise der französischen Reporters Sans Frontières vertreten werden. Sie fürchten um die eigene Sicherheit, wenn sie anlasslos überwacht und ihre Daten anschließend im

großen Datenaustausches an Dienste in ihren eigenen Ländern übermittelt werden. Für manche, wie die Beschwerdeführerin Khadija Ismayilova, bedeutet das, dass sie für kritische Berichterstattung ins Gefängnis gehen. <h3 class=„subheading“ id=„nav_divide_et2“>Divide et Impera! Kooperieren verboten</h3> Die Schlagkraft der neuen Aufsicht im Angesicht des internationalen Datenmonopolys überzeugt viele Kritiker – auch innerhalb des Bundestages – keineswegs. Zu eingeschränkt ist das UGr in seinen Kontrollmöglichkeiten. Die Gründung des exklusiv für den Bundesnachrichtendienst zuständigen neuen Gremiums hat die Debatte um die Fragmentierung der deutschen Geheimdienstaufsicht noch mal so richtig angeheizt. Auch die Verfassungsrichter hakten nach. „Bedarf es gesetzlicher Maßnahmen gegen die Fragmentierungseffekte?“, wollte Verfassungsrichterin Susanne Baer vom 1. Senat wissen. <div class=„collapse-boxtarget collapse-boxcontent a-inline-textboxcontent a-inline-textboxcontent–horizontal-layout“ data-collapse-target=„“> <figure class=„a-inline-textboximage-container“></figure> Keine News verpassen! Mit unserem täglichen Newsletter erhalten Sie jeden Morgen alle Nachrichten von heise online der vergangenen 24 Stunden. <ul class=„a-inline-textboxlist“><li class=„a-inline-textboxitem“>Newsletter jetzt abonnieren [2] Das UGr ist nämlich zur Geheimhaltung seiner Einsichten verpflichtet, nicht nur gegenüber Öffentlichkeit und Parlament, sondern auch gegenüber den anderen Aufsehern des BND, insbesondere der G10-Kommission. Bei der G10-Kommission muss der BND anfragen, wenn er deutsche Bürger, ausgenommen so genannte „Funktionsträger“ – das sind deutsche Bürger, die für ausländische Firmen arbeiten – abhören will. Auch gegenüber dem Bundesbeauftragten für den Datenschutz, der dafür zuständig ist, die Sammlung, Verarbeitung und Speicherung personenbezogener Daten beim BND und den anderen Diensten zu überwachen, muss man stillhalten. Allein das Parlamentarische Kontrollgremium des Bundestags (PKGr), das einen breiteren Auftrag zur Kontrolle der deutschen Nachrichtendienste – also BND, Militärischer Abschirmdienst (MAD) und Bundesamts für Verfassungsschutz (BfV) – hat, wird zweimal jährlich vom UGr informiert. Die erzwungene Abschottung macht eine arbeitsteilige und effektive gemeinsame Aufsichtsarbeit für das UGr unmöglich und hat den Start der neuen Kontrolleure nicht erleichtert. Dabei hat das Prinzip „Teile und herrsche“ (divide et impera) in der deutschen Geheimdienstaufsicht klar Methode. Zwar vertrat der Vorsitzende des PKGr Armin Schuster (CDU) in Karlsruhe, dass beim PKGr die Fäden zusammenlaufen, sein Vorgänger und PKGr-Kollege André Hahn (Die Linke) will das so aber nicht bestätigen. Das PKGr weiß nicht, was die G10-Kommission auf den Tisch bekommt, und dann gibt es auch noch das Vertrauensgremium, das sich exklusiv um die finanzielle Ausstattung der Dienste kümmert. Als PKGr-Vorsitzender habe Hahn das Teile-und-Herrsche-Prinzip in der Praxis beobachten können. „Dem PKGr sagte man, die finanzielle Ausstattung der Dienste ist nicht eure Zuständigkeit“, so Hahn. Andererseits durfte das Vertrauensgremium auch nicht nachfragen, für welche Projekte die Haushaltstitel denn nun genau vorgesehen sind. Er sei gespannt, so Hahn, was das Verfassungsgericht dazu sage, dass man derart viele Kontrollgremien schaffe, die „eigentlich nicht miteinander sprechen dürfen.“ <h3 class=„subheading“ id=„nav_filter_eingebaut_3“>Filter eingebaut</h3> Zweischneidig ist aus Sicht von Praktikern und Experten auch eine andere Ergänzung der Aufsichtsstruktur: Der im Zug der

Geheimdienstreform 2016 ins PKGr-Gesetz geschriebene Ständige Bevollmächtigte bringt, zusammen mit dem aufgestockten Mitarbeiterstab, mehr Manpower für die parlamentarischen Kontrolleure. Als neues „Hilfsorgan“ managt Arne Schlatmann seit 2017 strukturelle und Adhoc-Kontrollen des aufgestockten 30köpfigen Mitarbeiterstabes des PKGr. Hahn und der Grüne Konstantin von Notz, Vizevorsitzender des PKGr, begrüßen, dass die Parlamentarier – und in Ausnahmefällen auch die Öffentlichkeit – mehr Informationen über die Arbeit und mögliches Versagen der Dienste, wie etwa im Fall des Anschlags am Berliner Breitscheidplatz. Gerade im Zusammenhang mit dem Breitscheidplatz-Bericht [3] hat die Opposition aber schon vor zwei Jahren gewarnt, der neue Bevollmächtigte könnte leicht zum Flaschenhals oder Vorfilter für die parlamentarische Kontrollarbeit werden. In einem geharnischten Sondervotum hatte Hahn etwa geschrieben, dass der Ständige Bevollmächtigte die PKGr-Mitglieder über anstehende Zeugenbefragungen nicht informiert und ihnen damit auch die Möglichkeit genommen worden ist, die Dienste selbst ins Kreuzverhör zu nehmen. Zusammenfassungen der Befragungen habe es nicht gegeben. Eine durch den Ständigen Bevollmächtigten vorgenommene Vorsortierung von Information aber hält Hahn für ein strukturelles Problem. Das PKGr hängt damit am Tropf eines Stabes, über dessen Besetzung es zudem nicht mitentscheiden kann. Denn ein Vorschlagsrecht der Opposition für die Besetzung von Mitarbeiterstellen, beziehungsweise die Möglichkeit, eigene Zuarbeiter für ihre PKGr-Arbeit einzustellen, gibt es nicht. Um effektiv kontrollieren zu können, fordert Hahn die Lockerung des Klagerechtes für die Minderheit im PKGr. Bislang braucht es im neunköpfigen Gremium, in dem vier Oppositionsmitglieder und vier Regierungsmitglieder sitzen, eine Zwei-Drittel-Mehrheit, wenn sie sich gegen unzureichende Auskünfte durch die Bundesregierung wehren will. <h3 class=„subheading“ id=„nav_bnd_schlägt4“>BND schlägt Aufsicht</h3> Als größte Hürde für eine effektive Aufsichtsarbeit beklagten in Karlsruhe die Vertreter praktisch aller Aufsichtsgremien einhellig die Geheimnistuerei des BND, wenn es um die Zusammenarbeit mit fremden Nachrichtendiensten ging. Das UGr, die PKGr, der Bundesbeauftragte für den Datenschutz – unisono teilten alle mit, dass ihre Aufsicht endet, wo der BND darauf verweist, dass es sich um den Datenaustausch oder gemeinsame Aktivitäten mit der NSA, GCHQ oder anderen fremden Schlapphüten geht. Etwas mehr als 50 Prozent der sogenannten Selektoren, der Suchbegriffe, mit denen der BND im Rahmen der strategischen Aufklärung die großen Datenmengen aus den Netzen durchkämmt, liefern ausländische Geheimdienste. Bei deren Stichproben-Prüfung wissen die UGr-Mitglieder laut Cirener nicht, von welchem Dienst die Begriffe stammen. Sie können lediglich prüfen, ob der jeweilige Dienst das Anforderungsformular korrekt ausgefüllt hat und ob Suchbegriffe einen Zusammenhang mit deutschen Grundrechtsträgern vermuten lassen. Kernbereichsschutzentscheidungen etwa für die so abgehörten EU-Bürger obliegen dem fremden Dienst, berichtete Cirener. Einen echten Einblick bekommen die drei Kontrolleure hier kaum und auch die Vereinbarungen, die die deutschen Dienste mit den ausländischen treffen, bekommen sie nicht zu Gesicht. „Die Third-Party-Rule“ – die Zusage des BND gegenüber den fremden Diensten, dass kein Dritter Einblick in die übermittelten Informationen bekomme – „ist das größte Hindernis“, sagte Cirener. „Ich habe einen gesetzlichen Prüfungsauftrag, wenn ich dann Unterlagen nicht bekomme, kann ich den Befund einfach nicht erheben.“ Die Verfassungsrichter in Karlsruhe hakten bei diesem Punkt selbst gleich mehrfach nach. Wie stellen BND und Bundesregierung bitte fest, ob die übermittelten Informationen nicht dazu genutzt werden, um Menschenrechtsverletzungen zu begehen oder gar extralegale Hinrichtungen vorzubereiten? Man habe Gespräche mit sämtlichen Partnern geführt, in denen

man das deutsche Verständnis von rechtsstaatlicher Verwendung dargelegt habe. Abgesehen von generellen Übereinkünften, werden alle übertragenen Datenpakete mit einem „Disclaimer“ versehen. Der BND führt eine eigene Stichprobenanalyse auf Kernbereichs- oder G10-relevante, das heißt Bundesbürger betreffende Vertraulichkeitsverletzungen durch. Bei der standardmäßigen automatisierten Übermittlung stellt das selbst laut BND eine „gewisse Herausforderung“ dar. Letztlich müsse man auf ein „gewisses gegenseitiges Vertrauen“ setzen, argumentierte die Juristin des Bundeskanzleramtes, in dem mittlerweile vier Referate sich mit den Fragen rund um die Dienste befassen. Wenn es Anhaltspunkte dafür gebe, dass vereinbarte Vorgaben von einem Partnerdienst nicht eingehalten würden, bringe man das zur Sprache. „Das kann dazu führen, dass man eine Zusammenarbeit aufkündigt,“ meinte die Vertreterin in Karlsruhe. Doch dafür gibt es keine aus Sicht des Kanzleramtes nennenswerten Beispiele. <h3 class=„subheading“ id=„nav_beschränkte5“>Beschränkte Kontrolle statt totaler Unterwerfung</h3> Die totale Unterwerfung der deutschen Exekutive unter das Geheimhaltungsmandat der ausländischen Partner wirkt unzeitgemäß. Es wird nicht nur von Experten in Frage gestellt, sondern hinkt auch hinter der Praxis in anderen Ländern zurück. Für Norwegens Parliamentary Oversight Committee (EOS), dessen Mitglieder übrigens keine aktiven Parlamentarier sind, ist der Verzicht auf Einsicht in „besonders sensible Daten“ des norwegischen Auslandsgeheimdienstes die Ausnahme, nicht die Regel. Laut gesetzlicher Vorgabe hat das Gremium Zugang zu allen Daten via direktem Zugriff auf die Datenbanken des Dienstes. Es soll lediglich Belange „der nationalen Sicherheit und der Auslandsbeziehungen“ im Auge behalten und seinen Zugang zu klassifizierten Informationen auf das für die eigenen Aufsichtstätigkeit notwendige Maß beschränken, heißt es im Abschnitt acht der Rechtsgrundlage. „Wo möglich, sollen wir den Schutz von Quellen und die Sicherung von Informationen, die aus dem Ausland kamen, berücksichtigen“, wiederholt das EOS im jüngsten Jahresbericht. EOS Committee Chair Svein Grønnern, spezifiziert auf eine Anfrage, dass das Komitee grundsätzlich Zugang zu allen Archiven und Datenbanken, allen Standorten, Einrichtungen und Gebäuden hat. „Bei unangemeldeten Vorortinspektionen hat das Komitee direkten Zugriff auf alle Systeme und Datenbanken der Dienste,“ erklärt Grønnern. Ausnahmen macht man demzufolge lediglich bei der Identität von Quellen sowie besonders sensibler Information, die man von ausländischen Partnern erhalten hat. <figure class=„a-u-inline-right a-inline-image a-u-inline“> <figcaption class=„a-caption“> Vorsitzender der norwegischen Aufsicht EOS (Bild: Ingar Sørensen) </figcaption></figure> Noch engmaschiger soll die Aufsicht für geplante neue Befugnisse des norwegischen Auslandsgeheimdienstes aussehen, die gerade vom Gesetzgeber vorbereitet werden. Den massenhaften Abgriff digitaler Datenströme, euphemistisch die „digitale Grenzkontrolle“ genannt, wollen die Norweger mit einer „erweiterten Aufsicht“ und einer, so wörtlich, „near real-time“ Kontrolle erweitern. Der Direktzugriff, den man seit den späten 90er Jahren langsam ausgebaut hat, wird so fortentwickelt. Auch die niederländischen Kollegen vom unabhängigen Review Committee of the Security Services (CTIVD) – wie in Norwegen eine Querschnittaufsicht für alle Dienste – berichten in ihrem Jahresbericht [4], dass der direkte Systemzugang

dabei hilft, den Ablauf ganzer Operationen von gewonnenen Informationen bis zu Entscheidungsprozessen zu prüfen. <h3 class=„subheading“ id=„nav_eu_statt6“>EU-statt US-Standards bei der Geheimdienstaufsicht</h3> Norweger und Niederländer gehören überdies zu einer Gruppe von Aufsichtsgremien, die offensiver als die Deutschen über den Clash von internationalem Datentransfers und national begrenzter Aufsicht sprechen. Die „Intelligence Oversight Group“, in der neben CTIVD und EOS auch die Geheimdienstkontrolleure aus Belgien, Dänemark, Großbritannien und der Schweiz vertreten sind, treffen sich seit 2015 regelmäßig und haben 2019 eine eigene Satzung [5] verabschiedet. Die Aufsichtslücke beim Datenmonopoly der Dienste ist ein Dauerbrennerthema der Aufseher. „Wenn ein norwegischer Dienst Informationen mit einem ausländischen Partner teilt, können wir zwar alles sehen, was bei unserem Dienst vor sich geht, aber die Aufsicht endet, sobald die Daten ins Ausland geschickt werden“, schreiben die EOS-Vertreter in einer ihrer Pressemitteilungen über die Arbeit der Intelligence Oversight Group an. Das CTIVD bereitet zum Austausch nicht-evaluierter Daten [6], über die auch das Bundesverfassungsgericht mehr erfahren wollte in der Verhandlung im Januar, gerade einen ausführlichen Prüfbericht vor. <figure class=„a-inline-image a-u-inline“> <figcaption class=„a-caption“> Zwei Tage lang verhandelt der 1. Senat des BVerfG zur Beschwerde gegen das BND-Gesetz </figcaption></figure> Mehr Zusammenarbeit bei der Aufsicht, Austausch über die eigenen Praktiken und die Suche nach Verbesserungen gehören zu den erklärten Zielen der Intelligence Oversight Group. Man trifft sich auf Sachbearbeiter- sowie auf Ebene der Vorsitzenden. Die deutsche Aufsicht glänzt hier bislang durch Abwesenheit, wohl auch wegen der harschen Auflagen bezüglich Geheimhaltung. Von Innovationen bei der Kontrolle schneiden sich die deutschen Dienste und ihre Aufseher damit allerdings ab, beklagt Thorsten Wetzling vom Berliner Think Tank Stiftung Neue Verantwortung. Wetzling ist Leiter des Bereichs Digital Rights, Surveillance and Democracy bei der Stiftung, in dem man sich mit eigenen Konferenzen und einem Netzwerk zur Geheimdienstkontrolle (European Intelligence Oversight Network, EION [7]) um den internationalen Austausch bemüht. Mit der Internationalisierung der Dienste sollte auch eine multilaterale Kontrolle einhergehen, rät Wetzling. Dringlich ist dies vor allem da, wo sich die Dienste explizit in transnationalen Plattformen zusammenschließen. In der nach den Anschlägen vom 11. September ins Leben gerufenen und 2017 formal in Den Haag etablierten Counter Terrorism Group (CTG) kooperieren jenseits einer nationalen Kontrolle 30 Geheimdienste. Dafür braucht es dann auch einen Rahmen, in dem Datenschutz und Löschungsauflagen klar geregelt werden, schreibt das CTIVD. Die niederländische Regierung, so Wetzling, macht sich nämlich durchaus Gedanken, wer eigentlich verantwortlich ist für diese frei schwebende Gruppe. Die deutsche Aufsicht, so Wetzling, täte gut daran, statt in Nibelungentreue zu den US-Diensten zu stehen, aktiv an europäischen Standards mitzuarbeiten. <h3 class=„subheading“ id=„nav_automatischer7“>Automatischer Datentransfers, automatisierte Kontrolle?</h3> Gerade dann, wenn die Dienste die Grundrechte der Bürger anderer Staaten nicht beachten – wie der BND oder die US-Geheimdienste

–, laufen die Schutzfunktionen, die man auch zum Schutz der eigenen Verfassungsgüter implementiert, ins Leere, sagt von Notz. Die Schutzvorkehrungen haben nur noch Feigenblattcharakter. „Wir setzen extra Filtersysteme zur Ausfilterung der Daten von deutschen Bürgern auf, aber am Ende stellt die große Datenmühle der international kooperierenden Dienste sicher, dass niemand vor der Durchleuchtung seiner privatesten Kommunikation geschützt ist.“ Noch viel zu unterbelichtet bei der Kontrolle der deutschen Dienste ist laut Notz auch die Sicherheit der eigenen Systeme. „Wer überprüft beispielsweise, dass die Technik beim Ausleiten der Daten am Datenknotenpunkt sicherheitstechnisch auf dem neuesten Stand ist“, so von Notz. Angesichts massiver Cybersabotage sei er entsetzt über das fehlende Problembewusstsein bei der Aufsicht in diesem Punkt. Vorerst prüfe man in erster Linie den Output der staatlichen Schnüffelei, nicht aber die technischen Voraussetzungen. Dabei sei klar, dass wie bei der Manipulation von Abgaswerten auch die Manipulation von Filter-, Übertragungs- oder Datenhaltungstechnik „nicht eingepreist“ sei. Viel zu wenig technischen Sachverstand hatte im Verfahren vor dem Verfassungsgericht auch Eco-Experte Klaus Landefeld kritisiert. Unter den 30 Mitarbeiter, die dem PKGr zuarbeiten, sind zwar einzelne mit technischer Expertise. Doch für eine echte Überprüfung der Technik wäre man auf externe Gutachter angeweisen, räumte der Ständige Bevollmächtigte ein. UGr-Mitglied Cirener sagte schlicht, dass man bei allen technischen Details den BND fragen müsse, also den, der kontrolliert wird. Auch in diesem Bereich sind die Aufsichtsgremien in anderen europäischen Ländern deutlich weiter. Für die Niederlande schreibt die CTIVD, dass man hart daran arbeite, die technischen Untersuchungen im Rahmen der Aufsicht weiter zu verbessern. „Eine solche technische Untersuchung besteht darin, Funktionalitäten von Teilen der technischen Systeme der Dienste zu überprüfen“, schreibt das CTIVD. Das können Algorithmen, Log-Files oder technische Anwendungen und deren Zusammenspiel sein. Die IT-Abteilung der CTIVD wurde dafür eigens erweitert. Übrigens will man den Beaufsichtigten in nichts nachstehen. Da automatisiert Daten transferiert werden, bemüht man sich auch selbst um die Schaffung automatisierter Kontrollsysteme. Diese sollen im Idealfall Verletzungen der geltenden Regeln automatisiert erkennen und durch eine Markierung die Aufseher aufmerksam machen. Ideen dazu gibt es schon viele, darauf macht die SNV in einem aktuellen Papier [8] aufmerksam. <figure class=„a-inline-image a-u-inline“> <figcaption class=„a-caption“> Tools für Automatisierte Aufsicht der Datenflüsse bei den Nachrichtendiensten </figcaption></figure><h3 class=„subheading“ id=„nav_neuaufschlag8“>Neuaufschlag nach Verfassungsgerichtsurteil?</h3> Ob das für den Frühsommer erwartete Verfassungsgerichtsurteil der lahmen deutschen Geheimdienstkontrolle auf die Sprünge helfen kann, ist vorerst ungewiss. Auf Seiten der Beschwerdeführer ist man sich ziemlich sicher, dass die Verfassungsrichter die Beschränkung des Grundrechts auf Vertraulichkeit allein auf Deutsche nicht so stehen lassen werden. Wird das Gericht darüber hinaus dem Gesetzgeber Verbesserungen bei der Kontrolle auftragen? Notwendig wäre das ganz sicher, will das Verfassungsgericht nicht alle Jahre wieder als Ersatzkontrolleur auftreten. So nämlich empfanden viele Beteiligte und Beobachter die zweitägige Verhandlung in Karlsruhe. Informationen, die der Dienst hartnäckig vor der parlamentarischen Kontrolle geheim halten wollte, wurden BND und

Kanzleramt von den Verfassungsrichtern da wie Würmer aus der Nase gezogen. Angesichts der vielen noch anhängigen Verfahren zur Post-Snowden-Gesetzgebungswelle im Bereich Überwachung, sieht es aber fast so aus, als ob das Verfassungsgericht noch für einige Zeit den Geheimdienstaufseher spielen muss. Das gerade von Innenminister Seehofer doch wieder geforderte Gesetz zum Trojanereinsatz durch Verfassungsschutz und BND lässt grüßen. ()<br class=„clear“/> <hr/> URL dieses Artikels:
<small>

```
https://www.heise.de/-4677705
```

</small> Links in diesem Artikel:
<small>

```
<strong>[1]</strong>&amp;#160;https://www.heise.de/thema/Missing-Link
```

</small>
<small>

```
<strong>[2]</strong>&amp;#160;https://www.heise.de/newsletter/manage/ho?wt_mc=nl.red.ho.daily.meldung.link.link
```

</small>
<small>

```
<strong>[3]</strong>&amp;#160;http://dip21.bundestag.de/dip21/btd/18/125/1812585.pdf
```

</small>
<small>

```
<strong>[4]</strong>&amp;#160;https://english.ctivd.nl/latest/news/2019/06/20/index
```

</small>
<small>

```
<strong>[5]</strong>&amp;#160;https://www.tet.dk/charter-of-the-intelligence-oversight-working-group/?lang=en
```

</small>
<small>

```
<strong>[6]</strong>&amp;#160;https://english.ctivd.nl/investigations/review-report-unevaluated-data
```

</small>
<small>

```
<strong>[7]</strong>&amp;#160;https://www.stiftung-nv.de/en/eion
```

</small>
<small>

```
<strong>[8]</strong>&amp;#160;https://www.stiftung-nv.de/sites/default/files/data_driven_oversight.pdf
```

</small>
<small>

```
<strong>[9]</strong> mailto:bme@heise.de
```

</small>
 Copyright © 2020 Heise Medien </html>