Deutscher Bundestag **Drucksache 19/23695**

19. Wahlperiode 27.10.2020

Antrag

der Abgeordneten Konstantin Kuhle, Manuel Höferlin, Stephan Thomae, Dr. Jens Brandenburg (Rhein-Neckar), Grigorios Aggelidis, Renata Alt, Jens Beeck, Dr. Marco Buschmann, Britta Katharina Dassler, Hartmut Ebbing, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Peter Heidt, Katrin Helling-Plahr, Markus Herbrand, Katja Hessel, Ulla Ihnen, Dr. Christian Jung, Dr. Marcel Klinge, Pascal Kober, Michael Georg Link, Alexander Müller, Christian Sauter, Hermann Otto Solms, Bettina Stark-Watzinger, Benjamin Strasser, Katja Suding, Michael Theurer, Sandra Weeser, Nicole Westig und der Fraktion der FDP

Freiheit und Sicherheit schützen – Für eine Überwachungsgesamtrechnung statt weiterer Einschränkungen der Bürgerrechte

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

1. Moderne Datenverarbeitung ist ein Schlüssel zur Effizienzsteigerung und Beschleunigung verschiedenster Vorgänge. Unterschiedliche Akteure profitieren von umfangreichen Datenbanken und automatisierter Datenerfassung durch technische Geräte und Sensoren. Diese Daten sind auch für die Sicherheitsbehörden von großem Interesse. Angesichts wachsender Kommunikations- und Datenverarbeitungsmöglichkeiten im digitalen Raum verändern sich auch die Gefahren durch Terrorismus und Kriminalität. Demzufolge ändern sich die Anforderungen an die technische und personelle Ausstattung sowie an die Befugnisse der Sicherheitsbehörden. Automatisierte Datenerfassung und die Ausforschung digitaler Kommunikation durch die Sicherheitsbehörden bergen jedoch auch die Gefahr, den einzelnen Bürger zum bloßen Informationsobjekt werden zu lassen. Mit dem Ziel der Verhinderung von Terrorismus und Kriminalität kann unter Zuhilfenahme technischer Überwachungsinstrumente eine weitreichende Erfassung der Freiheitswahrnehmung jedes einzelnen Bürgers erreicht werden. Dabei schränken die ergriffenen Maßnahmen regelmäßig das aus dem allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 und Art. 1 Abs. 1 GG abgeleitete Recht auf informationelle Selbstbestimmung und das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme, das Post- und Fernmeldegeheimnis aus Art. 10 Abs. 1 GG sowie das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG ein.

2. Eine Vielzahl an Sicherheitsgesetzen ermöglicht bereits heute den Zugriff der Behörden auf zahlreiche persönliche Informationen von Privatpersonen durch umfangreiche Datensammlungen und Datenverarbeitungsabläufe. Eine genaue Übersicht über die derzeit bestehenden Überwachungsmöglichkeiten, über ihre regelmäßige Nutzung und ihre Eingriffsintensität gibt es dabei nicht.

Oftmals sind die Befugnisse unterschiedlicher Behörden in unterschiedlichen Gesetzen geregelt, die in einem schwer durchschaubaren Geflecht an gesetzlichen Verschränkungen keinen einfachen Durchblick mehr erlauben, sodass weder Behörden noch Bürgerinnen und Bürger auf einen Blick das Ausmaß der Eingriffsbefugnisse erkennen können. Darüber hinaus befinden sich einige Gesetze, die neue Überwachungsnormen beinhalten, gegenwärtig bereits in der Ressortabstimmung oder im parlamentarischen Verfahren.

3. Die Bundesregierung strebt eine Ausweitung der Befugnisse des Bundesamtes für Verfassungsschutz (BfV) an. Insbesondere sollen verschlüsselte Kommunikationsdaten erfasst werden können, deren Dechiffrierung dem BfV derzeit erhebliche Schwierigkeiten bereitet. Um die Verschlüsselung zu umgehen, soll die Kommunikation daher auf den Endgeräten durch den Einsatz von Schadsoftware erfasst und ausgeleitet werden. Neben der Kommunikation können auf dieselbe Weise auch gespeicherte Daten ausgelesen werden, ohne die Notwendigkeit von Beschlagnahmeanordnungen und eine Dechiffrierung der Endgeräte (vgl. https://netzpolitik.org/2020/bundesregierung-einigt-sich-auf-staatstrojaner-fuer-inlandsgeheimdienst/#vorschaltbanner; letzter Abruf: 9. 9. 2020). Die Unterscheidung zwischen der sogenannten Quellen-Telekommunikationsüberwachung, bei der lediglich die laufende Kommunikation erfasst wird, und der Online-Durchsuchung, bei der auch dauerhaft gespeicherte Daten ausgelesen werden, droht dabei zu einer rein rechtlichen Unterscheidung zu verkommen. Die verwendete Software bietet keine missbrauchssicheren Vorkehrungen, die ihre Nutzung lediglich auf eine der beiden Maßnahmen beschränken (vgl. https://netzpolitik.org/2019/polizei-darf-staatstrojaner-nutzen-aber-oft-nicht-installieren/#vorschaltbanner, letzter Aufruf 11.09.2020). Diskutiert wird dabei, die Quellen-Telekommunikationsüberwachung als sogenannte "Quellen-TKÜ plus" auch auf Kommunikation zu erstrecken, die bereits vor Beginn der Maßnahme erfolgte (vgl. https://www.sueddeutsche.de/digital/staatstrojaner-quellen-tkue-verfassungsschutz-1.5001279, letzter Abruf 11.09.2020).

4. Die Bundesregierung plant auch für die Bundespolizei den Zugriff auf private Daten von verschlüsselten Endgeräten (vgl. https://www.heise.de/newsticker/meldung/Bundespolizeigesetz-Seehofer-opfert-Gesichtserkennung-fuer-Staatstrojaner-4645734.html, letzter Aufruf 11.09.2020). Sie verspricht sich von diesen technischen Instrumenten eine effektivere Strafverfolgung insbesondere in den Bereichen der organisierten, grenzüberschreitenden Kriminalität und im grenzüberschreitenden Terrorismus. In diesen Schwerpunktgebieten ist es für Ermittlungsbehörden grundsätzlich schwer, Informationen aus den kriminellen Organisationen zu erlangen, während gleichzeitig die kriminellen Netzwerke stark verzweigt sind. Die Bundespolizei soll deshalb ebenfalls mit der Quellen-Telekommunikationsüberwachung und der noch weiter reichenden Online-Durchsuchung ausgestattet werden (https://www.faz.net/aktuell/politik/inland/gesetzesreform-warum-hat-seehofer-die-gesichtserkennung-gestoppt-16599260.html, letzter Abruf 11.09.2020).

5. Gleichzeitig hat die Bundesregierung auch für den Bereich der Grenzsicherung durch die Bundespolizei und im Personenfernverkehr die Ausweitung der automatisierten Datenverarbeitung ins Auge gefasst. Hier verspricht sie sich besonders von der automatisierten Gesichtserkennung durch intelligente Kamerasysteme einen Gewinn bei der Sicherung der Grenz- und Verkehrsflächen sowie bei der Fahndung. Vorbild für diese Forderung ist das bereits am Berliner Bahnhof Südkreuz durchgeführte Pilotprojekt mit intelligenter Gesichtserkennung. Daneben können intelligente Kamerasysteme auch durch

Verhaltenserkennung die bereits bestehende Videoüberwachung ergänzen. Zwar hat das Bundesministerium des Innern die automatisierte Gesichtserkennung zugunsten eines schnelleren parlamentarischen Verfahrens aus dem jüngsten Entwurf eines reformierten Bundespolizeigesetzes gestrichen, hält aber nach wie vor an diesem Konzept fest (vgl. https://netzpolitik.org/2020/innenministerium-streicht-automatisierte-gesichtserkennung/#vorschaltbanner, letzter Abruf 11.09.2020).

6. Die Bundesregierung hat mit dem bereits am 19. Dezember 2019 verabschiedeten Gesetz zur Neustrukturierung des Zollfahndungsdienstgesetzes (BT-Drucks. 19/12088) Eingriffsgrundlagen für erhebliche Eingriffe in die Grundrechte der Bürgerinnen und Bürger geschaffen. Neben einer umfassenden Bestandsdatenauskunft enthält auch dieses Gesetz in § 72 Abs. 3 ZfdG eine Befugnis zur Durchführung der Quellen-Telekommunikationsüberwachung, ohne technisch sicherzustellen, dass hierbei auch nur auf die laufende Kommunikation zugegriffen wird. Das Gesetz wird auch im Lichte des Beschlusses des Bundesverfassungsgerichts vom 27. Mai 2020 (1 BvR 1873/13, 1 BvR 2618/13) zur Bestandsdatenauskunft hinsichtlich seiner Verfassungsmäßigkeit neu zu bewerten sein.

7. Die Europäische Union schuf im Jahr 2006 mit der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten die Grundlage für die Neuregelung von Speicherpflichten in den Mitgliedstaaten. Deutschland setzte diese am 01. Januar 2008 mit dem "Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG" um. Die hierdurch eingeführte sogenannte "Vorratsdatenspeicherung" von Telekommunikationsdaten erklärte das Bundesverfassungsgericht am 02. März 2010 für verfassungswidrig und und das Gesetz für nichtig. Seit dem 18. Dezember 2015 gilt stattdessen das "Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten", das Telekommunikationsanbieter verpflichtet, unterschiedliche Verkehrsdaten zwischen vier und zehn Wochen zu speichern. Nach einem Beschluss des OVG Nordrhein-Westfalen vom 22.06.2017, in welchem das Gericht feststellte, dass Internetzugangsanbieter nicht an die in § 113b TKG geregelten Speicherverpflichtungen gebunden sind, hat die Bundesnetzagentur mitgeteilt, dass sie die im Gesetz vorgesehen Speicherverpflichtungen bis zum rechtskräftigen Abschluss des Verfahrens nicht durchsetzen wird (vgl. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html). Damit ist die sogenannte Vorratsdatenspeicherung in Deutschland derzeit de facto ausgesetzt. Die Einführung einer anlasslosen Vorratsdatenspeicherung wird jedoch immer wieder zur Bekämpfung verschiedener Delikte gefordert. Zuletzt war Anlass für einen solchen Vorschlag das Vordringen zahlreicher Demonstranten auf die Treppe des Berliner Reichstagsgebäudes im Rahmen einer Versammlung gegen die von der Bundesregierung beschlossenen Maßnahmen zum Schutz gegen Covid-19 (vgl. https://www.computerbild.de/artikel/cb-News-Internet-Nach-Corona-Demo-CDU-Forderung-Online-Rechte-Polizei-CCC-27433595.html, letzter Abruf 11.09.2020). Dieser Vorstoß zeigt, dass die Vorratsdatenspeicherung nicht mehr nur Instrument zur Bekämpfung von hauptsächlich im Internet begangenen Straftaten sein soll, sondern zunehmend auch Mittel zur Überwachung von Kommunikation im Vorfeld physisch begangener Straftaten.

8. Nach einem Beschluss des Bundesverfassungsgerichts vom 27. Mai 2020 (1 BvR 1873/13, 1 BvR 2618/13), mit dem die Regeln zur manuellen Bestandsdatenauskunft für verfassungswidrig erklärt wurden, strebt die Bundesregierung bereits eine umfassende Neuregelung an (vgl. https://www.heise.de/news/Reaktionen-auf-Urteil-zu-Bestandsdaten-auskunft-Beratungsresistenter-Gesetzgeber-4847061.html, letzter Abruf 11.09.2020). Bestandsdaten sind im Gegensatz zu den von der sogenannten Vorratsdatenspeicherung betroffenen Verkehrsdaten solche, die die Kundin oder der Kunde seinem Telekommunikationsanbieter zum Zweck des Vertragsabschlusses mitteilt. Das Gericht hat dabei deutlich gemacht, dass eine verfassungsgemäße Regelung für die Verwendung der Daten durch die Behörde tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz vorsehen muss (vgl. https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-061.html, letzter Abruf 11.09.2020). Insbesondere bedürfe es des Vorliegens einer konkreten Gefahr beziehungsweise eines Anfangsverdachts.

9. Aus den beschriebenen politischen und gesetzgeberischen Projekten ergeben sich zahlreiche neue Überwachungsmöglichkeiten. Nach der Rechtsprechung des Bundesverfassungsgerichts, darf „die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden" (BVerfGE 125, 260, Rn. 218 (Vorratsdatenspeicherung)). Eine Überwachungsmaßnahme ist dabei nicht nur anhand ihrer eigenen Intensität zu bewerten, sondern immer auch vor dem Hintergrund der übrigen bereits bestehenden Überwachungsmöglichkeiten. Anhand der Vorgaben des Bundesverfassungsgerichts hat die Rechtswissenschaft das Modell einer "Überwachungsgesamtrechnung" erarbeitet (vgl. Roßnagel, NJW 2010, 1238). Demnach müsse die Summe der staatlichen Überwachungsmaßnahmen auf ein Maß beschränkt werden, bei dem die Freiheitswahrnehmung der Bürger nicht total erfasst wird. Dies ist nach der Rechtsprechung des Bundesverfassungsgerichts sogar ein Teil der "verfassungsrechtlichen Identität der Bundesrepublik Deutschland" (vgl. BVerfG NJW 2010, 833 Rn. 218). Eine Überwachungsgesamtrechnung wird auch vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in seinem 28. Tätigkeitsbericht, zusammen mit einem sogenannten "Sicherheitsgesetz-Moratorium", gefordert. Auch Akteure der Zivilgesellschaft wie der Verein digitalcourage (vgl. https://digitalcourage.de/ueberwachungsgesamtrechnung/sammlung) sowie die Freie Demokratische Partei (vgl. https://www.fdp.de/sites/default/files/uploads/2017/06/26/bilanzsicherheitsgesetzgebung18wp.pdf) haben mit Sammlungen von Sicherheitsgesetzen, die in eine Überwachungsgesamtrechnung einzubeziehen wären, zur öffentlichen Diskussion über bestehende Überwachungsbefugnisse beigetragen.

10. Dogmatisch kann diese Überwachungsgesamtrechnung vielfältig ausgestaltet werden, eine konkrete Methodik wurde bisher aber noch nicht vorgelegt. Sie verpflichtet den Gesetzgeber jedoch in jedem Fall dazu, die technisch-gesellschaftliche Entwicklung genau zu beobachten, um sicherzustellen, dass die Summe der Überwachung das für die freiheitlich-demokratische Grundordnung erträgliche Maß nicht überschreitet. Der Gesetzgeber muss demnach vor der Ausweitung staatlicher Überwachungsmöglichkeiten das Gesamtmaß der Überwachung durch Datensammlungen und Überwachungsbefugnisse analysieren und deren Eingriff in die Bürger- und Freiheitsrechte unter Hinzuziehung der geplanten Verschärfungen bewerten. Als unabhängiges Gremium zur kontinuierliche Bewertung von freiheitseinschränkenden und Überwachungsmaßnahmen hat die Fraktion der Freien Demokraten im Deutschen

Bundestag bereits eine sogenannte "Freiheitskommission" nach dem Vorbild der "Wirtschaftsweisen" oder des Deutschen Ethikrats, mit Experten aus den Bereichen Justiz, Wissenschaft und Zivilgesellschaft, vorgeschlagen (siehe Bundestags-Drucksache 19/19009).

11. Debatten zu neuen Sicherheitsgesetzen haben sich in den vergangenen Jahren zunehmend dadurch ausgezeichnet, dass alle Seiten absolute Forderungen und Argumente ins Feld geführt haben, die jeweils nicht auf einer breiten Faktenbasis, sondern eher auf subjektiven Eindrücken aufbauten. Eine Überwachungsgesamtrechnung unter Berücksichtigung der aktuellen und zukünftigen technischen Möglichkeiten und Technologien wäre geeignet, Fehlentwicklungen bei der Sicherheitsgesetzgebung und der damit einhergehenden Schaffung von Rechtsgrundlagen für Überwachung und Datenerfassung vorzubeugen. Zudem könnte sie dazu beitragen, das Maß an Überwachung, dem die Bürgerinnen und Bürger täglich ausgesetzt sind, plastisch zu veranschaulichen und die Debatte um neue Sicherheitsgesetze durch die Evaluierung bereits bestehender Befugnisse evidenzbasiert zu begründen und nicht benötigte abzuschaffen.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

den Auftrag des Bundesverfassungsgerichtes ernst zu nehmen und beim Vorschlag neuer Überwachungsbefugnisse Zurückhaltung walten zu lassen. Ziel muss es sein, das Gesamtmaß staatlicher Überwachung, dem die Bürgerinnen und Bürger durch Eingriffsbefugnisse und Zugriffspraxis der Sicherheitsbehörden täglich ausgesetzt sind, so gering wie möglich zu halten. Das bislang nur abstrakt in der Wissenschaft entwickelte Modell einer "Überwachungsgesamtrechnung" soll zu diesem Zweck für die Anwendung innerhalb von Gesetzgebungsverfahren und für eine gesamtgesellschaftliche Debatte praktisch handhabbar gemacht werden. Diesem Ziel folgend ist die Bundesregierung dazu aufgefordert,

1. eine Methodik für eine Überwachungsgesamtrechnung zu entwickeln und vorzulegen, mit der alle bestehenden Datenspeicherungen und Überwachungsbefugnisse zusammengestellt und in ihrer Gesamtheit evaluiert werden sowie bis zur Erstellung einer solchen Methodik für eine Überwachungsgesamtrechnung keine neuen Sicherheitsgesetze vorzuschlagen, die Überwachungsbefugnisse beinhalten (Sicherheitsgesetz-Moratorium);

2. die kontinuierliche und systematische Analyse und Evaluierung sowohl bestehender als auch neu vorgeschlagener Überwachungsbefugnisse zu befördern, indem in Entwürfe neuer Sicherheitsgesetze Mechanismen eingeführt werden, die zur Schaffung einer besseren Datengrundlage für eine Überwachungsgesamtrechnung beitragen. Dies sind insbesondere:

    a. Evaluierungsklauseln für Überwachungsbefugnisse, die nach Ablauf einer bestimmten Zeit die Evaluierung neu eingeführter Befugnisse vorsehen. Die Evaluierung soll auch dann erfolgen, wenn Befugnisse zwischenzeitlich abgeschafft oder abgeändert wurden, um trotzdem Erkenntnisse für künftige Gesetzgebungsverfahren zu gewinnen;

    b. Berichtspflichten darüber, wie häufig und mit welchem Ergebnis eine Überwachungsbefugnis angewendet wurde;

    c. Forschungsklauseln, die der Wissenschaft Zugang zu Daten für wissenschaftliche Auswertungen von Sicherheitsgesetzen und einzelnen Befugnissen ermöglichen, der ihnen momentan oftmals unter Verweis auf Geheimhaltungsinteressen im Sicherheitsbereich verwehrt wird;

3. sich um eine Versachlichung der Debatten im Bereich der Sicherheitsgesetzgebung zu bemühen, indem insbesondere

    a. bei zukünftigen Gesetzgebungsvorhaben bereits bestehende Überwachungsbefugnisse evaluiert werden und die Notwendigkeit der neuen Befugnisse mit Blick auf das Ergebnis dieser Evaluation bewertet und fundiert begründet wird;

    b. zusätzlich eine Regelung geschaffen wird, die vorsieht, dass für alle Gesetzgebungsverfahren im Sicherheitsbereich eine Gesetzesfolgenabschätzung - nach dem Vorbild der einschlägigen Vorgaben zu Datenschutzfolgenabschätzungen - vorgenommen wird, die von den Regelungen zur Datenerhebung und -verarbeitung ausgehende Risiken für die Rechte und Freiheiten natürlicher Personen darlegt und bewertet;

    c. eine Freiheitskommission als unabhängiges Gremium nach dem Vorbild der "Wirtschaftsweisen" oder des Deutschen Ethikrats mit Experten aus den Bereichen Justiz, Wissenschaft und Zivilgesellschaft eingesetzt wird. Grundlage hierfür muss ein förmliches Gesetz sein. Aufgabe der Freiheitskommission ist die kontinuierliche Bewertung von freiheitseinschränkenden und Überwachungsmaßnahmen. Die Freiheitskommission ist langfristig zu institutionalisieren und soll als ständiges Beratungsgremium im Gesetzgebungsverfahren mitwirken;

4. Forschungsvorhaben zu fördern, welche die Auswirkungen von Überwachungsmaßnahmen und dem staatlichen Zugriff auf private und staatliche Datenbestände auf Freiheit und Demokratie untersuchen, um eine wissenschaftliche Durchdringung der immer größer werdenden Möglichkeiten der Überwachung der Bürgerinnen und Bürger zu erreichen und so auch die wissenschaftlichen Grundlage einer Überwachungsgesamtrechnung stetig zu verbessern.

Berlin, den 27. Oktober 2020

Christian Lindner und Fraktion