DPolG
DEUTSCHE POLIZEIGEWERKSCHAFT
im DBB

Bundesleitung

Friedrichstraße 169
10117 Berlin

Telefon (+49 30) 4081 6550
Telefax (+49 30) 4081 6559
dpolg@dbb.de
www.dpolg.de

An das
Bundesverfassungsgericht
- Erster Senat -
Postfach 1771
76006 Karlsruhe

vorab per
Fax: 0721/9101-382

19.06.2023/rw

Stellungnahme im Rahmen der Verfassungsbeschwerde 1 BvR 180/23

Die Deutsche Polizeigewerkschaft (DPolG) bedankt sich für die Gelegenheit zur Stellungnahme im Verfahren 1 BvR 180/23. Zur grundsätzlichen Haltung der DPolG zunächst einige Vorbemerkungen:

Die Möglichkeiten der Quellen-Telekommunikationsüberwachung (TKÜ) und der „Online-Durchsuchung“ sind für die DPolG unerlässliche Instrumente einer effektiven Verbrechensbekämpfung zur Wahrnehmung des grundgesetzlichen Schutzauftrages des Staates für die Menschen in unserem Land. Sie tragen dem Umstand Rechnung, dass das Kommunikationsverhalten von Straftätern im Zeitalter der Digitalisierung rasanten Veränderungsprozessen unterliegt.

Der Versuch, Kommunikation zu verschleiern und den Sicherheitsbehörden unzugänglich zu machen, dient in der Regel dem Zweck, Kriminalität und Terror zu ermöglichen, ihre Ziele zu optimieren und den Vorsprung vor den Sicherheitsbehörden auszubauen und konstant zu erweitern.

Auch in der Vergangenheitsbetrachtung gibt es keine Veranlassung, den Sicherheitsbehörden in Deutschland grundsätzliches Misstrauen entgegen zu bringen. Die gelegentlich vorgetragene Auffassung, die Instrumente würden zu einer „Destabilisierung der IT-Sicherheit“ beitragen, eine „Gefahr für die Innere Sicherheit“[1] darstellen und „Nutzer von Smartphones würden zum schutzlosen, gläsernen Objekt staatlicher Beobachtung“[2] lässt sich jedenfalls durch die bisherige Strafrechtspraxis nicht belegen, im Gegenteil.

---

[1] „Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung“ Chaos Computer Club – Sachverständigenauskunft zu Drucksache 18/11272
https://www.ccc.de/system/uploads/227/original/Stellungnahme_CCC-Staatstrojaner.pdf

[2] Verfassungsbeschwerde von unter anderem Rechtsanwälten, Künstlern und Journalisten zu der Frage, ob die durch das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl I 3202, in Kraft getreten am 24. August 2017) bewirkten Änderungen der Strafprozessordnung (StPO), insbe-

Die deutschen Sicherheitsbehörden zeigen durchgehend bis heute, dass sie die ihnen zur Verfügung stehenden Instrumente grundrechtsschonend und korrekt anzuwenden wissen. Darauf, dass diese Instrumente rechtsstaatlichen Grundsätzen genügen, haben Politik und Justiz, aber auch eine kritische Öffentlichkeit zurecht ein wachsames Auge[3].

Diese zurückhaltende Praxis der Rechtsanwendung[4] hat Gründe. Das vom BVerfG entwickelte Grundrecht auf informationelle Selbstbestimmung ist ein Kernbestandteil polizeilicher Aus- und Fortbildung und gehört gleichzeitig zum Wesensgehalt sicherheitspolitischer Handlungsmaxime. Zweifellos stellt der Eingriff in informationstechnische Systeme und die Erlangung von Informationen auf diesem Wege einen intensiven Eingriff in die Grundrechte dar. Dabei kann dahingestellt bleiben, ob er von gleicher Eingriffstiefe wie etwa die akustische Wohnraumüberwachung ist, er bewegt sich jedenfalls sicher in der gleichen Intensitätsklasse. Deshalb darf er ohnehin nur in Fällen schwerster Kriminalität und Terrorverdacht zur Anwendung kommen. Gleichzeitig muss der Schutzpflicht des Staates vor Angriffen auf informationstechnische Systeme durch Dritte gefolgt werden[5].

Strenge Eingriffsbeschränkungen, Richtervorbehalte und ständige Dokumentation und Prüfung der Fortdauer solcher Maßnahmen gehören zum Standard rechtsstaatlicher Eingriffe und werden ausdrücklich von der DPolG anerkannt.

Allerdings würde der völlige Verzicht auf diese notwendigen Instrumente der grundgesetzlichen Verpflichtung des Staates, auch alle anderen Grundrechte zu achten und zu schützen, nicht gerecht.

Zu den Kritikpunkten im Einzelnen:

<u>Quellen-Telekommunikationsüberwachung</u>

Die Beschwerde richtet sich gegen die angebliche Verletzung der durch Art 1 Abs. 1 Grundgesetz geschützten Menschenwürde. Die Beschwerdeführer hätten recht, wenn die Behauptung zuträfe, dass der Kernbereich privater Lebensgestaltung tatsächlich zum Ziel staatlicher Ermittlungen würde. Das ist allerdings ausdrücklich nicht der Fall.

---

sondere die Möglichkeit der Anordnung der sogenannten Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung (mittels des sogenannten „Staatstrojaners“), verfassungsgemäß sind.
https://www.bundesverfassungsgericht.de/DE/Verfahren/Jahresvorausschau/vs_2023/vorausschau_2023_node.html

[3] Zweifelsohne sind in den vergangenen Jahrzehnten bemerkenswerte Fortschritte erreicht worden, um auf die komplexer werdenden Bedrohungen zu reagieren und gleichzeitig die Errungenschaften rechtsstaatlicher Prinzipien nicht aufs Spiel zu setzen. Umfangreiche Gesetzgebungsschritte wurden stets flankiert von engagierten parlamentarischen Debatten, organisatorischen Entscheidungen und politischen Auseinandersetzungen, sowie von einer nach wie vor wachsamen Justiz, die gelegentlich einschritt, korrigierte oder Entscheidungen des Gesetzgebers verwarf. (Wendt) Vgl: Handbuch Polizeimanagement, 2. Auflage, ISBN 978-3-658-34387-3 S. 217.

[4].Statistiken zur Telekommunikationsüberwachung und zur Erhebung von Verkehrsdaten
https://www.praeventionstag.de/nano.cms/news/details/6704
hierzu auch: Michael Greven (OStA): Stellungnahme zum Gesetzentwurf Drs. 18(6)334 vom 29. Mai 2017, S. 6 ff.

[5] Leitsätze des BVerfG (IT-Sicherheitslücken), Beschluss des Ersten Senats vom 08. Juni 2021
- 1 BvR 2771/18 -.

Zweifelsohne stellt die Quellen-TKÜ einen außergewöhnlich schwerwiegenden Eingriff in die Persönlichkeitsrechte Einzelner dar. Unzweifelhaft ist aber genauso, dass die Sicherheitsbehörden in einer nie da gewesenen Situation der Bedrohung durch Kriminalität und Terror und gleichzeitig einer rasanten Beschleunigung der Entwicklung informationstechnischer Systeme gegenüberstehen, der es wirkungsvoll und möglichst grundrechtsschonend zu begegnen gilt.

Diesem Anspruch tragen die Bestimmungen der §§ 100a ff. StPO in ausreichendem, aber auch notwendigen Maße Rechnung. Die Überwachung von Telekommunikation ist in vielen Fällen polizeilicher Ermittlungen ein unerlässliches Instrument, um beweissichere Aussagen zum Tatgeschehen und seiner Beteiligten zu treffen, aber auch Hintergründe, Netzwerke und Zusammenhänge zu erkennen, die für die Erlangung wichtiger struktureller Informationen von Bedeutung sind.

Die Kommunikation hat sich mit der technischen Entwicklung in hohem Tempo verändert; verschlüsselte Telekommunikation ist längst nicht mehr das Privileg weniger, hoch spezialisierter und professioneller Täter, sie ist vielmehr Teil des standardisierten Angebots von Anbietern, für die die Möglichkeiten der Verschlüsselung längst zum „Werbeargument“ für ihre Produkte geworden ist.

Nur noch vergleichsweise wenig Telekommunikation durch Tatverdächtige wird über unverschlüsselte Wege durchgeführt, die dadurch entstehenden Verluste bei der Erkenntnisgewinnung durch die Strafverfolgungsbehörden sind nicht hinnehmbar. Sie würden potentielle Opfer im Stich lassen und die Möglichkeiten effektiver Strafverfolgung in völlig unangemessener Weise schwächen. Der verfassungsrechtliche Schutzauftrag des Staates geriete ins Hintertreffen.

Die Quellen-TKÜ verfolgt auch nicht das Ziel, die Sicherheitsbehörden mit grundsätzlich neuen, eingriffsintensiveren Möglichkeiten auszustatten. Sie bringt sie lediglich in den „Stand vorher“, als Telefonie über klassische Systeme abgewickelt wurde. Wenn und insoweit durch diese Möglichkeit auch andere Daten des jeweiligen Systems erhoben werden können, was technisch gelegentlich unvermeidbar scheint, kann dies durch andere rechtsstaatliche Kontrollinstrumente wie Zugriffsbefugnisse, Verwertungsregeln, Richtervorbehalte usw. geregelt werden.

In den Gesetzen des Bundes und der Länder ist die Quellen-TKÜ als Instrument der Gefahrenabwehr längst etabliert und wird erfolgreich angewendet[6]. Dabei gelten strenge Einzelfallentscheidungen und Richtervorbehalte zum Standard polizeilichen Handelns. Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit werden dort nicht per se unterstellt, sondern jeweils umfassenden Prüfungen durch voneinander unabhängige Begutachtung unterzogen.

Als Mittel der Gefahrenabwehr ist die Quellen-TKÜ auch höchstrichterlichen Betrachtungen unterzogen gewesen und wird es auch künftig wohl bleiben[7]. Tatsache ist aber, dass diese Entscheidungen zumeist zugunsten der gesetzlichen Regelungen endeten.

---

[6] BKAG und Polizeigesetze der Länder

[7] So der Beschluss des Ersten Senats des BVerfG vom 08. Juni 2021 – 1 BvR 2772/18 – zu § 54 Absatz 2 des Polizeigesetzes Baden-Württemberg oder BVerfG Urteil vom 20.04.2016 – 1 BvR 977/06 – zur Zulässigkeit der Quellen-TKÜ im BKAG.

Gefahrenabwehr ist ohne erfolgreiche Strafverfolgung kaum vorstellbar; obwohl unterschiedliche Rechtsgebiete und Zuständigkeiten, korrespondieren sie doch in etlichen Wirkungszusammenhängen. Die durch erfolgreiche Strafermittlungen gewonnenen Erkenntnisse, zum Beispiel zu Hintergründen von Strukturen, Vorbereitungshandlungen, Entwicklungen zur Tatbegehungsweisen u.v.a.m. fließen selbstverständlich in die Betrachtungen zur Gefahrenabwehr ein.

Es wäre daher wenig erklärbar, warum ein erfolgreiches Instrument der Gefahrenabwehr den Strafermittlungsbehörden a priori verwehrt bleiben sollte. Die erforderliche klare gesetzliche Befugnis ist daher auch im Sinne der Rechtsklarheit und Rechtssicherheit, sowohl für Ermittlungsbehörden als auch für die Bevölkerung unerlässlich.

Zu bedenken wäre auch, dass alternative Methoden, um an Kommunikationsinhalte von Verdächtigen zu gelangen, mit weitaus intensiveren Grundrechtseingriffen verbunden wäre, von denen möglicherweise völlig unbeteiligte Personen betroffen sein könnten (Observationen, Abhörmaßnahmen).

Auch in dieser Hinsicht stellt die Quellen-TKÜ eine rechtsstaatlich vertretbare, aber auch erforderliche Maßnahme dar.

<u>Online-Durchsuchung</u>

Für sie gilt zunächst das unter Seite 3, Absätze 1-3 genannte entsprechend.

Der Bundesgerichtshof[8] hat entschieden, dass die Online-Durchsuchung nicht auf die Ermächtigung zur Durchsuchung, bzw. der Telefon- oder Wohnraumüberwachung gestützt werden kann. Nunmehr ist der Gesetzgeber in der Verantwortung, durch eine spezielle Rechtsgrundlage den Ermittlungsbehörden die Möglichkeit zu geben, in das Recht auf Vertraulichkeit, und die Integrität informationstechnischer Systeme unter bestimmten Bedingungen, zur Verfolgung schwerster Straftaten, einzugreifen.

Bislang war in der Rechtsprechung, auch durch verschiedene Entscheidungen des BVerfG, die Möglichkeit der Online-Durchsuchung als Maßnahme der Strafverfolgung jedenfalls nicht für unmöglich erklärt worden. Vielmehr war das Gericht der Auffassung, dass diese Maßnahme nach der Intensität des Grundrechtseingriffs mit dem Eingriff in das Recht auf Unverletzlichkeit der Wohnung vergleichbar ist[9]. Insofern ist die Anlehnung an den Straftatenkatalog zur Wohnraumüberwachung nachvollziehbar und ausreichend.

Über die Verwertbarkeit der durch die Online-Durchsuchung gewonnenen Erkenntnisse dürfte nach verfassungsrechtlich abgesicherter Einführung einer Rechtsgrundlage kein Zweifel mehr bestehen. Insofern greift die Befürchtung, sie könne für die Strafverfolgungspraxis unbrauchbar sein, nicht.

---

[8] Entscheidung vom 31.1.2007 BGHSt. 51, 211; Online-Durchsuchung (Unzulässigkeit mangels Eingriffsermächtigung;

[9] Z.B. BVerfG vom 20.4.2016 – 1 BvR 966/09; 1 BvR 1140/09 Leitsatz 1a

Der Eingriff in das informationstechnische System eines Tatverdächtigen wird durch das verdeckte „Aufspielen“ einer Software vollzogen, mit deren Hilfe sämtliche Informationen ausgelesen werden könnten. Dem Schutz des Kernbereichs privater Lebensgestaltung, kommt in diesem Zusammenhang eine hohe Bedeutung zu, zumal durch diese Art des Eingriffs auch der Zugriff z.B. auf Kamerasysteme möglichwäre, die mittlerweile zur Standardausstattung nahezu sämtlicher informationstechnischer Systeme gehören.

Die Regelung des § 100d StPO ist nach Auffassung der DPolG umfassend, klar und ausreichend formuliert.

Nutzung von Schadsoftware – „Trojanersoftware“

Die Möglichkeit, mittels „Schwachstellen“ in der Software des zu durchsuchenden informationstechnischen Systems in das System selbst „einzudringen“, ist Gegenstand heftiger öffentlicher Diskussionen. Auch und insbesondere die Geheimhaltung bekannter „Schwachstellen“ und die daraus zumindest abstrakt darstellbaren Gefahren, erfordern rechtsstaatliche Lösungen, die durch klare gesetzliche Vorgaben formuliert werden müssen.

So formuliert der Chaos Computer Club in seiner Stellungnahme vom 31. Mai 2017[10] die Gefahren für Kritische Infrastrukturen wie folgt: „IT-Sicherheit ist ein kritischer Bestandteil der inneren Sicherheit. Kritische Infrastrukturen werden zu großen Teilen mit Standard-Software betrieben und verfügen über die gleichen Schwachstellen, die zur Infektion mit staatlicher Schadsoftware benötigt werden. Das Geheimhalten dieser Schwachstellen setzt somit die Kritischen Infrastrukturen einem direkten und unnötigen Angriffsrisiko aus.“[11]

Jedenfalls ist es den Beschäftigten der Ermittlungsbehörden nicht zuzumuten, sich in einer nicht vollständig geregelten und klar formulierten „Grauzone“ zu bewegen und sowohl als Person, als auch Behörde das Risiko von Prozessen mit unbestimmtem Ausgang zu tragen. Vielmehr ist es Aufgabe des Gesetzgebers, eine grundrechtskonforme Regelung so zu treffen, dass sich daraus für die Beschäftigten der Sicherheitsbehörden nachvollziehbare und rechtssichere Handlungsleitlinien ergeben.

Mit freundlichen Grüßen

Rainer Wendt
Bundesvorsitzender

[10] Chaos Computer Club: Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung, Neumann, Kurz, Rieger, vom 31. Mai 2017 Sachverständigenauskunft zu Ausschussdrucksache 17/11272.
[11] Zum Umgang mit Sicherheitslücken auch Arne Schönbohm (seinerzeit Präsident des Bundesamts für Sicherheit in der Informationstechnik BSI, im Interview mit Deutschlandfunk: https://www.deutschlandfunk.de/weltweiter-cyberangriff-sicherheitsluecken-stehen-jedem-zur-100.html.