GESELLSCHAFT FÜR FREIHEITSRECHTE

Stellungnahme als sachkundige Dritte

in den Verfahren

1 BvR 180/23

vor dem Bundesverfassungsgericht

betreffend

den Einsatz von „Staatstrojanern“ zur Strafverfolgung (§ 100a Abs. 1 Satz 2 und 3, Abs. 3 bis 6, § 100b, § 100d Abs. 1 bis 3 und Abs. 5 StPO)

Stand der Bearbeitung: 12. Juli 2023

Gesellschaft für Freiheitsrechte e.V.
Boyenstraße 41, D-10115 Berlin
Telefon (030) 555 71 665 - 0, E-Mail info@freiheitsrechte.org
freiheitsrechte.org

Inhalt

1 Mit Schreiben vom 12. April 2023 wurde die Gesellschaft für Freiheitsrechte e.V. (im Folgenden: **GFF**) vom Bundesverfassungsgericht im Rahmen des Verfahrens 1 BvR 180/23 die Gelegenheit gegeben, nach § 27a Bundesverfassungsgerichtsgesetz (BVerfGG) Stellung zu nehmen.

2 In dem Verfahren geht es um die grundrechtlichen Anforderungen an den Einsatz sogenannter „Staatstrojaner“ als Standardmaßnahme im strafrechtlichen Ermittlungsverfahren. Die Verfassungsbeschwerde rügt die Vereinbarkeit der Online-Durchsuchung (§ 100b StPO), der sogenannten kleinen Online-Durchsuchung (§ 100a Abs. 2 Satz 2 und 3 StPO) sowie der Quellen-Telekommunikationsüberwachung (im Folgenden: „**Quellen-TKÜ**“) mit Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 10 Abs. 1 GG, Art. 13 Abs. 1 GG und Art. 19 Abs. 4 GG.

3 Die GFF teilt die verfassungsrechtlichen Bedenken der Beschwerdeführer*innen. Um Redundanzen zu vermeiden, beschränkt sich die Stellungnahme auf zwei Aspekte, die besonders gewichtig und deshalb in einigen Punkten ergänzungswürdig sind:

- Die kleine Online-Durchsuchung verletzt das sog. Computergrundrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (**I**).
- Es mangelt an einer verfassungsrechtlich gebotenen verfahrensrechtlichen Absicherung der Beschränkung auf „laufende Telekommunikation“ in Art. 100a Abs. 5 Satz 1 Nr. 1 lit. b StPO (**II**).

I. KLEINE ONLINE-DURCHSUCHUNG NACH § 100A ABS. 1 SATZ 2 UND 3 STPO VERLETZT COMPUTERGRUNDRECHT

4 Die kleine Online-Durchsuchung (§ 100a Abs. 1 Satz 2 und 3 StPO) greift in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein **(1)**. Den dafür geltenden Voraussetzungen genügt die gesetzliche Regelung nicht **(2)**.

1. EINGRIFF IN DAS SOG. COMPUTERGRUNDRECHT

5 Wie die Beschwerdeführer*innen zutreffend feststellen, handelt es sich bei der kleinen Online-Dursuchung gem. § 100a Abs. 1 Satz 2 und 3 StPO um einen Eingriff in das allgemeine Persönlichkeitsrecht in seiner Ausprägung des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

Beschwerdeschrift, S. 67.

6 Diese Bewertung gründet insbesondere darauf, dass bei der kleinen Online-Durchsuchung auf ruhende Kommunikation zugegriffen wird **(1.1)** und sie sich quantitativ und qualitativ von der Quellen-TKÜ unterscheidet **(1.2)**. Stattdessen steht sie der klassischen Online-Durchsuchung im Eingriffsgewicht nicht nach, da sie einen Vollzugriff auf der ersten Stufe voraussetzt (**1.3.**), ein identisches Risiko der Ausspähung der Persönlichkeit (**1.4.**) und ein erhöhtes Missbrauchs- und Fehlerpotenzial birgt (**1.5.**)

1.1 ZUGRIFF AUF RUHENDE KOMMUNIKATION

7 Die Beschwerdeführer*innen führen (zwar erst auf Rechtfertigungsebene) zutreffend aus, dass es sich um bereits perpetuierte Kommunikationsinhalte handele, sodass die Grenze der ausschließlichen Anwendbarkeit von Art. 10 GG überschritten sei. Sie führen weiter aus, dass die Konstruktion einer „funktionalen Adäquanz“ nicht überzeuge, da es sich faktisch um eine Online-Durchsuchung handele. Eine Abstufung dazwischen sei nicht möglich. Es ginge um den Schutz der Daten um ihrer selbst willen, unabhängig davon, ob diese anderweitig hätten erlangt werden können. Die These der „funktionalen Adäquanz“ ziele unzulässig auf Ergebnis der Datenerhebung ab.

Vgl. Beschwerdeschrift, S. 69 f.

8 Darüber hinaus ist zu berücksichtigen, dass auch die im Gesetz angelegten Einschränkungen keine andere Bewertung zulassen.

9 Ausgangspunkt ist die Rechtsprechung des Senats, wonach es sich bei einer (klassischen) Online-Durchsuchung (§ 100b StPO) um einen Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme handelt.

10 Es besteht eine Bereichsausnahme hinsichtlich Eingriffen in die Telekommunikation, sodass insofern Art. 10 Abs. 1 GG zum Tragen kommt. Diese Ausnahme greift jedoch nur so weit, wie der Zugriff auf laufende Kommunikation begrenzt ist. Ein darüber hinausgehender Zugriff ist hingegen weiterhin an Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu messen.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 308.

11 Auch § 100a Abs. 1 Satz 2 und 3 StPO sind als Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu qualifizieren. Denn trotz der Einschränkungen wird nicht auf laufende, sondern auf ruhende Telekommunikation zugegriffen.

12 Die Vorschrift ermöglicht den Zugriff auf gespeicherte Daten mit zwei Einschränkungen. Die beiden Einschränkungen rechtfertigen aber keine andere rechtliche Bewertung, da dennoch auf ruhende Kommunikation zugegriffen wird und ein solcher Eingriff anderen verfassungsrechtlichen Maßstäben unterliegt.

13 Erstens darf nur auf Informationen zugegriffen werden, wenn diese auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können (§ 100a Abs. 1 Satz 3 Halbsatz 2 StPO).

14 Zweitens darf nur auf Informationen zugegriffen werden, die nach der Anordnung gespeichert wurden (§ 100a Abs. 5 Satz 1 Nr. 1 lit. b StPO).

15 Die Vorschrift knüpft mit der ersten Einschränkung an die Möglichkeit der Quellen-TKÜ in § 100a Abs. 1 Satz 2 an. Daraus ergibt sich die Beschränkung, dass auch Satz 3 nur einen Zugriff auf Telekommunikationsdaten ermöglicht wird. Dieser ist aber nicht auf die laufende Telekommunikation beschränkt, sondern geht darüber hinaus. Während bei Satz 2 gerade die Überwachung und Aufzeichnung ermöglicht wird, umfasst Satz 3 Fälle, in denen dies nicht möglich war und ermöglicht als Ausgleich den Zugriff auf die gespeicherte Kommunikation. Damit handelt es sich faktisch aber gerade um einen Zugriff auf die ruhende Kommunikation und damit nach der Kategorisierung des Senats um einen Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

> Vgl. *Brodowski*, in: BeckOK IT-Recht, 1. Aufl. 2020, StPO, § 100a Rn. 10; *ders./Sieber*, in: Hoeren/Sieber/Holznagel MMR-HdB, 58. EL März 2022, Teil 19.3 Strafprozessrecht, Rn. 151; *Martini/Fröhlingsdorf*, NVwZ 2020, 1803; *Großmann*, JA 2019, 241 (243); *Freiling/Safferling/Rückert*, JR 2018, 9 (21); *Singelnstein/Derin*, NJW 2017, 2646 (2648); in Bezug auf die vergleichbare Vorschrift im Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10): *Roggan*, DVBl 2021, 1471 (1474); *Poscher/Kappler*, Staatstrojaner für Nachrichtendienste, Verfassungsblog vom 6. Juli 2021, abrufbar unter https://verfassungsblog.de/staatstrojaner-nachrichtendienste/.

16 Dessen war sich auch der Gesetzgeber bewusst, sonst hätte er sich nicht mit der Konstruktion einer „funktionalen Adäquanz“ behelfen müssen. Der Gesetzgeber ist der Auffassung, dass es verfassungsrechtlich nicht geboten sei, ebenso wie bei laufender Kommunikation auch bei früherer Kommunikation die „wegen der besonderen Sensibilität informationstechnischer Systeme ... aufgestellten höheren Anforderungen des Bundesverfassungsgerichts [für Eingriffe in das Computergrundrecht] anzuwenden“.

BT-Drs. 18/12785, S. 50.

17 Auch diesbezüglich überzeugt die Argumentation des Gesetzgebers − wie auch die Beschwerdeführer*innen zutreffend herausstellen – nicht.

Beschwerdeschrift, S. 69.

18 Denn die Quellen-TKÜ für laufende Kommunikation stellt eine restriktiv auszulegende Ausnahme von der Regel dar, dass Trojaner-Einsätze grundsätzlich einen Eingriff in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG begründen.

19 Auch die zweite – zeitliche – Einschränkung ändert nichts daran, dass ein Zugriff auf ruhende Kommunikation vorliegt. Dass durch diese Einschränkung faktisch nur auf die gleiche Kommunikation zugegriffen werden kann, die bereits als laufende Kommunikation überwacht werden könnte und dementsprechend kein intensiverer Eingriff als bei der Quellen-TKÜ vorliegt, überzeugt nicht.

20 So kann auf die ruhende Kommunikation eben gerade nicht durch die Quellen-TKÜ zugegriffen werden.

1.2 QUALITATIVE UND QUANTITATIVE UNTERSCHIEDE ZUR QUELLEN-TKÜ

21 Auch darüber hinaus stellen sich aber die Überwachung nach Satz 2 und die Durchsuchung nach Satz 3 quantitativ und qualitativ äußerst unterschiedlich dar. Denn die Behörden sind bei einer beschränkten Online-Durchsuchung nicht gezwungen, mit hohem Aufwand pausenlos mitzuhören oder -lesen, um die Kommunikation vollständig zu überwachen oder zuvor selbst aufgezeichnete Kommunikation im Nachhinein auszuwerten. Sie benötigen einen Bruchteil des Aufwands, um zu einem von ihnen bestimmten Zeitpunkt in wenigen Sekunden faktisch die gesamte in einem längeren Zeitraum gelebte Kommunikation einzusehen. Diese enorme Vereinfachung erhöht die Bereitschaft zur Nutzung der Befugnis und damit die Wahrscheinlichkeit solcher Eingriffe faktisch erheblich.

22 Des Weiteren nähert sich die Kommunikation mittels Text- und Sprachnachrichten in einem Messenger in der praktischen Handhabung sehr stark der Flüchtigkeit der gesprochenen Sprache an. Die Nutzer*innen wenden hier typischerweise gerade nicht die erhöhte Sorgfalt auf, die herkömmlicherweise auf schriftliche Äußerungen gerade deshalb gerichtet wird, weil jene verkörpert und damit beständig sind. Die Überwachung der aufgezeichneten Chat-Kommunikation weist diesen Äußerungen nachträglich ein Gewicht zu, das die Betroffenen selbst ihnen im Moment der Kommunikation typischerweise gerade nicht zugemessen haben.

1.3 VOLLZUGRIFF AUF ERSTER STUFE

23 Auch bei der kleinen Online-Durchsuchung findet auf erster Stufe mit Infiltration des Systems ein Vollzugriff statt.

24 Da zunächst unklar ist, bei welchen auf einem System gespeicherten Daten es sich überhaupt um Telekommunikation handelt, muss eine Sichtung und Überprüfung der Dateien durchgeführt werden. Um diese Prüfung ausführen zu können, müsste der Trojaner zunächst alle gespeicherten Kommunikationsinhalte auslesen und auswerten, um entscheiden zu können, welche davon nach dem Beginn der Maßnahme gespeichert wurden, sodass sie als Quellen-TKÜ erhoben werden können.

Vgl. BT-Drs. 18/12785, S. 53

25 In dieser vollumfänglichen, zeitlich naturgemäß nicht begrenzten Auswertung der gespeicherten Kommunikationsinhalte liegt jedoch bereits eine dem Staat zuzurechnende Kenntnisnahme und damit eine Online-Durchsuchung, auch wenn die Daten nicht ausgeleitet, sondern noch „vor Ort“ auf dem infizierten System der Zielperson analysiert werden.

26 Mithin startet auch die beschränkte Online-Durchsuchung als klassische Online-Durchsuchung mit einem Vollzugriff auf das System. Erst auf einer zweiten Stufe werden dann Informationen ausgesiebt.

27 Dementsprechend betont der Senat in seiner Rechtsprechung auch, dass bei der klassischen Online-Durchsuchung durch die Infiltration des Systems bereits die entscheidende Hürde genommen wurde, um das System insgesamt auszuspähen und damit auch weitere persönlichkeitsrelevante Informationen zu erheben.

Vgl. BVerfGE 120, 274 <308 f.>; siehe hierzu auch *Roggan*, DVBl 2021, 1471 (1474).

28 Eine Infiltration nur der Telekommunikationsdaten ist nicht möglich.

1.4 IDENTISCHES RISIKO DER AUSSPÄHUNG DER PERSÖNLICHKEIT

29 Die Beschwerdeführer*innen stellen zutreffend fest, dass die kleine Online-Durchsuchung stehe klassischen Online-Durchsuchung im Eingriffsgewicht nicht nachsteht, da sie sich in Reichweite und Umfang faktisch nicht von der klassischen Online-Durchsuchung unterscheide. Dies gründe vor allem auf dem weiten Begriffsverständnis der Telekommunikationsdaten und der Dauer der Maßnahme. Dadurch könne ein umfassendes Persönlichkeitsprofil erstellt werden. Aufgrund regelmäßiger Synchronisierung, des Zugriffs auf Clouds, Backups etc. blieben nur wenige Daten verschont.

vgl. Beschwerdeschrift, S. 70-72.

30 Für die klassische Online-Durchsuchung hat der Senat herausgestellt, dass diese von besonderer Intensität ist, da sie das Risiko einer weitgehenden Ausspähung der Persönlichkeit birgt.

Vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17, Rn. 168.

31 Dieses Risiko liegt auch bei der kleinen Online-Durchsuchung vor.

32 Denn zum einen werden private Gedanken, Wünsche und Pläne vor allem auch in der Kommunikation mit anderen geäußert. Diese höchst sensiblen Telekommunikationsdaten dürfen keinem geringeren Schutzniveau unterliegen wie gleichartige Informationen, die in Dateien gespeichert sind, die nicht der Kommunikation dienen.

33 Auch die Einschränkung auf Inhalte, die nach der Anordnung gespeichert wurden, bewirkt keine Einschränkung, die einer Übertragung der Grundsätze der klassischen Online-Durchsuchung entgegenstehen würde.

34 So findet heutzutage ein erheblicher Anteil an Kommunikation über informationstechnische Systeme statt. Auch wenn also im Zeitpunkt der Anordnung selbst noch auf keine Inhalte zugegriffen werden kann, wächst die Zahl der Daten, auf die zugegriffenen werden kann, sodann rapide an und ermöglicht schnell eine

Erfassung der Persönlichkeit der Nutzer*innen. Dass vergangene Inhalte ausgeschlossen sind, ist insofern nicht von größerer Relevanz, da gerade die aktuellen Inhalte zur Erfassung der Persönlichkeit von besonderer Relevanz sind.

35 Wie die Beschwerdeführer*innen zutreffend herausstellen und insofern keiner tiefer gehenden Ausführung bedarf, führt der weite Telekommunikationsbegriff dazu, dass die beschränkte Online-Durchsuchung faktisch nicht begrenzt ist. Das Begriffsverständnis ermöglicht den Zugriff auf sämtliche Dateitypen. Durch regelmäßige Synchronisierung, den Zugriff auf Clouds und Backups vergrößert sich der Datenbestand, auf den mit der kleinen Online-Durchsuchung zugegriffen wird. Dadurch entfaltet auch die zeitliche Einschränkung in § 100a Abs. 5 Satz 1 Nr. 1 lit. b StPO faktisch keine Wirkung.

Beschwerdeschrift, S. 70 ff.

36 Ferner ergibt sich die besondere Intensität des Grundrechtseingriffs auch aus der Heimlichkeit der Maßnahme, dem Umstand, dass Schutzvorkehrungen umgangen werden, sowie der Streubreite.

Vgl. BVerfGE 120, 274 <322 ff.>.

37 Diese intensitätssteigernden Faktoren liegen auch bei § 100a Abs. 1 Satz 2 und 3 StPO in gleichem Maße vor.

1.5 ERHÖHTES MISSBRAUCHS- UND FEHLERPOTENZIAL

38 Erschwerend wirkt sich das der Regelung immanente Missbrauchs- und Fehlerpotential aus.

39 Durch den Vollzugriff auf erster Stufe besteht die Möglichkeit, dass es zu Fehlern oder Missbrauch bei der Aussonderung kommt.

40 Darüber hinaus würden beispielsweise auch falsche Zeitstempel einer gespeicherten Nachricht dazu führen, dass Inhalte ausgelesen würden, die vor Beginn einer Maßnahme gespeichert wurden. Dies jedoch würde bewirken, dass statt der angeordneten Quellen-TKÜ eine „irrtümliche“ Online-Durchsuchung durchgeführt würde. Der Irrtum ändert jedoch nichts an der damit verbundenen Eingriffstiefe und die anzusetzenden verfassungsrechtlichen Anforderungen an eine Rechtfertigung dieses Eingriffs.

2. VERFEHLEN DER VERFASSUNGSRECHTLICHEN ANFORDERUNGEN

41 Ein Eingriff in das sog. Computergrundrecht ist nur unter strengen verfassungsrechtlichen Voraussetzungen angemessen. Im präventiv-polizeilichen Berich darf er nur vorgesehen werden, wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen."

BVerfGE 120, 274 <328>.

42 Wie die Beschwerdeführer*innen zutreffend vortragen, sind diese Anforderungen auf den repressiven Bereich zu übertragen.

Beschwerdeschrift, S. 45 ff.

43 Dabei ist zu fragen, welche Rechtsgüter durch die Strafrechtspflege letztlich konkret geschützt werden sollen. Diese können und müssen sodann in Beziehung gesetzt werden zu denjenigen Rechtsgütern, in die Ermittlungsmaßnahmen eingreifen, die zur Verfolgung einer Straftat durchgeführt werden sollen.

44 Darüber hinaus ist insbesondere auf der Ebene der Verhältnismäßigkeit zu berücksichtigen, dass – bildhaft gesprochen – bei einem Eingriff in das Computer-Grundrecht zu präventiven Zwecken (hoffentlich) noch verhindert werden, dass „das Kind in den Brunnen fällt", also eine Rechtsgutsverletzung tatsächlich eintritt. Ist das Kind indes bereits gefallen, so dienen die dann nur noch möglichen repressiven Eingriffe primär der Sanktionierung der Verantwortlichen, können – um im Bilde zu bleiben – das Kind aber nicht wieder zum Leben erwecken, da die Rechtsgutsverletzung bereits eingetreten ist. Da die Strafrechtspflege kein Wert an sich ist, sondern dieser sich aus den durch sie zu schützenden Rechtsgütern ableitet, sind an Eingriffe in das Computergrundrecht zu repressiven Zwecken jedenfalls keine geringeren Anforderungen zu stellen als an präventive Eingriffe. Mit Blick auf die Gewichtung von Prävention und Repression im Hinblick auf den verfolgten Rechtsgüterschutz sind bei der Verfolgung allein repressiver Ziele eher höhere Anforderungen zu stellen. Denn es wird am Ende „nur" die Sanktionierung eines bereits irreversibel eingetretenen Rechtsgutsverstoßes verfolgt. Dass von

Verfassungs wegen deutlich größere Spielräume für präventive als für repressive Eingriffe bestehen, zeigt sich schließlich auch an der Wertung des Art. 13 GG (Unverletzlichkeit der Wohnung), der zu präventiven Zwecken (Art. 13 Abs. 3 GG) weitaus mehr Eingriffe zulässt als zu repressiven Zwecken (Art. 13 Abs. 4 GG).

Diese Anforderungen verfehlt § 100a Abs. 1 Satz 2 und 3 StPO deutlich.

Beschwerdeschrift, S. 68.

II. UNZUREICHENDE VERFAHRENSRECHTLICHE ABSICHERUNG

45 Die Beschwerdeführer*innen rügen, dass es weiterhin an einer verfassungsrechtlich gebotenen, verfahrensrechtlichen Absicherung, dass die einzusetzende Software den rechtlichen Anforderungen, insbesondere der Beschränkung auf „laufende Telekommunikation“ in Art. 100a Abs. 5 Satz 1 Nr. 1 lit. b StPO entspricht, fehle. Es sei verfassungsrechtlich nicht hinnehmbar, wenn unklar bliebe, ob und wer die Einhaltung der technischen Vorgaben überwache. Dem Gericht würde dies schon tatsächlich nicht möglich sein. Sie könne und dürfe nicht in das Belieben der mit der Durchführung der Maßnahmen betrauten Stellen überantwortet werden. Es sei vielmehr eine unabhängige Stelle zu benennen.

Beschwerdeschrift, S. 77 f.

46 Diese Einschätzung verdient im Folgenden eine vertiefende Erörterung.

47 Laut der Gesetzesbegründung darf ein Zugriff auf ein informationstechnisches System „grundsätzlich nur auf technischem Wege oder mittels kriminalistischer List“ erfolgen. Weitere Vorgaben an die technische Gestaltung enthält die Gesetzesbegründung gerade nicht.

BT-Drs. 18/12785, S. 52.

48 Die § 100a Abs. 5, § 100b Abs. 1 StPO enthalten zwar bestimmte Einschränkungen, etwa eine Beschränkung von Veränderungen auf das Notwendige oder einen Schutz vor unberechtigten Zugriffen durch Dritte. Die aus verfassungsrechtlichen Gründen notwendige Unterscheidung zwischen Quellen-TKÜ und Online-Durchsuchung macht auch eine entsprechende technische Trennung erforderlich. In diesem Sinne ist nach § 100a Abs. 5 Satz 1 Nr. 1 StPO technisch sicherzustellen, dass die Maßnahme ausschließlich die laufende Telekommunikation oder Inhalte und Umstände der Kommunikation betrifft, die ab dem Zeitpunkt der Anordnung

auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können. Nach § 100a Abs. 5 Satz 1 Nr. 2 und 3, § 100b Abs. 4 StPO ist zudem technisch sicherzustellen, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und dass die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden. Bei der Online-Durchsuchung ist zusätzlich gemäß § 100d Abs. 3 Satz 1 StPO technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.

49 Die Vorschriften in der StPO enthalten keine diesbezüglichen verfahrensrechtlichen Regelungen **(1)**. Der Einsatz von Staatstrojanern ohne einen objektiven, externen Überprüfungsmechanismus ist rechtsstaatlich nicht haltbar (**2**). Dies offenbart sich am Einsatz der Software „Pegasus“ in besonderem Maße **(3)**. Eine Abwälzung auf die Gerichte kommt nicht in Betracht **(4)**. Vielmehr bedarf es einer verpflichtenden Kontrolle durch eine unabhängige Stelle **(5)**.

1. KEINE VERFAHRENSRECHTLICHE REGELUNG IN § 100E ABS. 3 UND 4 STPO

50 In § 100e Abs. 3 und 4 StPO ist vorgegeben, welche Angaben und Begründungen die Anordnung enthalten muss. Das „technische Mittel“, dessen Einsatz beabsichtigt ist, also der einzusetzende Staatstrojaner muss danach aber weder benannt, noch müssen seine technischen Spezifikationen näher bezeichnet werden.

51 In der Literatur wird zwar vertreten, dass die die anordnende Stelle nach § 100e Abs. 1 S. 1 zu prüfen hat, ob die Voraussetzungen des § 100a Abs. 5 S. 1 Nr. 1 eingehalten werden. Diese Prüfungspflicht könne nur entfallen, wenn ein technisches Mittel eingesetzt wird, das hinsichtlich der Einhaltung der Anforderungen aus Abs. 5 von einer unabhängigen Stelle im Vorhinein geprüft und zertifiziert wurde.

> Rückert, in Münchener Kommentar StPO, 2. Aufl. 2023, § 100a Rn. 266.

52 Dies entspricht indes nicht der Praxis. Für eine solche Überprüfung sind die Gerichte schon nicht ausgestattet sodass sie sich bestenfalls auf die Angaben der Ermittlungsbehörden verlassen (dazu näher unten unter 4.).

53 Dies führt im Ergebnis dazu, dass die Ermittlungsbehörde beliebige Staatstrojaner nach Gutdünken einsetzten kann, sofern ein Beschluss über eine Maßnahme einmal erlangt werden kann.

2. ERFORDERNIS EINER ÜBERPRÜFUNG

54 Aus der Perspektive des Schutzes der Integrität und Vertraulichkeit informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ist ein derart blindes Vertrauen in die von den Ermittlungsbehörden einzusetzenden Staatstrojaner ohne einen rechtsstaatlich ausreichenden Überprüfungsmechanismus nicht hinnehmbar. Das ist angesichts der erheblichen Eingriffstiefe, aber auch der massiven Gefahren einer schleichenden Ausweitung einer Quellen-TKÜ hin zu einer Online-Durchsuchung, denen nur durch die Gestaltung des Trojaners entgegengewirkt werden kann, in jeder Hinsicht unangemessen. Es kommt erschwerend hinzu, dass die einzusetzende Software auch von einem externen Anbieter stammen kann, sodass die Ermittlungsbehörden mitunter selbst nicht mit Sicherheit einzuschätzen vermöchten, welche Funktionen die einzusetzende Software ausführt.

55 Diese enthalten oftmals zusätzliche, in Deutschland verfassungsrechtlich schlechthin nicht zugelassene Funktionen, etwa zur bewussten Manipulation des Zielsystems durch Unterschieben von Beweismitteln, die dann bei einer offenen Durchsuchung aufgefunden werden können. Der Gesetzgeber nimmt damit billigend in Kauf, dass auch in Deutschland Staatstrojaner zum Einsatz kommen, die gerade nicht den (ohnehin nur fragmentarischen) gesetzlichen Anforderungen an deren technische Gestaltung genügen.

3. RECHTSSTAATLICHE DEFIZITE IN DER PRAXIS AM BEISPIEL PEGASUS

56 Die Problematik zeigt sich beispielhaft am Einsatz der Pegasus-Software durch das BKA.

57 Pegasus ist eine Spähsoftware, die von dem israelischen Unternehmen „NSO Group“ zum Ausspähen von iOS- und Android-Geräten entwickelt wurde. Die Software kann ohne physischen Zugriff auf den Endgeräten installiert werden und anschließend unbemerkt auf sämtliche Daten zugreifen, inklusive verschlüsselter Chats. Darüber hinaus ist die Software in der Lage, unbemerkt Kamera und Mikrofon des Geräts anzuschalten. Den Recherchen von IT-Spezialist*innen zufolge kommt Pegasus durch drei Wege auf das Endgerät: Durch den Einsatz von

verseuchten Links, durch zero-klick Infektionen oder durch Netzwerkumleitungen von IMSI-Catchern. Dabei macht sich die Software sogenannte Zero-Day-Schutzlücken, also noch unbekannte Sicherheitslücken auf den jeweiligen technischen Geräten, zunutze. Diese werden in der Regel von Hackern aufgedeckt und anschließend für viel Geld an Geheimdienste oder Unternehmen wie die NSO Group verkauft, die sie nutzen, ohne sie dem Hersteller selbst zu melden. Sobald die Pegasus-Software einmal das Handy infiltriert hat, setzt sie dort Schutzmechanismen außer Kraft und verhindert automatische Sicherheitsupdates.

> Amnesty International, Forensic Methodology Report – How To Catch NSO Group's Pegasus, 2021, abrufbar unter https://www.amnesty.org/en/documents/doc10/4487/2021/en/;
>
> Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware, Bericht über die Prüfung von behaupteten Verstößen gegen das Unionsrecht und Missständen bei der Anwendung desselben im Zusammenhang mit dem Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware v. 22.05.2023 (2022/2077(INI)), abrufbar unter https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_DE.html;

58 Die NSO Group verkauft die Software nach eigenen Angaben nur an staatliche Stellen, unterschied dabei aber bisher nicht zwischen demokratischen und autokratischen Systemen. Zweck sei die Kriminalitäts- und Terrorismusüberwachung.

59 Im EU-Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware gab NSO an, dass derzeit fast 50 Länder den Staatstrojaner Pegasus etwa 12.000 bis 13.000 Mal pro Jahr einsetzten, um Smartphones zu hacken, darunter auch zwölf EU-Mitgliedstaaten.

> Netzpolitik.org v. 22.06.2022, abrufbar unter https://netzpolitik.org/2022/pega-untersuchungsausschuss-staatstrojaner-pegasus-wird-alle-40-minuten-eingesetzt/.

60 Im Juli 2021 wurde durch Recherchen von Amnesty International und einem internationalen Journalist*innenkonsortium bekannt, dass wahrscheinlich in mehreren Ländern hunderte von Journalist*innen, Menschenrechtler*innen, Rechtsanwält*innen und Oppositionellen sowie ausländischen Politiker*innen und Diplomat*innen ausgespäht wurden. Die Software wurde dabei unter anderem von Autokratien wie Saudi-Arabien, die Vereinigten Arabischen Emirate, Ruanda, Aserbaidschan und Marokko eingesetzt.

> Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware, Bericht über die Prüfung von behaupteten Verstößen

gegen das Unionsrecht und Missständen bei der Anwendung desselben im Zusammenhang mit dem Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware v. 22.05.2023 (2022/2077(INI)), abrufbar unter https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_DE.html;

Forbidden Stories, The Pegasus Project, alle Artikel abrufbar über https://forbiddenstories.org/case/the-pegasus-project/.

61 Medienberichten zufolge ließ sich das BKA im Jahr 2017 über die Software informieren. Damals sei der Einsatz jedoch wegen rechtlicher Bedenken abgelehnt worden,

ZEIT ONLINE vom 19. Juli 2021, abrufbar unter https://www.zeit.de/politik/ausland/2021-07/ueberwachungsaffaere-spionage-software-pegasus-einsatz-deutschland-bundeskriminalamt-handydaten-rechtsstaat.

62 Am 7. September 2021 teilten Vertreter*innen des BKA im Rahmen einer Sitzung des Innenausschusses des Bundestags mit, dass auch das BKA später eine Version dieser Software beschaffte und seit März 2021 einsetzt. Das Beschaffungsverfahren habe 2019 begonnen und sei 2020 abgeschlossen worden. Dabei seien keine Kontrollbehörden beteiligt gewesen. Nach Angaben des BKA wurde die Software allein bis 2021 in einer mittleren einstelligen Zahl von Verfahren eingesetzt und soll auch weiterhin eingesetzt werden. Dabei werde sie sowohl zur Gefahrenabwehr als auch zur Strafverfolgung eingesetzt.

ZEIT ONLINE vom 7. September 2021, abrufbar unter https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-bka-einsatz-nso-trojaner-israel

63 Angaben des BKA zufolge soll die eingesetzte Version der Software einen eingeschränkten Funktionsumfang haben. So soll eine Löschfunktion für den Schutz des Kernbereichs privater Lebensgestaltung eingebaut worden sein. Zudem sollen alle Einsätze protokolliert werden. Die Telefonnummern der Zielpersonen würden „gehasht“ übermittelt. Es sei zudem vertraglich vereinbart worden, dass keine sensiblen Daten an die NSO Group gehen.

ZEIT ONLINE vom 7. September 2021, abrufbar unter https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-bka-einsatz-nso-trojaner-israel.

64 Ein vom BKA verfasster Bericht über die modifizierte Version ist als Verschlusssache eingestuft.

Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware, Bericht über die Prüfung von behaupteten Verstößen gegen das Unionsrecht und Missständen bei der Anwendung desselben im Zusammenhang mit dem Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware v. 22.05.2023 (2022/2077(INI)), Nr. 365 m.w.N., abrufbar unter https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_DE.html.

65 Auch eine Kleine Anfrage zum Einsatz von Pegasus in Deutschland lieferte keine Erkenntnisse. Die Bundesregierung berief sich bei allen relevanten Fragen auf ein Geheimhaltungsbedürfnis.

Vgl. BT-Drs. 19/32246, S. 3 und S. 5.

66 Die Pegasus-Software kennt die Unterscheidung zwischen Online-Durchsuchung und Quellen-TKÜ grundsätzlich nicht. Sobald sie einmal in das Endgerät eingeschleust ist, übernimmt sie dieses vollständig. Ob die nach Angaben des BKA modifizierte Version der Software tatsächlich technisch sicherstellt, dass ausschließlich laufende Telekommunikation überwacht wird, erscheint zweifelhaft. Auch der Bericht des PEGA-Ausschusses stellt fest, dass es unklar sei, wie dies in der Praxis funktionieren solle.

Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware, Bericht über die Prüfung von behaupteten Verstößen gegen das Unionsrecht und Missständen bei der Anwendung desselben im Zusammenhang mit dem Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware v. 22.05.2023 (2022/2077(INI)), Nr. 365, abrufbar unter https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_DE.html.

67 Der Gesetzgeber hat auf diese Praxis zu reagieren und ist verfassungsrechtlich gehalten, einen Überprüfungsmechanismus zu etablieren, der sicherstellt, dass die rechtlichen Anforderungen an die eingesetzten technischen Mittel eingehalten werden.

Vgl. allgemein zur Beobachtungs- und Korrekturpflicht: BVerfGE 112, 304 <316 Rn. 51>; 141, 220 <290 Rn. 161>.

4. KEINE ABWÄLZUNG AUF DIE GERICHTE

68 Die Verantwortung für die Einhaltung der rechtlichen Anforderungen kann dabei nicht auf die Gerichte abgewälzt werden, die die Maßnahme anordnen. Denn zum einen müssten sie gezielt Rückfragen stellen, um überhaupt zu erfahren, welches technische Mittel eingesetzt werden soll und wie dieses im Einzelnen beschaffen

ist. Zum anderen kann von dem*der zuständigen Ermittlungsrichter*in (bei der Quellen-TKÜ, vgl. § 100e Abs. 1 StPO) und der zuständigen Kammer bzw. dem Senat (bei der Online-Durchsuchung, vgl. § 100e Abs. 2 StPO) nicht ernsthaft verlangt werden, eine EDV-technische Überprüfung des beabsichtigten Staatstrojaners selbst vorzunehmen. Eine ex-ante Prüfung durch die Gerichte ist angesichts der hierfür notwendigen Zeit auch deshalb ungeeignet, da sie in vielen Fällen den Zweck der Maßnahme gefährden dürfte. Im Zweifel werden sich Gerichte wohl auf die Einschätzung der Staatsanwaltschaft verlassen.

5. ERFORDERNIS EINER VERPFLICHTENDEN KONTROLLE DURCH EINE UNABHÄNGIGE STELLE

69 Deshalb bedarf es – wie auch die Beschwerdeführer*innen fordern − einer verpflichtenden Kontrolle durch eine unabhängige Stelle auf Ebene des Quelltextes, weil nur diese oder eine ähnlich unabhängige Stelle die Gewähr für eine wirklich neutrale Begutachtung der Software bietet.

> Beschwerdeschrift, S. 78.

70 Dafür käme beispielsweise die Kontrolle durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Betracht.

71 Zwar mögen die technischen Details eines Staatstrojaners nicht unbedingt durch formelles Gesetz zu regeln sein. Zumindest aber muss das Gesetz im Lichte des Wesentlichkeitsgrundsatzes eine unabhängige technische Überprüfung der einzusetzenden Staatstrojaner vorschreiben. Die durch einen Staatstrojaner zu erfüllenden Spezifikationen könnten etwa im Verordnungswege durch das Bundesamt für Sicherheit in der Informationstechnik unter verpflichtender Mitwirkung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vorgegeben werden. Die geltende gesetzliche Regelung sollte hierzu um eine entsprechende Verordnungsermächtigung ergänzt werden. Zudem sollte ausschließlich der Einsatz erfolgreich geprüfter Staatstrojaner zulässig sein. Eine entsprechende Darlegung dessen sollte in den Katalog der obligatorischen Inhalte einer Anordnung (§ 100e Abs. 3 und 4 StPO) aufgenommen werden. Solange dies nicht geschehen ist, trifft die geltende Regelung das Verdikt der Verfassungswidrigkeit.

Dr. Bijan Moini
Rechtsanwalt (Syndikusrechtsanwalt)