GESELLSCHAFT FÜR FREIHEITSRECHTE

**16. August 2024**

**Stellungnahme**
**der Gesellschaft für Freiheitsrechte e.V.**

**zum Referentenentwurf des Bundesministeriums des Inneren und für Heimat**
**„Entwurf eines Gesetzes zur Änderung des Sprengstoffgesetzes und weiterer Gesetze“**

## A. Zusammenfassung

Es besteht im Hinblick auf die Sprengung von Geldautomaten nach geltender Rechtslage keine Strafbarkeitslücke, die die Einführung eines neuen Qualifikationstatbestandes in § 308 Abs. 3 StGB rechtfertigt (**B.**).

Der Gesetzentwurf sieht außerdem eine Ausweitung des Einsatzes von Staatstrojanern vor, von der wir abraten (**C.**). Vielmehr sollten die Versprechen aus dem Koalitionsvertrag umgesetzt werden, zum einen die Eingriffsvoraussetzungen für den Einsatz von Staatstrojanern zu Ermittlungszwecken an die Vorgaben des Bundesverfassungsgerichtes für die Online-Durchsuchung anzupassen und zum anderen – wie vom Bundesverfassungsgericht gefordert – endlich eine gesetzliche Regelung zum Schwachstellenmanagement zu schaffen.

## B. Zur Einführung eines neuen Qualifikationstatbestands in § 308 Abs. 3 StGB

Bei dem neu eingeführten Absatz 3 in § 308 StGB handelt es sich um einen Qualifikationstatbestand, der die Kombination aus Sprengstoffexplosion und Diebstahl (§ 242 StGB) bzw. Bandendiebstahl (§ 244 Abs. 1 Nr. 2 StGB) oder schwerer Bandendiebstahl (§ 244a StGB) spezifisch erfasst und eine Mindeststrafandrohung von einer Freiheitsstrafe nicht unter 2 bzw. nicht unter 5 Jahren vorsieht.

Diese Neuerung ist im Ergebnis **überflüssig**, da die Geldautomatensprengung – auch als „Bande“ – im Strafgesetzbuch bisher bereits ausreichend abgedeckt ist: So kann unter Anwendung des § 243 Abs. 1 Nr. 2 StGB bereits der Diebstahl aus einem Geldautomaten höher bestraft werden; der Qualifikationstatbestand § 244 Abs. 1 Nr. 1 StGB deckt den Diebstahl mit Waffen ab, zusätzlich gibt es mit § 244a StGB auch bereits den Diebstahl mit Waffen als Mitglied einer Bande. Eine Schutzlücke, die die Einführung einer weiteren Qualifikation erfordert, ist nicht ersichtlich. Vielmehr erweckt der Referentenentwurf den Anschein, Geldautomatensprengungen wäre nach geltender Rechtslage straflos gestellt. Verurteilungen aus jüngerer Zeit zeigen aber deutlich, dass die Gerichte auch nach

geltender Rechtslage zum Teil hohe Strafen verhängen können.[1] Auch das im Entwurf angeführte rücksichtlose Fluchtverhalten kann entsprechend sanktioniert werden.[2]

## C. Zur Ausweitung des Einsatzes von Staatstrojanern

Der Gesetzentwurf sieht außerdem eine Ausweitung des Einsatzes von Staatstrojanern vor, indem ein weiterer Tatbestand (§ 40 Abs. 3a SprengG) in die Liste schwerer Straftaten in § 100a Abs. 2 StPO aufgenommen werden soll (als Nr. 9 lit. b).

Wir raten davon ab, die Befugnisse zum Einsatz von Staatstrojaner auszuweiten. Erstens genügen die Befugnisse zur Quellen-TKÜ und zur sogenannten kleinen Online-Durchsuchung nicht den verfassungsrechtlichen Anforderungen (**1.**). Zweitens fehlt es nach wie vor an einer Regelung zum Schwachstellenmanagement (**2.**).

### 1. Verfassungswidrigkeit der Befugnisse zur kleinen Online-Durchsuchung und Quellen-TKÜ in der StPO

Die Befugnis zur sogenannten kleinen Online-Durchsuchung in § 100a Abs. 1 Satz 2 und Satz 3 StPO verletzt das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Außerdem mangelt es an einer verfassungsrechtlich gebotenen verfahrensrechtlichen Absicherung der Beschränkung auf „laufende Telekommunikation" in Art. 100a Abs. 5 Satz 1 Nr. 1 lit. b StPO.

Diese Aspekte sind Gegenstand mehrerer **noch anhängiger Verfassungsbeschwerden**. Darunter befindet sich auch eine von der Gesellschaft für Freiheitsrechte e.V. koordinierte Verfassungsbeschwerde[3] sowie eine Verfassungsbeschwerde mehrerer FDP-Abgeordneter.[4] Im Rahmen eines weiteren Verfahrens hat die Gesellschaft für Freiheitsrechte e.V. zudem eine

---

[1] *Grimmer*, Lange Haftstrafen für Geldautomatensprenger, BR24 v. 24 Juli 2024, abrufbar unter https://www.br.de/nachrichten/bayern/bamberg-urteil-im-gelautomatensprenger-prozess-gefallen,UJPz9pt.

[2] Redaktion beck-aktuell v. 12. Juli 2024, "Vollendeter Mord": Lebenslang für Unfalltod bei Flucht, abrufbar unter https://rsw.beck.de/aktuell/daily/meldung/detail/lg-karlsruhe-geldautomatensprengung-mord-lebenslang-unfalltod-flucht.

[3] Verfassungsbeschwerde v. 22. August 2018, abrufbar unter https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Staatstrojaner/Verfassungsbeschwerdeschrift-Gesellschaft_fuer_Freiheitsrechte-2018-Staatstrojaner-Freiheit_im_digitalen_Zeitalter.pdf.

[4] Verfassungsbeschwerde v. 17. August 2018, Beschwerdeschrift veröffentlicht unter https://netzpolitik.org/2023/staatstrojaner-marco-buschmann-und-das-staatliche-hacken/.

ausführliche Stellungnahme abgegeben.[5] Das Bundesministerium des Innern und für Heimat (BMI) und der Gesetzgeber sollten deshalb zunächst die notwendigen Änderungen vornehmen und die Befugnisse an die verfassungsrechtlichen Vorgaben anpassen, mindestens aber die Entscheidung des Bundesverfassungsgerichts abwarten und die verfassungswidrige Befugnis nicht ausweiten.

§ 100a StPO erlaubt nicht nur die „klassische" Telekommunikationsüberwachung, sondern enthält in Absatz 1 Satz 2 und Satz 3 auch Befugnisse zum Einsatz von Staatstrojanern. § 100a Abs. 1 Satz 2 und Satz 3 StPO erlauben dabei nicht nur den Zugriff auf die laufende Kommunikation, sondern sehen auch vor, dass auf dem informationstechnischen System der betroffenen Person „gespeicherte Inhalte und Umstände der Kommunikation" überwacht und aufgezeichnet werden dürfen. Wie bei der Online-Durchsuchung findet zunächst ein Vollzugriff auf das System statt. Dadurch, dass eine Aussonderung erst nach dem Zugriff stattfindet, ist das Missbrauchs- und Fehlerrisiko denkbar hoch. Es besteht ein identisches Risiko der Ausspähung der Persönlichkeit der betroffenen Person. Die kleine Online-Durchsuchung unterscheidet sich damit erheblich von der Quellen-TKÜ in § 100a Abs. 1 Satz 2 StPO. Die Quellen-TKÜ wird ausnahmsweise lediglich an den geringeren verfassungsrechtlichen Anforderungen des Art. 10 GG gemessen, nämlich wenn sichergestellt ist, dass ausschließlich die laufende Kommunikation erfasst wird. Durch die kleine Online-Durchsuchung wird Ermittler*innen hingegen ermöglicht, auch auf die ruhende Kommunikation zuzugreifen. Ein solcher Eingriff muss deshalb den strengeren Anforderungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG genügen. § 100a Abs. 1 Satz 2 und Satz 3 StPO wird diesen Anforderungen in seiner derzeitigen Ausgestaltung nicht gerecht.

Insbesondere bei § 40 Abs. 3a SprengG handelt es sich um einen Vorfeldstraftatbestand, der noch vor einer konkreten Gefährdung oder gar Verletzung von Rechtsgütern eine Strafbarkeit auslöst.[6] Die Begehung setzt nicht einmal die Absicht späterer Begehung der eigentlich rechtsgutsverletzenden Tat voraus.[7] § 308 StGB, der nach geltender Rechtslage für die Strafbarkeit von Geldautomatensprengungen relevant ist, befindet sich bereits in der Liste der schweren Straftaten in § 100a Abs. 2 Nr. 1 lit. u StPO.

Auch verfahrensrechtlich ist der Einsatz von Staatstrojanern im Rahmen der kleinen Online-Durchsuchung nicht abgesichert. Weder muss der einzusetzende Staatstrojaner benannt, noch

[5] Gesellschaft für Freiheitsrechte e.V., Stellungnahme als sachkundige Dritte in den Verfahren 1 BvR 180/23 v. 12. Juli 2023, abrufbar unter https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Staatstrojaner/2023-07-12-BVerfG-Stellungnahme-GFF-Staatstrojaner-StPO.pdf.

[6] Vgl. zur Charakteristik von Vorfeldtatbeständen BVerfG, Beschluss des Ersten Senats vom 09. Dezember 2022, 1 BvR 1345/21, Rn. 50

[7] *Hilgendorf*, in: Arzt/Weber/Heinrich/Hilgendorf, Strafrecht Besonderer Teil, 4. Aufl. 2021, § 35 Rn. 20.

müssen seine technischen Spezifikationen näher bezeichnet werden. Da in Deutschland Software externer Anbieter*innen genutzt wird, die verfassungswidrige Funktionen wie das bewusste Manipulieren des Zielsystems durch das Unterschieben von Beweismitteln enthalten, ist ein objektiver, externer Überprüfungsmechanismus aus rechtsstaatlicher Sicht unbedingt erforderlich. So nutzt das Bundeskriminalamt die Software „Pegasus" der NSO-Group[8], die die Unterscheidung zwischen Online-Durchsuchung und Quellen-TKÜ grundsätzlich nicht kennt.[9] Es bedarf deshalb einer verpflichtenden Kontrolle durch eine unabhängige Stelle, zum Beispiel durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

Statt mit dem vorliegenden Entwurf erneut die Befugnisse zum Einsatz von Staatstrojanern auszuweiten, sollten das BMI und der Gesetzgeber die Befugnisse einschränken. Dafür legte das **Bundesministerium der Justiz bereits im letzten Jahr einen Referentenentwurf** vor, der einige der genannten Kritikpunkte aufgreift. Demnach soll die Quellen-TKÜ auf Sachverhalte beschränkt werden, bei denen ein Tatverdacht hinsichtlich einer besonders schweren Straftat im Sinne des Anlasstatenkataloges der Online-Durchsuchung gemäß § 100b Abs. 2 StPO besteht. Darüber hinaus wird der Anwendungsbereich der Quellen-TKÜ durch Aufhebung des § 100a Abs. 1 Satz 3 StPO so beschränkt, dass gespeicherte Kommunikationsdaten (insbesondere „Chats"), die ab dem Zeitpunkt der gerichtlichen Anordnung der Telekommunikationsüberwachung angefallen und zum Zeitpunkt des Beginns der Überwachung noch vorhanden sind, nicht mehr erhoben werden dürfen. Eine solche Erhebung wäre dann nur unter den Voraussetzungen der Online-Durchsuchung nach § 100b StPO möglich.[10] An diesem Entwurf sollte festgehalten werden.

Im **Koalitionsvertrag** haben sich die Regierungsparteien verpflichtet, die Eingriffsschwellen für den Einsatz von Überwachungssoftware, auch kommerzieller, hochzusetzen und das geltende Recht so anzupassen, dass der Einsatz nur nach den Vorgaben des Bundesverfassungsgerichtes für die Online-

[8] *Biermann*, ZEIT ONLINE v. 7. September 2021, abrufbar unter https://www.zeit.de/politik/deutschland/2021-09/spionagesoftware-pegasus-bka-einsatz-nso-trojaner-israel.

[9] 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. Mai 2023 (2022/2077(INI)), Nr. 365, abrufbar unter https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_DE.html.

[10] Referentenentwurf des Bundesministeriums der Justiz, Entwurf eines Gesetzes zur Begrenzung der Eingriffsbefugnisse im Rahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung, abrufbar unter https://netzpolitik.org/2023/gesetzentwurf-polizei-soll-staatstrojaner-etwas-seltener-nutzen-duerfen/.

Durchsuchung zulässig ist.[11] Eine Ausweitung des Einsatzes von Staatstrojanern stünde diesem Versprechen diametral entgegen.

## 2. Nach wie vor fehlendes Schwachstellenmanagement

Darüber hinaus fehlt es nach wie vor an einem Schwachstellenmanagement hinsichtlich des Einsatzes von Staatstrojanern. Um Staatstrojaner in die jeweiligen Systeme einzuschleusen, werden unter anderem IT-Sicherheitslücken ausgenutzt. Deshalb haben Behörden ein Interesse daran, die Sicherheitslücken nicht bei den Hersteller*innen zu melden, sondern sie offen zu halten. Dem steht entgegen, dass das Computergrundrecht den Staat dazu verpflichtet, zum Schutz der Systeme vor Angriffen durch Dritte beizutragen.[12]

Obwohl die Regierungsparteien im **Koalitionsvertrag** festgeschrieben haben, dass der Staat keine Sicherheitslücken ankaufen oder offenhalten, sondern sich in einem Schwachstellenmanagement unter Federführung eines unabhängigeren Bundesamtes für Sicherheit in der Informationstechnik immer um die schnellstmögliche Schließung bemühen wird,[13] ist weiterhin der Einsatz von Staatstrojanern unter Ausnutzung von Sicherheitslücken möglich, ohne dass bisher ein Schwachstellenmanagement vom Gesetzgeber etabliert wurde.

Dass ein solches Schwachstellenmanagement unbedingt erforderlich ist, hat das **Bundesverfassungsgericht** bereits deutlich gemacht:

> „Die grundrechtliche Schutzpflicht des Staates verlangt auch eine Regelung zur grundrechtskonformen Auflösung des Zielkonflikts zwischen dem Schutz informationstechnischer Systeme vor Angriffen Dritter mittels unbekannter Sicherheitslücken einerseits und der Offenhaltung solcher Lücken zur Ermöglichung einer der Gefahrenabwehr dienenden Quellen-Telekommunikationsüberwachung andererseits.“[14]

Es ist aus grundrechtlicher Perspektive nicht vertretbar, dass das BMI eine Ausweitung der Befugnisse zum Einsatz von Staatstrojanern plant, während bewusst in Kauf genommen wird, dass

---

[11] Mehr Fortschritt wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP, abrufbar unter https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf, S. 87.
[12] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021, 1 BvR 2771/18, Ls. 2 lit. a.
[13] Mehr Fortschritt wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP, abrufbar unter https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf, S. 87.
[14] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021, 1 BvR 2771/18, Ls. 2 lit. b.

Schwachstellen weiterhin nicht gemeldet und gezielt für Hackerangriffe ausgenutzt werden können. Im Jahr 2023 haben bundesweit über 800 Unternehmen und Institutionen Ransomware-Fälle bei der Polizei zur Anzeige gebracht, wobei von einer hohen Dunkelziffer auszugehen ist.[15] Die Ausnutzung einer Schwachstelle in einem Softwareprogramm gehört zu den drei häufigsten Einfallsvektoren von Ransomware-Gruppen.[16] Der Gesetzgeber muss seiner verfassungsrechtlichen Schutzpflicht schnellstmöglich nachkommen, statt Überwachungsbefugnisse auszuweiten und überflüssige Straftatbestände zu schaffen.

[15] BKA, Bundeslagebild Cybercrime 2023, abrufbar unter https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.html?nn=229942, S. 15.

[16] BSI, Die Lage der IT-Sicherheit in Deutschland, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2023/bsi-lagebericht2023.pdf?__blob=publicationFile&v=2, S. 22.