PRIVACY INTERNATIONAL

# Sellungnahme an das Bundesverfassungsgericht zum Verfassungsbeschwerdeverfahren 2 BvR 1850/18

September 2019

PRIVACY INTERNATIONAL

# Stellungnahme
# an das Bundesverfassungsgericht
# zum Verfassungsbeschwerdeverfahren 2 BvR 1850/18

September 2019

## Inhalt

ZUSAMMENFASSUNG ..... 2

EINLEITUNG ..... 3

I. DER EINSATZ VON STAATSTROJANERN KANN DEN KERN DES RECHTS AUF PRIVATSPHÄRE UND DATENSCHUTZ NACH INTERNATIONALEN UND EUROPÄISCHEN MENSCHENRECHTSBESTIMMUNGEN GEFÄHRDEN, WENN ER NICHT ANGEMESSEN EINGESCHRÄNKT WIRD; ..... 5

II. DER EINSATZ VON STAATSTROJANERN VERSTÖßT GEGEN DIE VERPFLICHTUNG DER STAATEN, DIE SICHERHEIT UND INTEGRITÄT VON IT-SYSTEMEN WIRKSAM ZU GEWÄHRLEISTEN ..... 8

III. DER EINSATZ VON STAATSTROJANERN DARF NICHT GEGEN DIE GRUNDSÄTZE DER NOTWENDIGKEIT UND VERHÄLTNISMÄßIGKEIT SOWOHL DES INTERNATIONALEN ALS AUCH DES EUROPÄISCHEN RECHTS VERSTOßEN ..... 13

A. STAATSTROJANER ZUM ZWECKE DER STRAFVERFOLGUNG MÜSSEN AUF DAS UNBEDINGT NOTWENDIGE BESCHRÄNKT WERDEN ..... 13

B. STAATSTROJANER NUTZEN BEVORRATETE SYSTEMSCHWACHSTELLEN, DEREN RISIKO FÜR DIE RECHTE DES EINZELNEN NICHT IN EINEM ANGEMESSENEN VERHÄLTNIS ZU DEM IN EINER EINZIGEN STRAFRECHTLICHEN UNTERSUCHUNG ANGESTREBTEN NUTZEN STEHEN KANN ..... 16

FAZIT ..... 19

## Zusammenfassung

Privacy International möchte mit diesem Schreiben im Verfahren 2 BvR 1850/18 vor dem Bundesverfassungsgericht zum Einsatz sogenannter "Staatstrojaner" als Standardmaßnahme in Strafermittlungsverfahren Stellung nehmen.

Privacy International ist eine gemeinnützige Nichtregierungsorganisation mit Sitz in London, die sich der Verteidigung des Rechts auf Privatsphäre auf der ganzen Welt widmet. Privacy International wurde 1990 gegründet und führt Forschungen und Untersuchungen zur staatlichen und kommerziellen Überwachung durch, wobei der Schwerpunkt auf den Technologien liegt, die diese Praktiken ermöglichen.

Privacy International hat vor den Gerichten Europas, einschließlich des Europäischen Gerichtshofs für Menschenrechte und des Gerichtshofs der Europäischen Union, und vor verschiedenen nationalen Gerichten, einschließlich der des Vereinigten Königreichs, Frankreichs, Ungarns, der Vereinigten Staaten von Amerika (US), Kolumbiens, Südafrika und Südkorea, Beschwerden eingebracht oder in Verfahren als Dritte interveniert, die das Recht auf Privatsphäre betreffen. Um die allgemeine Achtung des Rechts auf Privatsphäre zu gewährleisten, setzt sich Privacy International für starke nationale, regionale und internationale Gesetze zum Schutz der Privatsphäre ein. Privacy International wird regelmäßig aufgefordert, vor parlamentarischen und Regierungsausschüssen auf der ganzen Welt Sachverständigengutachten zu Fragen der Privatsphäre vorzulegen, und hat, unter anderem, den Europarat, das Europäische Parlament, die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung und die Vereinten Nationen beraten und ihnen Bericht erstattet. Ein weiterer Aufgabenbereich von Privacy International ist die Fähigkeit von Partnerorganisationen in Entwicklungsländern zu fördern.

In dieser Stellungnahme, die sich auf die Datenschutz- und Sicherheitsbedenken konzentriert, die durch den Einsatz von Staatstrojanern hervorgerufen werden, werden die folgenden Punkte aufgegriffen:

> I. Der Einsatz von Staatstrojanern bedroht den Kern des Rechts auf Privatsphäre und Datenschutz nach internationalen und europäischen Menschenrechtsbestimmungen.
>
> II. Der Einsatz von Staatstrojanern verstößt gegen die Verpflichtung der Staaten, die Sicherheit und Integrität von IT-Systemen wirksam zu gewährleisten.

III. Der Einsatz von Staatstrojanern kann mit den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit sowohl nach internationalem als auch nach europäischem Recht unvereinbar sein.

## Einleitung

Hacking ist eine Handlung oder eine Reihe von Handlungen, die ein System stören und es dazu veranlassen, unbeabsichtigt oder unvorhersehbar durch den Hersteller, Benutzer oder Eigentümer dieses Systems zu handeln.[1] System bezieht sich sowohl auf eine beliebige Kombination von Hard- und Software als auch auf eine Komponente davon. Gegenstand der vorliegenden Stellungnahme ist eine besondere Form des Hackings, wie sie die angregriffenen §§ 100a, 100b StPO erlauben, nämlich der staatliche Einsatz von Trojanern unter Ausnutzung von Schwachstellen im System der Zielperson (Einsatz von Staatstrojanern).

Als eine Form der staatlichen Überwachung stellt der Einsatz von Staatstrojanern eine einzigartige und schwerwiegende Bedrohung für die Privatsphäre und Sicherheit dar. Es hat das Potenzial, weitaus eindringender zu sein als jede andere Überwachungstechnik, die es der Regierung ermöglicht, aus der Ferne und heimlich auf persönliche Geräte und alle darin gespeicherten vertraulichen Informationen zuzugreifen.[2]

Der Einsatz von Staatstrojanern erlaubt der Regierung auch, neuartige Formen der Echtzeitüberwachung durchzuführen, indem sie im Geheimen die Mikrofon-, Kamera- oder GPS-basierte Ortungstechnologie eines Geräts einschaltet, kontinuierliche Screenshots macht oder alles sieht, was in das Gerät eingegeben und von ihm ausgegeben wird.[3] Er ermöglicht es Regierungen, Daten auf Geräten zu manipulieren, indem sie Daten löschen, beschädigen oder einpflanzen, gelöschte Daten wiederherstellen oder Code-Änderungen oder -Editierungen vornehmen, um Fähigkeiten zu ändern oder hinzuzufügen, während sie gleichzeitig jede Spur des Eindringens löschen. Diese Ziele sind nicht auf Geräte beschränkt. Sie können sich auch auf Kommunikationsnetze und die ihnen zugrunde liegende Infrastruktur erstrecken.

---

[1] Privacy International, 'Government Hacking', https://privacyinternational.org/topics/government-hacking.

[2] U.S. District Court, Western District of New York, *Privacy International and Others v. Federal Bureau of Investigation and Others* (Case No. 18-cv-1488), https://privacyinternational.org/sites/default/files/2019-01/pi_v._fbi_-_hacking_foia_-_complaint_-_as_filed.pdf, Ziff. 5-6.

[3] Investigatory Powers Tribunal (IPT), *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, Witness Statement of Eric King (5. Oktober 2015), https://privacyinternational.org/sites/default/files/2018-03/2015.10.05%20Witness_Statement_Of_Eric_King.pdf, S. 11-12.

Gleichzeitig hat der Einsatz von Staatstrojanern das Potenzial, die Sicherheit von Zielgeräten, Netzwerken oder Infrastrukturen und möglicherweise sogar das Internet als Ganzes zu gefährden. Computersysteme sind komplex und enthalten mit an Sicherheit grenzender Wahrscheinlichkeit Schwachstellen, die Dritte ausnutzen können, um ihre Sicherheit zu gefährden. Regierungshacken hängt oft davon ab, Schwachstellen in Systemen auszunutzen, um ein Überwachungsziel zu erreichen. Hacking kann auch die Manipulation von Menschen beinhalten, um in ihr eigenes System einzugreifen. Diese letztgenannten Techniken setzen auf das Vertrauen der Nutzer, dessen Verlust die Sicherheit der Systeme und des Internets untergraben kann.

Eine wachsende Zahl von Regierungen auf der ganzen Welt machen Gebrauch von Überwachungstechnologien wie Staatstrojanern,[4] aber viele setzen diese Technologien heimlich und ohne klare Rechtsgrundlage ein. In den Fällen, in denen Regierungen versuchen, diese Befugnisse auf eine gesetzliche Basis zu stellen, tun sie dies ohne ausreichende Garantien und Kontrollen, um die Auswirkungen von Hacking auf die Privatsphäre und Sicherheit zu minimieren.

Im Jahr 2017 wurde die StPO dahingehend geändert, dass die Untersuchungsbehörden in die Informationstechnologiesysteme "eingreifen" können, um Daten von ihnen zu erheben.[5] Dies wiederum würde die Installation von Software erfordern, die Daten liest, um sie aus dem Gerät der Person zu extrahieren, und an die Strafverfolgungsbehörden überträgt. Diese Überwachungstechnologie wird allgemein als "Staatstrojaner" bezeichnet.[6]

[4] Zum Beispiel, UK Investigatory Powers Act 2016, Part 5 (Equipment interference); U.S. Federal Rules of Criminal Procedure, Rule 41, und auch Privacy International, 'Whose World Is This? US and UK Government Hacking' (Juli 2016) https://privacyinternational.org/feature/1691/whose-world-us-and-uk-government-hacking; Artikel 15 des Föderalen Gesetzes der Russischen Föderation über den Föderalen Sicherheitsdienst (Nr. 40-FZ) 1995 ("*[J]uristische Personen in der Russischen Föderation, die elektronische Kommunikationsdienste aller Art erbringen.... sind auf Verlangen der Organe des Föderalen Sicherheitsdienstes verpflichtet, zusätzliche Hard- und Software in die Vorrichtung aufzunehmen und andere Bedingungen zu schaffen, die erforderlich sind.... zur Durchführung operativer/technischer Maßnahmen*").

[5] § 100a Abs. 1 und § 100b StPO nach dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017, Bundesgesetzblatt 2017 I, 3202.

[6] Sven Herpig und Julia Schuetze, 'Umfassende Cyber-Sicherheitspolitik für Deutschland' (Stiftung Neue Verantwortung, 6. Oktober 2017), https://www.stiftung-nv.de/de/publikation/umfassende-cyber-sicherheitspolitik-fuer-deutschland.

## I. Der Einsatz von Staatstrojanern kann den Kern des Rechts auf Privatsphäre und Datenschutz nach internationalen und europäischen Menschenrechtsbestimmungen gefährden, wenn er nicht angemessen eingeschränkt wird;

Menschenrechtsbestimmungen, die das Recht auf Privatsphäre und den Schutz personenbezogener Daten gewährleisten, können Einschränkungen dieser Rechte zulassen, solange sie sich an bestimmte Grundsätze wie Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit halten und den "Kern" oder den "Wesensgehalt" dieser Rechte achten.[7]
Der UN-Sonderberichterstatter für Terrorismusbekämpfung und Menschenrechte betonte, dass "*die Beeinträchtigungen [des Rechts auf Privatsphäre] in keinem Fall in einer Weise angewendet oder geltend gemacht werden dürfen, die den Kern eines Paktrechts beeinträchtigen würde*".[8] Das Büro des Hochkommissars der Vereinten Nationen für Menschenrechte hat ebenfalls darauf hingewiesen, dass "*jede Einschränkung des Rechts auf Privatsphäre das Wesen des Rechts nicht bedeutungslos machen darf und mit anderen Menschenrechten vereinbar sein muss*".[9]

Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) sieht vor, dass jede Person "*das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz*" hat. Der Europäische Gerichtshof für Menschenrechte (EGMR) hat entschieden, dass Maßnahmen wie die heimliche Kommunikationsüberwachung zur Aufdeckung oder Verhütung von Straftaten in den Anwendungsbereich von Artikel 8 der Konvention fallen, und betont, dass Einschränkungen dieses Rechts den

[7] Vgl. Artikel 17 Abs. 1 Internationale Pakt über bürgerliche und politische Rechte ("*Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden*"); Artikel 8 Abs. 2 Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) ("*Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist …*"); Artikel 52 Abs. 1 Charta der Grundrechte der Europäischen Union ("*Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten*").

[8] Bericht des UN-Sonderberichterstatters für Terrorismusbekämpfung und Menschenrechte (A/69/397, 23. September 2014), Ziff. 51.

[9] UNO-Hochkommissariat für Menschenrechte, ‚Das Recht auf Privatheit im digitalen Zeitalter' (A/HRC/27/37, 30. Juni 2014), Ziff. 23; vgl. EMRG, *Zakharov v. Russland* (Beschwerde Nr. 47143/06, 4. Dezember 2015), Ziff. 232 (unter Hinweis darauf, dass es "die Gefahr bestand, dass ein zum Schutz der nationalen Sicherheit eingerichtetes System der geheimen Überwachung die Demokratie unter dem Deckmantel ihrer Verteidigung untergraben oder sogar zerstören kann").

durch dieses Recht gewährten Schutz nicht unannehmbar schwächen sollten.[10] In *Christine Goodwin*[11] stellte der EGMR fest:

> „Dennoch ist das Wesen der Konvention die Achtung der Menschenwürde und der Freiheit des Menschen. Insbesondere nach Artikel 8 der Konvention, in dem der Begriff der persönlichen Autonomie ein wichtiger Grundsatz bei der Auslegung ihrer Garantien ist, wird der persönlichen Sphäre jedes Einzelnen Schutz gewährt."[12]

Ebenso garantieren Artikel 7 und Artikel 8 der Charta der Grundrechte der Europäischen Union (GRCh) das Recht auf Privatsphäre bzw. das Recht auf Schutz personenbezogener Daten. In Artikel 52 Abs. 1 der GRCh heißt es, dass die in der Charta anerkannten Einschränkungen der Rechte und Freiheiten "*den Wesensgehalt dieser Rechte und Freiheiten achten*" müssen. In *Digital Rights Ireland*[13] prüfte der EuGH die Vereinbarkeit der Richtlinie 2006/24/EG (Vorratsdatenspeicherungsrichtlinie),[14] die die Speicherung und den Zugang zu Verkehrs- und Standortdaten zum Zwecke der Verhütung, Aufdeckung und Verfolgung schwerer Straftaten vorsieht, mit den Artikeln 7 und 8 GRCh. Zum Wesensgehalt des Rechts auf Privatsphäre stellte das Gericht fest, dass

> "die nach der Richtlinie 2006/24 vorgeschriebene Vorratsspeicherung von Daten zwar einen besonders schwerwiegenden Eingriff in diese Rechte darstellt, doch nicht geeignet ist, ihren Wesensgehalt anzutasten, da die Richtlinie die Kenntnisnahme des Inhalts elektronischer Kommunikation als solchen nicht gestattet."[15]

Mit anderen Worten, diese Begründung deutet darauf hin, dass Störungen, die den Zugang zu den Inhalten der elektronischen Kommunikation ermöglichen, als Antasten des Wesensgehalts des Rechts auf Privatsphäre und des Rechts auf Schutz personenbezogener Daten angesehen werden *könnten*.

---

[10] EMRG, *S. and Marper v. das Vereinigte Königreich* (Beschwerden Nr. 30562/04 und 30566/04, 4. Dezember 2008), Ziff. 112.

[11] EMRG, *Christine Goodwin v. das Vereinigte Königreich* (Beschwerde Nr. 28957/95, 11. Juli 2002).

[12] Ibid, Ziff. 90.

[13] EuGH, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & Others and Seitlinger and Others*, Urteil vom 8. April 2014, Rs. C-293/12 und C-594-12.

[14] Richtlinie 2006/24/EG des Europäischen Parlaments und des rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.

[15] EuGH, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & Others and Seitlinger and Others*, Urteil vom 8. April 2014, Rs. C-293/12 und C-594-12, Ziff. 39.

Heute haben die IT-Geräte einer Person, wie ein Telefon und/oder ein Computer, ihre Fotoalben, persönlichen Tagebücher, Briefe und Papiere, Adressbücher und vieles mehr ersetzt.[16] Dies wird durch die Vielzahl der Möglichkeiten unterstrichen, mit denen IT-Geräte ausgestattet sind, wie z.B. verschiedene Plug-Ins, mit denen Einzelpersonen nicht nur Nachrichten, E-Mails, Sprachaufzeichnungen, Videos und Fotos speichern können, sondern auch Kreditkartendaten, einschließlich Mobile Banking und mobiler Zahlungsdaten,[17] Passdaten (biometrische Daten),[18] Passwörter, virtuelle Schlüssel zu digitalen Schlössern[19] usw.

Der Einsatz von Staatstrojanern ermöglicht den Fernzugriff auf diese Systeme, die Steuerung von Funktionen wie Kameras, Mikrofonen und Tastaturen und damit den potenziellen Zugriff auf alle darauf gespeicherten Daten.[20] Privacy International hat festgestellt, dass die Polizei im Vereinigten Königreich sehr eindringende Technologien einsetzt, um Daten aus den Handys von Einzelpersonen zu extrahieren und zu speichern. Die Technologie, die auf nationaler Ebene eingeführt wurde, nachdem sie vom Metropolitan Police Service während der Olympischen Spiele in London 2012 eingesetzt wurde, gibt der Polizei die Möglichkeit, Daten von unseren Handys zu erhalten, zu denen wir selbst keinen Zugang haben und von denen wir nicht wissen, dass sie existieren.[21]

Staatstrojaner sind daher auch bei Einsatz gegen einzelne Geräte gleichermaßen eine extrem eindringliche Untersuchungstechnik, da sie, wie oben gezeigt, den Zugang zu

---

[16] Oberrichter *Roberts* äußert sich zur Eindringlichkeit des Zugangs zu einem modernen Telefon: "Ein Handy sammelt an einem Ort viele verschiedene Arten von Informationen - eine Adresse, eine Notiz, ein Rezept, einen Kontoauszug, ein Video -, die in Kombination viel mehr enthüllen als jede einzelne Aufzeichnung.... Die Summe des Privatlebens einer Person kann durch tausend Fotos rekonstruiert werden, die mit Daten, Orten und Beschreibungen beschriftet sind; dasselbe kann nicht von einem Foto oder zwei Lieben gesagt werden, die in einer Brieftasche versteckt sind...", *Riley v. California*, Oberster Gerichtshof der Vereinigten Staaten, 573 U. S. ____ (2014), S. 18.

[17] Siehe, zum Beispiel, Visa, ‚Kontaktloses Bezahlen mit Visa', https://www.visa.de/bezahlen-mit-visa/genutzte-technologien/kontaktloses-bezahlen-mit-visa.html.

[18] Siehe, zum Beispiel, Mobile QuickClear, https://mobilepassport.us/#quickclear.

[19] Siehe, zum Beispiel, Nuki, ‚Eintreten in die Smart Home Welt mit Nuki deinem smarten Türschloss für Zuhause', https://nuki.io/de/.

[20] Investigatory Powers Tribunal (IPT), *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, Witness Statement of Eric King (5. Oktober 2015), https://privacyinternational.org/sites/default/files/2018-03/2015.10.05%20Witness_Statement_Of_Eric_King.pdf, S. 10-11. SS. Siehe u.a. Der Spiegel, ‚How the NSA Accesses Smartphone Data' (9. September 2013) https://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html.

[21] Privacy International, ‚Digital stop and search: how the UK police can secretly download everything from your mobile phone' (März 2018), https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf.

einer Vielzahl von sensiblen personenbezogenen Daten oder zu intimen Aspekten des Privatlebens ermöglichen.

Wenn Untersuchungsbehörden einen Straatstrojaner einsezten, können sie Erkenntnisse erlangen, die einen wesentlich tiefgreifenderen Eingriff in die Privatsphäre darstellen, als wenn das Haus der betroffenen Person durchsucht oder abgehört würde, order wenn der Person ein Micro-Chip eingeplanzt worden wäre. Aufgrund der beispiellosen Schwere dieses Eindringens und um sicherzustellen, dass sie nicht gegen den Wesenskern der genannten Rechte verstoßen, brauchen Maßnahmen, an denen sich staatliche Trojaner beteiligen, nur in Fällen eingesetzt zu werden, in denen es sich um schwere Straftaten oder Handlungen handelt, die eine spezifische, ernsthafte Bedrohung für die nationale Sicherheit darstellen. Insbesondere müssen die Ermittlungsbehörden sicherstellen, dass diese Maßnahmen auf das unbedingt Notwendige beschränkt sind, indem sie beispielsweise die Identität der Personen oder die Einzelheiten des Zielsystems so weit wie möglich angeben (siehe Punkt III.a. unten).[22]

## II. Der Einsatz von Staatstrojanern verstößt gegen die Verpflichtung der Staaten, die Sicherheit und Integrität von IT-Systemen wirksam zu gewährleisten

Die Ausübung des Rechts auf Privatsphäre ist mit der Sicherheit der Geräte, Netzwerke und Dienste verbunden, auf die sich Personen verlassen, um miteinander zu kommunizieren. Dementsprechend sind die Auswirkungen von Maßnahmen wie Staatstrojaner auf die Sicherheit für eine Bewertung des Umfangs und der Art der Einschränkung des Rechts auf Privatsphäre durch diese Maßnahme relevant.

Der UN-Sonderberichterstatter zur Meinungsfreiheit hat erklärt, dass Personen ihr Recht auf Privatsphäre auf eine „private" und „sichere" Kommunikationsweise ausüben.[23] Der Sonderberichterstatter hat diese Begriffe wie folgt definiert:

> „Die Geheimhaltung der Kommunikationen führt dazu, dass Personen in einem Raum, der für andere Mitglieder der Gesellschaft, des Privatsektors und letztlich des Staates selbst unerreichbar ist, Informationen und Ideen austauschen können. Sicherheit der Kommunikationen bedeutet, dass Personen in der Lage sein sollten, zu überprüfen, ob ihre Kommunikationen nur von ihren beabsichtigten Empfängern empfangen werden, ohne

[22] Vgl. Privacy International, 'Hacking Safeguards and Legal Commentary' (Juni 2018) https://privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary#3.

[23] Bericht des UN-Sonderberichterstatters zur Meinungsfreiheit (A/HRC/23/40, 17. April 2013), Ziff 23.

> Beeinträchtigung oder Veränderung, und dass die Kommunikationen, die sie empfangen, ebenso frei von Beeinträchtigungen sind."[24]

Der Sonderberichterstatter hat auch den Zusammenhang zwischen dem Recht auf Privatsphäre und Sicherheit erläutert und festgestellt, dass Personen, die "E-Mail, Instant Messaging, Voice-over-Internet-Protokolle, Videokonferenzen und Social Media"[25] nutzen, "ein Bedürfnis nach Sicherheit im Internet entwickelt haben, so dass sie Informationen suchen, empfangen und weitergeben können, ohne das Risiko von Auswirkungen, Offenlegung, [oder] Überwachung".[26] Der Sonderberichterstatter stellte weiter fest, dass es "entscheidend ist, dass Einzelpersonen Wege finden, sich online zu schützen, dass Regierungen eine solche Sicherheit in Recht und Politik bieten und dass Unternehmen sichere Produkte und Dienstleistungen entwerfen, entwickeln und vermarkten".[27] Der Sonderberichterstatter kam zu dem Schluss, dass "die Staaten alle Maßnahmen vermeiden sollten, die die Sicherheit, die Einzelpersonen online genießen können, schwächen".[28]

Der Sonderberichterstatter hat auch die wichtige Rolle hervorgehoben, die Unternehmen sowohl bei "den Veränderungen in der Art und Weise, wie wir Informationen kommunizieren, empfangen und weitergeben"[29] als auch bei der Erleichterung der "staatlichen Kommunikationsüberwachung"[30] spielen, unter anderem durch "Reaktion auf die Anforderungen, dass digitale Netze und Kommunikationsinfrastrukturen so konzipiert sein müssen, dass sie ein Eindringen des Staates ermöglichen".[31] Der Sonderberichterstatter erkannte daher an, dass die Staaten "ihren internationalen Menschenrechtsverpflichtungen nachkommen müssen, wenn sie mit Unternehmensvertretern Verträge abschließen oder Gesetze erlassen, die sich auf die Wahrnehmung der Menschenrechte auswirken können",[32] und "sicherstellen müssen, dass der Privatsektor in der Lage ist, seine Aufgaben unabhängig und in einer Weise wahrzunehmen, die die Menschenrechte des Einzelnen fördert".[33] Der Sonderberichterstatter kam zu dem Schluss, dass "die Staaten davon absehen müssen, den Privatsektor zu zwingen, Maßnahmen zu

[24] Ibid.
[25] Bericht des UN-Sonderberichterstatters zur Meinungsfreiheit (A/HRC/29/32, 22 May 2015), Ziff. 6.
[26] Ibid.
[27] Ibid, Ziff. 11.
[28] Ibid, Ziff. 60.
[29] Bericht des UN-Sonderberichterstatters zur Meinungsfreiheit (A/HRC/23/40, 17 April 2013), Ziff. 72-74.
[30] Ibid.
[31] Ibid.
[32] Ibid, Ziff. 76-77.
[33] Ibid,

ergreifen, die die Privatsphäre und Sicherheit der Kommunikationsdienste gefährden".[34]

Grundsätzlich geht es beim Einsatz von Staatstrojanern darum, Technologien dazu zu bringen, sich so zu verhalten, wie es der Hersteller, Eigentümer oder Benutzer nicht beabsichtigt oder vorhergesehen hat. Ein einzelner Hack kann viele Menschen betreffen, einschließlich solcher, die zufällig oder in keinem Zusammenhang mit einer Untersuchung oder Operation stehen. Mit anderen Worten geht es bei Staatstrojanern darum, Schwachstellen in der Computersicherheit - oft auf kreative Weise - auszunutzen/zu erkunden.[35]

Das Bundesverfassungsgericht (BVerfG) hat ein Recht auf Gewährleistung der Vertraulichkeit und Integrität von informationstechnischen Systemen anerkannt. In seiner Entscheidung vom 27.02.2008 - 1 BvR 370/07 und 1 BvR 595/07 - hat das Gericht geklärt:

> „Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informations-technischer Systeme ist hingegen anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, das sein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden. Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen. Der spezifische Grundrechtsschutz erstreckt sich ferner beispielsweise auf solche Mobiltelefone oder elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können."[36]

---

[34] Ibid, Ziff. 96 (unter Hinweis auf das Büro des Hohen Kommissars für Menschenrechte, ‚Leitprinzipien für Wirtschaft und Menschenrechte', 2011); siehe u.a. Bericht des UN-Sonderberichterstatters zur Meinungsfreiheit (A/HRC/29/32, 22. Mai 2015), Ziff. 28.

[35] Vgl. U.S. District Court, Central District of California (Eastern Division), In the matter of the search of an apple iPhone seized during the execution of a search warrant on a black Lexus is300, California license plate 35KGD203, Stellungnahme der Amici Curiae Privacy International und Human Rights Watch, https://privacyinternational.org/sites/default/files/2018-03/Amicus%20Brief%20-%20PI%20and%20HRW.pdf, S. 6-7.

[36] BVerfG, Urteil des Ersten Senats vom 27. Februar 2008, 1BvR370/071 und BvR 595/07, Ziff. 203.

Die EMRK erlegt Staaten auch positive Verpflichtungen auf, die in der Konvention verankerten Rechte, einschließlich des Rechts auf Privatsphäre, zu gewährleisten.[37] Der EGMR hat festgestellt, dass der "Schutz personenbezogener Daten [....] von grundlegender Bedeutung für den Genuss des Rechts einer Person auf Achtung des Privat- und Familienlebens gemäß Artikel 8 der Konvention ist".[38]

Das Recht der EU erlegt den Mitgliedstaaten ähnliche Verpflichtungen auf, die Sicherheit und Integrität der Informationssysteme zu gewährleisten. Insbesondere die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016[39] legt Regeln für die Verarbeitung personenbezogener Daten fest, auch im Rahmen einer Strafuntersuchung.[40] Die Richtlinie, die in deutsches Recht umgesetzt wurde,[41] unterstreicht eine Reihe von Verpflichtungen, die sich in der Notwendigkeit für die Mitgliedstaaten zusammenfassen lassen, die Sicherheit, Integrität und Vertraulichkeit personenbezogener Daten durch geeignete Maßnahmen zu gewährleisten. Artikel 29 (Sicherheit der Verarbeitung) Abs. 1 der Richtlinie lautet:

> Die Mitgliedstaaten sehen vor, dass der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu

[37] Siehe, zum Beispiel, EMRG, *K.U. v. Finnland* (Beschwerde Nr. 2872/02, 2. Dezember 2008), Ziff. 42.
[38] EMRG, *I v. Finnland* (Beschwerde Nr. 20511/03, 17. Juli 2008), Ziff. 38.
[39] Richtlinie 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.
[40] Zum Zusammenspiel zwischen Privatsphäre und Datenschutz, einschließlich der Frage, wie Überwachungstechnologien auch die Datenschutzrechte beeinträchtigen können, siehe Agentur der Europäischen Union für Grundrechte (FRA), *Handbuch zum europäischen Datenschutzrecht* (Ausgabe 2018) https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, S. 20; Juliane Kokott und Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' International Data Privacy Law (Band Nr. 3, Nr. 4, November 2013) S. 222-228; EuGH, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & Others and Seitlinger and Others*, Urteil vom 8. April 2014, Rs. C-293/12 und C-594-12.
[41] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), Bundesgesetzblatt 2017 I, 2097.

> gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten…[42]

Während wir Computersysteme weiterhin in das Gefüge unseres Lebens, unserer Wirtschaft und unserer Gesellschaft integrieren, wird der Schutz der Sicherheit dieser Systeme immer wichtiger. Entgegen diesen Verpflichtungen, um Staatstrojaner einsetzen zu können, müssen Regierungen Sicherheitslücken im System zum Schutz von Computern, Telefonen und Netzwerken induzieren.[43]

Unter Berücksichtigung der Verpflichtungen der Staaten zur Aufrechterhaltung der Integrität und Sicherheit der Informationssysteme, damit der Einzelne seine Grundrechte wirksam ausüben kann, kann die Einleitung von Maßnahmen, die sich auf Staatstrojaner stützen, und die die Sicherheit der Systeme untergraben, als mit den Menschenrechtsbestimmungen unvereinbar angesehen werden. Der Einsatz von Staatstrojanern steht unter solchen Umständen im Widerspruch zu den Verpflichtungen der Staaten, die Privatsphäre und den Datenschutz des Einzelnen zu gewährleisten, indem sie Maßnahmen ergreifen, die die Sicherheit, Integrität und Vertraulichkeit der informationstechnischen Systeme schützen. Von Natur aus erfordert der Einsatz von Staatstrojanern genau das Gegenteil: eine kontinuierliche Untergrabung der Sicherheit.

---

[42] Diese Verpflichtungen werden beispielsweise in Absatz 2 weiter präzisiert, der die Kontrolleure, einschließlich der zuständigen Strafverfolgungsbehörden, verpflichtet, Maßnahmen zu ergreifen, um die Folgendes zu bezwecken: *(a) Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle); (b) Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle); (c) Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle); (f) Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle); (h) Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle); (i) Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellung); (j) Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)* usw.

[43] Vgl. Investigatory Powers Tribunal (IPT), *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, Expert report of Professor Ross Anderson (30. September 2015) https://privacyinternational.org/sites/default/files/2018-03/2015.09.30%20Anderson_IPT_Expert_Report_2015_Final.pdf, S. 17-19; Investigatory Powers Tribunal (IPT), *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, Witness Statement of Eric King (5. Oktober 2015) https://privacyinternational.org/sites/default/files/2018-03/2015.10.05%20Witness_Statement_Of_Eric_King.pdf, S. 22ff.

## III. Der Einsatz von Staatstrojanern darf nicht gegen die Grundsätze der Notwendigkeit und Verhältnismäßigkeit sowohl des internationalen als auch des europäischen Rechts verstoßen

Aufgrund ihres extrem eindringenden Charakters und der damit verbundenen ernsthaften Sicherheitsbedenken an die Privatsphäre und den Datenschutz des Einzelnen kann sich der Einsatz von Staatstrojanern als schwierig erweisen, mit den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit vereinbar zu sein.

### a. Staatstrojaner zum Zwecke der Strafverfolgung müssen auf das unbedingt Notwendige beschränkt werden

Sowohl internationale als auch das europäische Menschenrechtsbestimmungen schreiben vor, dass jede Einschränkung des Rechts auf Privatsphäre notwendig und verhältnismäßig sein muss. Diese Prinzipien wurden in der Resolution des Menschenrechtsrates der Vereinten Nationen über "*das Recht auf Privatsphäre im digitalen Zeitalter*", die im März 2017 im Konsens angenommen wurde, verbindlich bestätigt.[44]

Der Grundsatz der Notwendigkeit "*impliziert, dass Beschränkungen nicht einfach nützlich, vernünftig oder wünschenswert sein dürfen, um ein legitimes Regierungsziel zu erreichen*", sondern dass "*ein Staat ‚auf spezifische und individualisierte Weise die genaue Art der Bedrohung*', die er anzugehen versucht, und einen ‚*direkten und unmittelbaren Zusammenhang zwischen der Freiheit und der Bedrohung' nachweisen muss*".[45]

Der EGMR hat den Grundsatz der strikten Notwendigkeit auch auf Überwachungsmaßnahmen angewandt, die das Recht auf Privatsphäre einschränken. In *Szabó und Vissy*[46] wies der Gerichtshof darauf hin, angesichts des "Potenzials modernster Überwachungstechnologien, in die Privatsphäre der Bürger einzudringen":

> „Eine Maßnahme der geheimen U berwachung kann nur dann der Konvention entsprechen, wenn sie – als allgemeine U berlegung – zur Erhaltung der

[44] UN-Menschenrechtsrat, Das Recht auf Privatsphäre im digitalen Zeitalter (A/HRC/34/L.7/Rev.1, 22. März 2017), Ziff. 2 ("*Daran erinnern, dass Staaten sicherstellen sollten, dass jede Beeinträchtigung des Rechts auf Privatsphäre mit den Grundsätzen der Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit vereinbar ist*").

[45] CCPR, General Comment Nr. 34 (CCPR/C/GC/34, 12. September 2011), Ziff. 35.

[46] EGMR, *Szabó und Vissy v. Ungarn* (Beschwerde Nr. 37138/14, 12. Januar 2016), Ziff. 73.

> demo- kratischen Einrichtungen unbedingt notwendig ist und wenn sie außerdem – als spezielle U berlegung – unbe- dingt notwendig ist, um in einer konkreten Operati- on entscheidende Informationen zu erlangen. Nach Ansicht des GH wird jede Maßnahme der geheimen U berwachung, die diesen Kriterien nicht entspricht, fu r Missbrauch durch die Beho rden anfa llig sein, denen beachtliche Technologien zur Verfu gung stehen."[47]

Auch im Zusammenhang mit Maßnahmen zur Datenspeicherung hat der Gerichtshof der EU entschieden, dass diese Maßnahmen Voraussetzungen unterliegen müssen, die in der Prxis geeignet sind, "*den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen*".[48]

Wie in Punkt 1 oben bereits erwähnt, können Staatstrojaner einen allgemeinen Echtzeitzugang der Ermittlungsbehörden nicht nur zu den Kommunikationsdaten und dem Inhalt der Kommunikation einer Person, sondern auch zu den intimsten Aspekten ihres Privatlebens ermöglichen, da die Behörden in der Lage sind, in Echtzeit in die Privatsphäre einer Person einzugreifen, indem sie nicht nur auf kommunizierte Fotos, Videos, Tagebücher, Notizen und andere sensible oder personenbezogene Daten zugreifen können, die auf ihrem Gerät gespeichert sind, sondern auch Mikrofone, Kameras, GPS-Tracking und andere Sensoren heimlich aktivieren können.

Moderne mobile Betriebssysteme können von mehreren Nutzern (oder mehreren Benutzerprofilen, die einem oder mehreren Nutzern entsprechen können), genutzt werden. Es ist daher schwierig für Regierungsbehörden eine Zielperson genau zu lokalisieren, auch wenn die Überwachung auf ein bestimmtes Gerät gerichtet ist. So kann sich beispielsweise die IP-Adresse eines Gerätes auf mehr als eine Person beziehen, die das gleiche Netzwerk nutzt. Dies kann unweigerlich dazu führen, dass Ermittlungsbehörden auf eine Fülle von Informationen über das Privatleben von Personen zugreifen, die nicht unter strafrechtlichen Ermittlungen stehen. [49]

Ausgehend von den oben genannten Überlegungen stellt Privacy International stark in Frage, ob der Einsatz von Staatstrojanern jemals notwendig und verhältnismäßig geregelt werden kann.

---

[47] Ibid.

[48] EuGH, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson, Urteil vom 21. Dezember 2016, Rs. C–203/15 und C–698/15, Ziff. 110.

[49] Vgl. U.S. Court of Appeals, U.S.A. v. Alex Levin, Brief of Amicus Curiae Privacy International in support of Defendant-Appellee and in support of affirmance of the decision below (Nr. 16-1567, 10. Februar 2017) https://privacyinternational.org/sites/default/files/2018-10/2017.02.10_DOCKETED_Amicus_Brief.pdf. In diesem Fall wurden Staatstrojaner von der Strafverfolgungsbehörde eingesetzt, um eine große Anzahl von Menschen zu erreichen.

Zumindest sollte der Einsatz von Staatstrojanern als Verletzung des Notwendigkeitsprinzips betrachtet werden, es sei denn, sie sind auf das unbedingt Notwendige beschränkt. Insbesondere müssen Regierungen vor der Durchführung dieser Hacking-Maßnahme mindestens Folgendes festlegen:

(i) Ein hoher Grad an Wahrscheinlichkeit, dass:
1. eine schwere Straftat begangen wurde oder Handlung(en) vom Gewicht einer spezifischen, schwerwiegenden Bedrohung der nationalen Sicherheit begangen werden wird;
2. das IT-System, das von der Person verwendet wird, die verdächtigt wird, die schwere Straftat oder Handlung(en) zu begehen, die eine spezifische, ernste Bedrohung für die nationale Sicherheit darstellen, enthält wahrscheinlich Beweise, die für die schwere Straftat oder Handlung(en), die eine spezifische, ernste Bedrohung für das angebliche nationale Sicherheitsinteresse darstellen, relevant und wesentlich sind;
3. Beweise, die für die schwere Straftat oder die schweren Handlungen, die eine spezifische, ernste Bedrohung für das angebliche nationale Sicherheitsinteresse darstellen, relevant und wesentlich sind, werden durch Hacking des Zielsystems gewonnen;

(ii) dass so weit wie möglich die Person, die verdächtigt wird, dass sie die schwere Straftat oder Handlung(en) begangen hat, die eine spezifische, ernsthafte Bedrohung für die nationale Sicherheit darstellt, eindeutig identifiziert wird wie auch die Details des Zielsystems, einschließlich seines Standorts und seiner spezifischen Konfigurationen;

(iii) dass alle weniger eindringenden Methoden erschöpft wurden, oder sinnlos wären, sodass der Einsatz von Staatstrojanern die am wenigsten eindringende Option ist;

(iv) die Methode, den Umfang und die Dauer der vorgeschlagenen Maßnahme;

(v) dass der Zugriff auf und die Sammlung von Daten beschränkt wird auf jene, die für schwere Straftaten oder Handlungen, die eine spezifische, schwerwiegende Gefahr für die nationale Sicherheit begründen, relevant und wesentlich sind, und dass Maßnahmen ergriffen werden, um den Zugriff auf und die Sammlung von irrelevanten und unwesentlichen Daten zu minimieren;

(vi) dass die Daten nur von der angegebenen Behörde abgerufen und gesammelt werden und nur für den Zweck und die Dauer, für die die Genehmigung erteilt wird, verwendet und weitergegeben werden.

Privacy International hat eine Reihe von Sicherheitsvorkehrungen festgelegt, die mit dem staatlichen Hacking verbunden sein müssen, wenn es durchgeführt werden soll.[50]

### b. Staatstrojaner nutzen bevorratete Systemschwachstellen, deren Risiko für die Rechte des Einzelnen nicht in einem angemessenen Verhältnis zu dem in einer einzigen strafrechtlichen Untersuchung angestrebten Nutzen stehen kann

Der UN-Sonderberichterstatter für Terrorismusbekämpfung und Menschenrechte hat den Staaten zusätzliche Leitlinien für den Nachweis der Verhältnismäßigkeit im Rahmen der Kommunikationsüberwachung gegeben. Er hat geltend gemacht, dass "*Verhältnismäßigkeit darin besteht, das Ausmaß des Eingriffs in die Datenschutzrechte im Internet gegen den spezifischen Nutzen abzuwägen, der sich aus den Untersuchungen einer Behörde im öffentlichen Interesse ergibt*".[51] Er hat auch darauf hingewiesen, dass *"[i]m Rahmen der geheimen Überwachung ... [d]ie Verhältnismäßigkeit einer Beeinträchtigung des Rechts auf Privatsphäre [ ] nach den besonderen Umständen des Einzelfalls beurteilt werden [sollte]."*[52]

Bei der Beurteilung, ob in einer demokratischen Gesellschaft eine Beeinträchtigung des Rechts auf Privatsphäre notwendig ist, prüft der EGMR auch, ob die Beeinträchtigung im Verhältnis zu den verfolgten Zielen steht. Dabei handelt es sich zwangsläufig um einen Ausgleich zwischen konkurrierenden Interessen.[53] In diesem Zusammenhang genießen die nationalen Behörden "*einen Ermessensspielraum, dessen Umfang nicht nur von der Art des angestrebten legitimen Ziels, sondern auch von der Besonderheit der betreffenden Beeinträchtigung abhängig sein wird*".[54]

In *S. und Marper*[55] befasste sich der EGMR mit der Speicherung von DNA-Profilen zum Zwecke der Aufdeckung und Verfolgung von Verbrechen. Er stellte fest:

> „Der Gerichtshof weist darauf hin, dass der durch Artikel 8 der Konvention gewährte Schutz unannehmbar geschwächt wäre, wenn der Einsatz moderner wissenschaftlicher Techniken im Strafrechtssystem um jeden Preis und ohne ein sorgfältiges Abwägen der potenziellen Vorteile einer umfassenden

---

[50] Privacy International, ‚Hacking Safeguards and Legal Commentary' (Juni 2018) https://privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary#3.

[51] Berict des UN-Sonderberichterstatters zu Menschenrechten bei der Bekämpfung von Terrorismus (A/69/397, 23. September 2014), Ziff. 51.

[52] Ibid.

[53] EMRG, *Z v. Finnland* (Beschwerde Nr. 22009/93, 25. Februar 1997), Ziff. 94.

[54] EMRG, *Leander v. Schweden* (Beschwerde Nr. 9248/81, 26. März 1987), Ziff. 59.

[55] EMRG, *S. and Marper v. das Vereinigte Königreich* (Beschwerde Nr. 30562/04 und 30566/04, 4. Dezember 2008).

> Nutzung solcher Techniken gegenüber wichtigen Privatlebensinteressen zugelassen würde. Nach Ansicht des Gerichts ist der in dieser Hinsicht zwischen den Vertragsstaaten herrschende starke Konsens von erheblicher Bedeutung und verengt den Ermessensspielraum, der dem beklagten Staat bei der Beurteilung der zulässigen Grenzen der Beeinträchtigung des Privatlebens in diesem Bereich bleibt. Der Gerichtshof ist der Auffassung, dass jeder Staat, der eine Vorreiterrolle bei der Entwicklung neuer Technologien beansprucht, eine besondere Verantwortung dafür trägt, in dieser Hinsicht das richtige Gleichgewicht zu finden."[56]

Der Einsatz von Staatstrojanern beruht auf der Ausnutzung von Systemschwachstellen durch die Ermittlungsbehörden, wie beispielsweise Zero-day-Schwachstellen. Eine 0-Tage-Schwachstelle bezieht sich auf einen Sicherheitsfehler in einer Software, der dem Anbieter unbekannt ist.[57] 0-Tage-Schwachstellen erhalten ihren Namen von der Tatsache, dass der Systemhersteller, wenn sie identifiziert werden, "0 Tage" Zeit hat, diese zu beheben, bevor Angreifer die Schwachstellen ausnutzen können. Wenn Forscher, White-Hat-Hacker und andere Schwachstellen entdecken, melden sie den Fehler in der Regel an das für die Sicherheit der betroffenen Software verantwortliche Unternehmen.

Wenn Regierungen 0-Tage-Schwachstellen nutzen, stehen sie vor einer Dichotomie - sollten sie 0 Tage lagern oder horten, um eine Hacking-Maßnahme durchzuführen, die möglicherweise zu einem erfolgreichen Strafverfahren führen könnte, oder sollten sie den Verkäufer benachrichtigen und ihn bitten, die Schwachstelle für das Allgemeinwohl zu beheben? Wenn es den Behörden erlaubt ist, solche Lücken auszunutzen, werden sie eher ein Interesse daran haben, ein "Arsenal" von Sicherheitslücken aufzubauen, um im Falle einer Untersuchung ein Ziel angreifen zu können. Dieses Interesse wiederum wird sie daran hindern, den betroffenen Hersteller von IT-Systemen zu informieren, der dazu beitragen kann, die entdeckte Sicherheitslücke zu schließen. Dies bedeutet in diesem Fall, dass das breitere und weltweite Sicherheitsrisiko die mögliche Erleichterung der Strafverfolgung im Einzelfall bei weitem überwiegen würde.[58]

---

[56] Ibid, Ziff. 112.

[57] Vgl. Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W. W. Norton & Company, 2015) ("Nicht veröffentlichte Schwachstellen werden als "Zero-Day"-Schwachstellen bezeichnet; sie sind sehr anfällig für Angreifer, da niemand vor ihnen geschützt ist, und sie können weltweit ungestraft verwendet werden.").

[58] Siehe Investigatory Powers Tribunal (IPT), *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, Expert report of Professor Ross Anderson (30. September 2015) https://privacyinternational.org/sites/default/files/2018-03/2015.09.30%20Anderson_IPT_Expert_Report_2015_Final.pdf, S. 8.

Schwachstellen werden heutzutage für sechsstellige Summen verkauft.[59] Regierungen sind zu einigen der größten Entwickler und Käufer von Informationen geworden, die 0-Tage identifizieren. [60] In den meisten Fällen zögern die Regierungen, diese nach dem Kauf von 0 Tagen den Softwareherstellern offen zu legen, da die Sicherheitslücke dann repariert werden könnte, was den Zugang der Regierung einschränkt. Regierungen riskieren daher die Sicherheit ihrer eigenen Bürger und Unternehmen zuwiderlaufen.[61] Leider riskieren Nachrichtendienste jedes Mal, wenn sie einen 0-Tage-Angriff nutzen, auch die Entdeckung durch Kriminelle und andere ausländische Geheimdienste und Akteure, die ihn gegen Staatsbürger einsetzen könnten. [62]

Cyberangriffe unterstrichen, dass das Horten von Systemschwachstellen lästige Folgen für die Bürger weltweit haben kann. [63] WannaCry z.B. wurde von Hackern entwickelt, die es geschafft haben, die von der National Security Agency (NSA) der Vereinigten Staaten gehorteten Schwachstellen effektiv zu nutzen, und die die europäische Infrastrukturbetreiber in den Bereichen Gesundheit, Energie, Verkehr, Finanzen und Telekommunikation schwer getroffen haben.[64]

Deutschland und das Vereinigte Königreich gehörten zu den ersten Ländern, in denen der WannaCry-Angriff gemeldet wurde. Nach Angaben der Berliner Staatsanwaltschaft waren nach dem Anschlag WannaCry insgesamt 450 Computer der Deutschen Bahn betroffen.[65] In Großbritannien hatte der WannaCry- Angriff potenziell schwerwiegende Auswirkungen auf das nationale Gesundheitswesen, was zu einer weit verbreiteten Störung bei mindestens 81 von 236 Krankenhauskonzernen in England führte, wobei 19.000 Arzttermine abgesagt wurden, Computer bei 600

---

[59] Ibid, S. 10.

[60] David E. Sanger, 'Obama Lets NSA Exploit Some Internet Flaws, Officials Say' (The New York Times, 12. April 2014) https://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html?_r=1.

[61] Sean Gallagher, 'NSA secretly hijacked existing malware to spy on N. Korea, others' (ArsTechnica, 19. Januar 2015) http://arstechnica.com/informationPtechnology/2015/01/nsa-secretly-hijacked-existing-malware-to-spy-on-n-korea-others.

[62] Vgl. Sven Herpig, 'A Framework for Government Hacking in Criminal Investigations' (Stiftung Neue Verantwortung, Oktober 2018) https://www.stiftung-nv.de/sites/default/files/framework_for_government_hacking_in_criminal_investigations.pdf.

[63] Linus Neumann, '"WannaCry"-Cyberattacke Die Lehren aus dem weltweit größten Angriff mit Erpressungssoftware' (Spiegel Online, 15. Mai 2017) https://www.spiegel.de/netzwelt/web/wannacry-die-lehren-aus-dem-cyberangriff-a-1147589.html.

[64] Agentur der Europäischen Union für Grundrechte (FRA), Fundamental Rights Report 2018, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf, S. 161.

[65] Markus Böhm, 'Experten über "WannaCry"-Attacke: "Wir hatten noch Glück"' (16. Mai 2017) https://www.spiegel.de/netzwelt/web/wannacry-450-bahn-computer-von-cyber-attacke-betroffen-a-1147921.html.

Hausarztpraxen gesperrt wurden und fünf Krankenhäuser Krankenwagen anderweitig schicken mussten.[66] Dies führte zu chaotischen Situationen für Patienten, deren vertrauliche, personenbezogene Daten durch die Malware verschlüsselt oder zerstört wurden.[67]

Die Erfassung von Systemschwachstellen durch den Staat für den Einsatz von Staatstrojanern ist unverhältnismäßig. Selbst wenn die Überwachung durch staatliche Trojaner im Rahmen legitimer Ziele wie gezielte Strafverfolgungen erfolgt, darf dies die Privatsphäre und die Sicherheitsinteressen von Personen nicht überwiegen, deren sensible personenbezogene Daten durch die Ausbeutung durch Dritte gefährdet werden. [68]

## Fazit

Insgesamt stellen Staatstrojaner einzigartige und schwerwiegende Bedrohungen für die Privatsphäre und Sicherheit dar. Staatstrojaner, die auf Systemschwachstellen oder "0-Tagen" basieren, sollten nicht verwendet werden, es sei denn, diese Risiken können vollständig gemindert werden.

Durchführungsmaßnahmen, die sich auf Staatstrojaner stützen, gefährden aufgrund ihrer enormen Eingriffstiefe den Wesenskern der Grundrechte, wie beispielsweise des Rechts auf Privatsphäre und Datenschutz.

Sich auf Staatstrojaner zu verlassen, die Sicherheitsschwachstellen ausnutzen, steht auch im Widerspruch zu den Verpflichtungen von Staaten, die Integrität und Sicherheit von Informationssystemen sowohl nach internationalen als auch nach EU-Rechtsstandards zu gewährleisten.

Der Einsatz von Staatstrojanern muss nach den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit sorgfältig geprüft werden. Der aktuelle Stand der Trojaner-Technologie macht es sehr schwierig, eine Untersuchung auf das unbedingt Notwendige zu beschränken. Darüber hinaus kann die Ausnutzung von Schwachstellen zur Erleichterung von Staatstrojanern nicht verhältnismäßig sein und

---

[66] Britischer Rechnungshof, Gesundheitsministerium, ‚Investigation: WannaCry cyber-attack and the NHS' (Report by the Controller and Auditor General, 27. Oktober 2017) https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

[67] Zeit Online, 'WannaCry: Microsoft gibt US-Regierung Mitschuld an Hackerangriff' (15. Mai 2017) https://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung.

[68] Vgl. Sven Herpig, 'Schwachstellen- Management für mehr Sicherheit: Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte' (Stiftung Neue Verantwortung, August 2018) https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf.

würde somit sowohl gegen internationale als auch gegen europäische Menschenrechtsstandards verstoßen, wenn sie die staatliche Ausnutzung von Schwachstellen gegen das allgemeine Sicherheitsrisiko für die Gesellschaft abwägt.

30. September 2019

Privacy International
62 Britton Street
London EC1M 5UY
+44 (0) 20 3422 4321




**Privacy International**
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

**UK Registered Charity No. 1147471**