



Ausarbeitung

**Zur menschenrechtlichen Schutzpflicht von Staaten bei der
Exportkontrolle digitaler Überwachungstechnologie**

Zur menschenrechtlichen Schutzpflicht von Staaten bei der Exportkontrolle digitaler Überwachungstechnologie

Aktenzeichen: WD 2 - 3000 - 058/21
Abschluss der Arbeit: Datum: 13. September 2021 (zugleich letzter Zugriff auf die Internetlinks)
Fachbereich: WD 2: Auswärtiges, Völkerrecht, wirtschaftliche Zusammenarbeit und Entwicklung, Verteidigung, Menschenrechte und humanitäre Hilfe

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

Inhaltsverzeichnis

1.	Fragestellung	4
2.	Spezielle völkerrechtliche Regelungen	4
3.	Menschenrechtliche Regelungen zum Schutz des Rechts auf Privatsphäre	5
3.1.	Das Menschenrecht auf Privatsphäre	5
3.2.	Zurechnungsfragen	6
3.3.	Menschenrechtliche Schutzpflicht	7
4.	Fazit	13

1. Fragestellung

Nach den Ergebnissen eines internationalen Rechercheteams wurden offenbar weltweit Journalisten, Oppositionelle, Menschenrechtsaktivisten und Politiker durch das Spionage- und Abhörprogramm „Pegasus“ abgehört.¹ Die entsprechende Software wird von dem privaten israelischen Softwareunternehmen *NSO Group* hergestellt und sollte nach Angaben der israelischen Regierung und des Herstellers ausschließlich bei der Verfolgung von Terroristen und Kriminellen helfen.² Die Software wurde auch an verschiedene Regierungen autoritärer Staaten verkauft. Der Auftraggeber/die Auftraggeberin fragt vor diesem Hintergrund, ob die israelische Regierung eine Mitverantwortung trägt, wenn ein Unternehmen aus ihrem Land für die weltweite Verbreitung eines Abhörprogramms, welches auch für illegale Spionagetätigkeiten genutzt wurde, verantwortlich ist.

2. Spezielle völkerrechtliche Regelungen

Spionage als solche ist völkerrechtlich nicht verboten.³ Internationale Verträge bzw. Konventionen, die privaten Unternehmen verbieten, Software zur Spionage zu verkaufen, existieren nicht. Auch **verbindliche globale Vorgaben zum Export von digitaler Überwachungssoftware fehlen** bislang.⁴ Mit dem sogenannten *Wassenaar Arrangement für Exportkontrollen von konventionellen Waffen und doppelverwendungsfähigen Gütern und Technologien* haben zwar bereits 42 Staaten eine multilaterale Vereinbarung getroffen, mit dem Ziel, durch gemeinsame und globale Ausfuhrkontrollstandards „destabilisierende Waffenanhäufungen“ zu verhindern und mehr Transparenz beim Export von Rüstungsgütern und Dual-Use-Gütern herzustellen.⁵ Seit 2013 gehört zudem auch Überwachungstechnologie zu den sogenannten Dual-Use-Technologien im Sinne des Abkommens. Jedoch hat sich das *Wassenaar-Arrangement* als wenig wirksam erwie-

1 Siehe dazu etwa Süddeutsche Zeitung vom 18. Juli 2021, „Das Pegasus-Projekt. Cyberangriff auf die Demokratie“, <https://projekte.sueddeutsche.de/artikel/politik/pegasus-project-die-uebersicht-e642044/>.

2 Tagesschau.de vom 19. Juli 2021, „NSO Group. Die Trojaner-Schmiede“, <https://www.tagesschau.de/investigativ/ndr-wdr/spionage-software-pegasus-nso-101.html>.

3 *Stefan Talmon*, „Sachverständigen Gutachten gemäß Beweisbeschluss SV-4 des 1. Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode“, S. 18, https://www.bundestag.de/resource/blob/282872/2b7b605da4c13cc2bc512c9c899953c1/mat_a_sv-4-2_talmon-pdf-data.pdf.

4 Auf europäischer Ebene wurde am 11. Juni 2021 die neue EU Dual-Use-Verordnung veröffentlicht, die auch Vorgaben zum Export digitaler Überwachungsindustrie enthält.

5 Siehe dazu Website des Auswärtigen Amtes, Internationale Exportkontrollen, Stand: 20. August 2019, <https://www.auswaertiges-amt.de/de/aussenpolitik/themen/aussenwirtschaft/exportkontrolle-international/213174>.

sen, da es **rechtlich nicht bindend** ist und es an einem Durchsetzungsmechanismus zur Einhaltung der Ausführstandards fehlt.⁶ **Israel hat das Wassenaar-Arrangement zudem nicht unterzeichnet.**

3. Menschenrechtliche Regelungen zum Schutz des Rechts auf Privatsphäre

Obgleich keine speziellen verbindlichen völkerrechtlichen Vorgaben hinsichtlich des Exports von digitaler Überwachungstechnologie existieren, bleiben die Staaten an die von ihnen ratifizierten internationalen Menschenrechtsverträge gebunden. Vor diesem Hintergrund soll im Folgenden der Schutzbereich des in diesem Zusammenhang einschlägigen Menschenrechts auf Privatsphäre skizziert werden (3.1) und dargelegt werden, warum potentielle Menschenrechtsverletzungen im vorliegenden Falle nicht dem israelischen Staat zugerechnet werden können (3.2). Da die Staaten jedoch verpflichtet sind, die Menschenrechte vor einem Missbrauch durch Dritte zu schützen, wird schließlich die menschenrechtliche Schutzpflicht von Staaten insbesondere im Zusammenhang mit dem Export von digitaler Überwachungstechnologie näher betrachtet (3.3.).

3.1. Das Menschenrecht auf Privatsphäre

Das Menschenrecht auf Privatsphäre ist in Art. 17 des *Internationalen Pakts über Bürgerliche und Politische Rechte* vom 16. Dezember 1966 (ICCPR – VN-Zivilpakt) verankert.⁷ Der VN-Zivilpakt wurde von Israel am 3. Oktober 1991 ratifiziert.⁸ Seine Bestimmungen sind damit grundsätzlich anwendbar.

Das Recht auf Achtung des Privatlebens gemäß Art. 17 des VN-Zivilpakts soll unter anderem alle natürlichen Personen im Anwendungsbereich des Paktes **vor der unrechtmäßigen oder willkürlichen Überwachung und Aufzeichnung der privaten Kommunikation schützen.**⁹ Der VN-Menschenrechtsausschuss sowie die VN-Generalversammlung haben mehrfach klargestellt, dass auch im digitalen Zeitalter der Schutz der Privatsphäre gewährleistet und rechtlich verankert sein

6 Siehe *Steven Feldstein*, „Governments Are Using Spyware on Citizens. Can They Be Stopped?“, Carnegie Endowment for International Peace, 21. Juli 2021, https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stop_ped-pub-85019.

7 Vgl. Gutachten der Wissenschaftlichen Dienste des Deutschen Bundestages, „Menschenrechte im digitalen Zeitalter“, WD 2-107-18 vom 3. August 2018, <https://www.bundestag.de/resource/blob/568306/39edaff23c4b48b1bee67944a169df27/WD-2-107-18-pdf-data.pdf>.

8 Zum Ratifikationsstand siehe: <https://indicators.ohchr.org/>.

9 Vgl. *Sarah Joseph/Melissa Castan*, „The International Covenant on Civil and Political Rights – Cases, Materials, and Commentary“, 3. Aufl., 2013 Oxford University Press, S. 547.
Siehe auch: Menschenrechtsausschuss der Vereinten Nationen (VN-Menschenrechtsausschuss), General Comment Nr. 16 vom 8. April 1988, Ziffer 10, <https://www.refworld.org/docid/453883f922.html>.

muss und der Begriff „Korrespondenz“ daher auch die elektronische Kommunikation erfasst.¹⁰ Das Recht auf den Schutz der Privatsphäre und der Korrespondenz umfasst daher auch das Recht auf den **Schutz personenbezogener Daten**.¹¹ Grundsätzlich kann jedes (unautorisierte) Erfassen von Kommunikationsdaten, einschließlich des Speicherns und Sammelns, unabhängig davon, ob diese auch tatsächlich verwendet werden, einen potenziellen Eingriff in das Recht auf Privatsphäre darstellen.¹² Die vorliegend betroffenen Personen (bspw. Politiker, Aktivisten, Journalisten) wurden durch die jeweiligen Staaten/autoritären Regime offenbar digital überwacht, d.h. ihre Kommunikation, Standorte und sonstigen digitalen Aktivitäten wurden wahrscheinlich abgefangen, sodass der Schutzbereich von Art. 17 VN-Zivilpakt betroffen wäre.

3.2. Zurechnungsfragen

Festzuhalten ist zunächst, dass **Israel nicht unmittelbar die Verantwortung für menschenrechtswidrige Überwachungsmaßnahmen in Drittstaaten** zugerechnet werden kann, nur weil die Spionagesoftware zuvor aus Israel importiert worden ist.¹³

Unabhängig von der Frage, ob das israelische Softwareunternehmen nach dem Export der Spionagesoftware Pegasus selbst auch unmittelbar an den potentiell unrechtmäßigen Überwachungsangriffen beteiligt war¹⁴, bzw. Sorgfaltspflichten nicht eingehalten wurden, können auch die

-
- 10 Siehe etwa VN-Generalversammlung, A/RES/68/167 vom 18. Dezember 2013, „Das Recht auf Privatheit im digitalen Zeitalter“, <https://undocs.org/A/RES/68/167>.
Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte, A/HRC/27/37 vom 30. Juni 2014, „Das Recht auf Privatheit im digitalen Zeitalter“, <https://www.un.org/depts/german/menschenrechte/a-hrc-27-37.pdf>.
Ausführlich zur Entwicklung des Menschenrechtsschutzes und -diskurses zum Recht auf Privatsphäre siehe: Gutachten der Wissenschaftlichen Dienste des Deutschen Bundestages, „Menschenrechte im digitalen Zeitalter“, WD 2-107-18 vom 3. August 2018, S. 33 ff., <https://www.bundestag.de/resource/blob/568306/39edaff23c4b48b1bee67944a169df27/WD-2-107-18-pdf-data.pdf>.
Siehe auch *Sarah Joseph/Melissa Castan*, „The International Covenant on Civil and Political Rights – Cases, Materials, and Commentary“, 3. Aufl., 2013 Oxford University Press, S. 547.
- 11 *Stefan Talmon*, „Sachverständigengutachten gemäß Beweisbeschluss SV-4 des 1. Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode“, S. 6, https://www.bundestag.de/resource/blob/282872/2b7b605da4c13cc2bc512c9c899953c1/mat_a_sv-4-2_talmon-pdf-data.pdf;
Sarah Joseph/Melissa Castan, „The International Covenant on Civil and Political Rights – Cases, Materials, and Commentary“, 3. Aufl., 2013 Oxford University Press, S. 559 f.
- 12 Vgl. *Walter Kälin/Jörg Künzli*, *Universeller Menschenrechtsschutz. Der Schutz des Individuums auf globaler und regionaler Ebene*, Basel: Helbing Lichtenhein Verlag, 3. Aufl. 2013, S. 446.
Siehe auch: *Christine Kaufmann/Sabrina Ghelmini/Gabriela Medici/Fanny Pulver*, „Das Recht auf Privatsphäre im digitalen Zeitalter – Staatliche Schutzpflichten bei Aktivitäten von Unternehmen“, Schweizerisches Kompetenzzentrum für Menschenrechte, Bern, 2016, S. 11.
- 13 Siehe dazu *Daniel Mossbrucker*, „Kriterien für die Exportkontrolle von Überwachungstechnologie zum wirksamen Schutz der Privatheit sowie der Meinungs- und Pressefreiheit“, *Humanitäres Völkerrecht*, 2018, S. 69-91 (82).
- 14 Vgl. zur Klage von WhatsApp und dem Vorwurf der Beteiligung der NSO Group: *Süddeutsche Zeitung* vom 30. Oktober 2019, „NSO-Trojaner Pegasus: Spionage-Krimi um WhatsApp“, <https://www.sueddeutsche.de/digital/whatsapp-nso-1.4662492>.

Handlungen der *NSO Group* **nicht** dem Staat **Israel zugerechnet** werden. Denn in der völkerrechtlichen Praxis ist nach Art. 8 des ILC-Entwurfs zur Staatenverantwortlichkeit – der gewohnheitsrechtlich gilt - das Handeln privater Akteure einem Staat nur dann zurechenbar, „wenn die Person oder Personengruppe in der Ausführung des Verhaltens tatsächlich auf Anweisung oder unter der Leitung oder Kontrolle dieses Staates handelt.“¹⁵ Anhaltspunkte, dass die *NSO Group* im Auftrag der israelischen Regierung gehandelt hat, bzw. dass die israelische Regierung über die Aktivitäten der *NSO Group* eine effektive Kontrolle ausgeübt hat, liegen indes nicht vor.

Losgelöst von der Frage der Zurechnung wäre zudem ein Individualbeschwerdeverfahren der betroffenen Personen wegen möglicher Vertragsverletzungen unmittelbar gegen den Staat Israel ohnehin nicht möglich, da Israel das erste Zusatzprotokoll zum VN-Zivilpakt, welches ein entsprechendes Verfahren vorsieht, nicht ratifiziert hat.¹⁶

3.3. Menschenrechtliche Schutzpflicht

Auch wenn weder ein potentiell völkerrechtswidriges Verhalten der Empfängerstaaten der Pegasus-Software noch die Handlungen des israelischen Softwareunternehmens *NSO Group* Israel zugerechnet werden können, ist im aktuellen Fall zu berücksichtigen, dass **Staaten völkerrechtlich zum Schutz vor Menschenrechtsverletzungen verpflichtet sind, die auf ihrem Hoheitsgebiet durch private Akteure begangen werden.**¹⁷

Die unter anderem in Art. 2 Abs. 2 des VN-Zivilpaktes enthaltene **menschenrechtliche Schutzpflicht** verpflichtet alle Paktstaaten „die erforderlichen Schritte zu unternehmen, um die gesetzgeberischen oder sonstigen Vorkehrungen zu treffen, die notwendig sind, um den in diesem Pakt anerkannten Rechten Wirksamkeit zu verleihen.“¹⁸ Der VN-Menschenrechtsausschuss hat diesbezüglich in seinem *General Comment* Nr. 31 im Jahre 2004 klargestellt, dass die Vertragsstaaten den Einzelnen auch vor Handlungen von privaten Akteuren schützen müssen, wenn diese den

15 Die mit Resolution A/56/83 vom 12. Dezember 2001 von der VN-Generalversammlung auf ihrer 56. Tagung (2001) zur Kenntnis genommenen *Draft Articles on Responsibility of States for Internationally Wrongful Acts* sind abrufbar unter: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Siehe auch: *Astrid Epiney*, „Zur Rechtsfigur des de facto-Organs im Recht der Staatenverantwortlichkeit“, in: *Frieden in Freiheit* : „Festschrift für Michael Bothe zum 70. Geburtstag“, Andreas Fischer-Lescano (Hrsg.), Baden-Baden: Nomos, 2008, S. 883-896 (884 f.).

16 Zum Ratifikationsstand siehe: <https://www.humanrights.ch/de/ipf/grundlagen/rechtsquellen-instrumente/uno/pakt-ii/>.

17 VN-Menschenrechtsausschuss, *General Comment* Nr. 31 vom 26. Mai 2004, UN Doc. (2004), Ziffer 8, <https://digitallibrary.un.org/record/533996>. Art. 2 Abs. 2 VN- Zivilpakt abrufbar unter: https://www.fedlex.admin.ch/eli/cc/1993/750_750_750/de.

18 *Thilo Mahraun*, „Sicherung grund- und menschenrechtlicher Standards gegenüber neuen Gefährdungen durch private und ausländische Akteure“, in: Hans-Christian Röhl/Andreas von Arnould (Hrsg.), „Öffnung der öffentlich-rechtlichen Methode durch Internationalität und Interdisziplinarität : Erscheinungsformen, Chancen, Grenzen“, Berlin: De Gruyter, 2015, S. 374-399 (387), <https://www.degruyter.com/document/doi/10.1515/9783110419122/html>.

Zugang zu Paktrechten beeinträchtigen.¹⁹ Der Pakt sieht zudem an einigen Stellen spezielle Schutzpflichten der Vertragsstaaten vor. So enthält **Art. 17 Abs. 2 des VN-Zivilpaktes** einen **Anspruch des Einzelnen auf rechtlichen Schutz gegen unrechtmäßige Eingriffe in seine Privatsphäre**.

Staatliche Verantwortlichkeit könnte sich daher auch aus der pflichtwidrigen Nichtverhinderung von Menschenrechtsverletzungen durch Private ergeben. **Positive Schutzpflichten** für Vertragsstaaten entstehen aber nur dann, wenn der Staat von einer Beeinträchtigung der Menschenrechte weiß oder bei **Anwendung entsprechender Sorgfalt hätte wissen müssen**.²⁰ Zum anderen muss der Staat tatsächlich die Möglichkeit der **Einflussnahme** auf Dritte haben und auch **rechtlich** in der Lage sein, entsprechende Vorkehrungen zu treffen, um eine Beeinträchtigung zu verhindern.²¹ Derartigen Schutzpflichten kann beispielsweise durch den Erlass von Gesetzen Rechnung getragen werden, die Menschenrechtsverletzungen präventiv verhindern sollen, bzw. sanktionieren.²²

Dass es beim Einsatz von digitaler Überwachungstechnologie insbesondere auch in autoritären Regimen zu Menschenrechtsverletzungen kommen kann, hat sich bereits in der Vergangenheit gezeigt.²³ Daran schließt sich die Frage an, ob ein Staat, der Genehmigungen für den Export von Überwachungssoftware erteilt, im Widerspruch zu seiner menschenrechtlichen Schutzpflicht handelt, wenn er weiß oder wissen müsste, dass die Software möglicherweise auch illegitim eingesetzt wird.²⁴

Zu berücksichtigen ist zunächst die Tatsache, dass die illegalen Ausspähangriffe offenbar in Drittstaaten erfolgt sind und nicht auf israelischen Territorium. Die **menschenrechtliche Schutzpflicht** der Vertragsstaaten erstreckt sich jedoch nach Art. 2 Abs. 1 des VN-Zivilpakts **grundsätzlich** nur auf alle **im Hoheitsgebiet** des Vertragsstaates befindlichen und seiner **Herrschaftsgewalt unterstehenden Personen**.²⁵ **Umstritten** ist dagegen, ob und inwieweit die Menschenrechtsverträge auch **extraterritoriale Schutzpflichten** zum Schutz von Personen, die sich nicht auf dem

19 VN-Menschenrechtsausschuss, General Comment Nr. 31 vom 26. Mai 2004, Ziffer 8, <https://digitallibrary.un.org/record/533996>.

20 *Walter Kälin/Jörg Künzli*, Universeller Menschenrechtsschutz. Der Schutz des Individuums auf globaler und regionaler Ebene, Basel: Helbing Lichtenhahn Verlag, 2013, S. 104.

21 *Walter Kälin/Jörg Künzli*, Universeller Menschenrechtsschutz. Der Schutz des Individuums auf globaler und regionaler Ebene, Basel: Helbing Lichtenhahn Verlag, 2013, S. 104.

22 Ebd.

23 Siehe dazu etwa *Daniel Moßbrucker*, „Digital durchleuchtet“, Amnesty International, 23. Mai 2017, <https://www.amnesty.de/journal/2017/juni/digital-durchleuchtet>.

24 Siehe *David Furger*, „Due Diligence bei der Waffenausfuhr genehmigung. Zu den völkerrechtlichen Anforderungen an die nationale Kriegsmaterialkontrolle,“ Sicherheit und Technik 2018, S. 171-184 (177), <https://static1.squarespace.com/static/5c38c18e9d5abbbf46544669/t/5c4ee56e1ae6cfaa21fca215/1548674417239/Furger+-+Due+Diligence.pdf>.

25 Art. 2 Abs. 1 VN-Zivilpakt, abrufbar unter: https://www.fedlex.admin.ch/eli/cc/1993/750_750_750/de.

eigenen Territorium befinden, begründen.²⁶ Der VN-Menschenrechtsausschuss geht jedenfalls davon aus, dass eine Anwendbarkeit des VN-Zivilpaktes auch für den Fall bestehen kann, dass ein Vertragsstaat Herrschaftsgewalt außerhalb seines Staatsgebietes ausübt (z.B. bei Besetzungen) und eine tatsächliche Kontrolle („effective control“) des Vertragsstaates vorliegt.²⁷ Da der israelische Staat jedoch in der vorliegenden Konstellation keine effektive Kontrolle über Gebiete oder Personen in den Drittstaaten ausübt und auch keine israelischen staatlichen Organe handeln, fehlt es an einem Anknüpfungspunkt, um eine entsprechende Schutzpflicht zu begründen.²⁸

Diskutiert werden darüber hinaus aber auch **menschenrechtliche Schutzpflichten der Staaten** mit Blick auf die **Regulierung unternehmerischen Handelns im Ausland** zum Schutz der Menschenrechte von Personen in Drittstaaten.²⁹ Zwar heißt es im Kommentar zu den VN-Leitprinzipien für Wirtschaft und Menschenrechte diesbezüglich: „Gegenwärtig verpflichten die Menschenrechte Staaten grundsätzlich nicht, die extraterritorialen Tätigkeiten in ihrem Hoheitsgebiet ansässiger und/oder ihrer Jurisdiktion unterstehender Unternehmen zu regulieren.“³⁰ Jedoch wird zunehmend die Ansicht vertreten, dass es sich hierbei nicht nur um eine rechtliche Mög-

-
- 26 Siehe etwa *Markus Krajewski*, „Regulierung transnationaler Wirtschaftsbeziehungen zum Schutz der Menschenrechte: Staatliche Schutzpflichten jenseits der Grenze?“, Erlangen: FAU University Press, 2018, S. 110 ff., <https://opus4.kobv.de/opus4-fau/frontdoor/index/index/docId/9934>.
Siehe auch *Jochen von Bernstorff*, „Extraterritoriale menschenrechtliche Staatenpflichten und Corporate Social Responsibility“, in: Archiv des Völkerrechts (AVR), 2011, S. 34-63 (47 ff.).
- 27 VN-Menschenrechtsausschuss, General Comment Nr. 31 vom 26. Mai 2004, Ziffer 10, <https://digitallibrary.un.org/record/533996>.
Jan-Philipp Redder, „Die exterritoriale Anwendbarkeit des Internationalen Paktes über bürgerliche und politische Rechte und der Europäischen Menschenrechtskonvention“, in: Humanitäres Völkerrecht, 2018, S. 261-275 (263 f.), <https://elibrary.bwv-verlag.de/article/99.105025/huv201803026101>.
Ibrahim Kanalan, „Extraterritoriale Staatenpflichten jenseits der Hoheitsgewalt: Ein neues Konzept für umfassende extraterritoriale Staatenpflichten“, in: Archiv des Völkerrechts (AVR), 2014, S. 495-521 (499f.), https://www.mohrsiebeck.com/artikel/extraterritoriale-staatenpflichten-jenseits-der-hoheitsgewalt-ein-neues-konzept-fuer-umfassende-extraterritoriale-staatenpflichten-101628000389214x14271941530745?no_cache=1.
- 28 Siehe auch *David Furger*, „Due Diligence bei der Waffenausfuhr genehmigung. Zu den völkerrechtlichen Anforderungen an die nationale Kriegsmaterialkontrolle“, Sicherheit und Technik 2018, S. 171-184, (178), <https://static1.squarespace.com/static/5c38c18e9d5abbbf46544669/t/5c4ee56e1ae6cfaa21fca215/1548674417239/Furger+-+Due+Diligence.pdf>. Der Autor verweist ferner auf die Ähnlichkeit zwischen Waffenexporten und der Non-refoulement-Situation, bei welcher eine menschenrechtliche Schutzpflicht anerkannt ist. Anders als beim Waffenexport befinde sich aber die geschützte Person beim Non-refoulement im maßgeblichen Zeitpunkt einer potentiellen Verletzung der menschenrechtlichen Schutzpflicht noch auf dem Territorium des zum Schutz verpflichteten Staates, weshalb es sich hier nach Ansicht des Autors nicht um eine extraterritoriale Geltung der Menschenrechte handelt.
- 29 Siehe etwa *Jochen von Bernstorff*, „Extraterritoriale menschenrechtliche Staatenpflichten und Corporate Social Responsibility“, in: Archiv des Völkerrechts (AVR), 2011, S. 34-63 (47 ff.).
- 30 Global Compact Netzwerk, Leitprinzipien für Wirtschaft und Menschenrechte, Umsetzung des Rahmens der Vereinten Nationen „Schutz, Achtung und Abhilfe“, 2. Aufl., 2014, S. 4, <https://www.auswaertiges-amt.de/blob/266624/b51c16faf1b3424d7efa060e8aaa8130/un-leitprinzipien-de-data.pdf>.

lichkeit zur Regulierung handelt, sondern auch eine „**menschenrechtliche Staatenpflicht zur Regelung von auslandsbezogenen Aktivitäten von Unternehmen**“ bestehen kann.³¹ Eine solche weitreichende Schutzpflicht sehen auch die *Maastrichter Prinzipien zu den Extraterritorialen Staatenpflichten im Bereich der wirtschaftlichen, sozialen und kulturellen Rechte* vor, die zwar rechtlich nicht verbindlich sind aber als Auslegungshilfe dienen können.³² Im Kern geht es dabei um den Gedanken, eine staatliche Schutzpflicht könne auch dann entstehen, wenn das **Verhalten Privater im Inland wesentliche Auswirkungen auf die Wahrnehmung der Menschenrechte außerhalb des eigenen Staatsgebietes** hat und für den Staat die Möglichkeit besteht, auf dieses Verhalten Einfluss zu nehmen.³³

Zur völkerrechtlichen Begründung einer solchen extraterritorialen Schutzpflicht wird von den Autoren *Markus Krajewski* und *David Furger* auf das zum Teil bereits völkergewohnheitsrechtlich anerkannte allgemeine Schädigungsverbot (*no harm-Prinzip*) verwiesen³⁴, wonach die Staaten verpflichtet sind ihre Rechte so auszuüben, dass keine anerkannten Rechtsgüter anderer Staaten geschädigt werden.³⁵ Im Umweltvölkerrecht sei etwa anerkannt, dass ein Staat in seinem Ho-

-
- 31 *Markus Krajewski*, „Völkerrechtliche Verpflichtung der Bundesrepublik zum Erlass eines Lieferkettengesetzes“, Verfassungsblog vom 5. Juni 2020, (Hervorhebung durch den Verfasser), <https://verfassungsblog.de/voelkerrechtliche-verpflichtung-der-bundesrepublik-zum-erlass-eines-lieferkettengesetzes/>. Der Beitrag befasst sich mit einer extraterritorialen Staatenpflicht in Bezug auf den Erlass eines Lieferkettengesetzes in Deutschland. Siehe auch *Ibrahim Kanalan*, „Extraterritoriale Staatenpflichten jenseits der Hoheitsgewalt: Ein neues Konzept für umfassende extraterritoriale Staatenpflichten“, in: Archiv des Völkerrechts (AVR), 2014, S. 495-521 (498). Siehe zudem *Daniel Augenstein*, Symposium, Business and Human Rights, „Extraterritoriale Regulierung als Staatenpflicht“, Völkerrechtsblog vom 3. August 2018, <https://voelkerrechtsblog.org/de/extraterritoriale-regulierung-als-staatenpflicht/>.
- 32 Maastricht Principles on the Extraterritorial Obligations of States in the Area of Economic, Social and Cultural Rights von 2011, abrufbar unter: <https://www.etoconsortium.org/en/main-navigation/library/maastricht-principles/>.
- 33 *David Furger*, „Due Diligence bei der Waffenausfuhrgenehmigung. Zu den völkerrechtlichen Anforderungen an die nationale Kriegsmaterialkontrolle,“ *Sicherheit und Technik* 2018, S. 171-184 (178), <https://static1.squarespace.com/static/5c38c18e9d5abbbf46544669/t/5c4ee56e1ae6cfaa21fca215/1548674417239/Furger+-+Due+Diligence.pdf>.
- 34 Siehe dazu vertiefend: *Jelena Bäumler*, *Das Schädigungsverbot im Völkerrecht*, Heidelberg: Springer 2017, S. 294.
- 35 *David Furger*, „Due Diligence bei der Waffenausfuhrgenehmigung. Zu den völkerrechtlichen Anforderungen an die nationale Kriegsmaterialkontrolle,“ *Sicherheit und Technik* 2018, S. 171-184 (178), <https://static1.squarespace.com/static/5c38c18e9d5abbbf46544669/t/5c4ee56e1ae6cfaa21fca215/1548674417239/Furger+-+Due+Diligence.pdf>.
Markus Krajewski, „Völkerrechtliche Verpflichtung der Bundesrepublik zum Erlass eines Lieferkettengesetzes“, Verfassungsblog vom 5. Juni 2020, <https://verfassungsblog.de/voelkerrechtliche-verpflichtung-der-bundesrepublik-zum-erlass-eines-lieferkettengesetzes/>.
Siehe zum Verbot erheblicher grenzüberschreitender Umweltbeeinträchtigungen auch: Gutachten der Wissenschaftlichen Dienste des Deutschen Bundestages, „Das völkergewohnheitsrechtliche Verbot erheblicher grenzüberschreitender Umweltbeeinträchtigungen im Streit um die Nordanflüge auf den Flughafen Zürich“, WD 2 - 3000 - 098/16 vom 23. August 2016, <https://www.bundestag.de/resource/blob/474566/304bc50a7245e93189c4364d8d8c94d5/WD-2-098-16-pdf-data.pdf>.

heitsgebiet Handlungen, z.B. Emissionen, unterbinden soll, die zu erheblichen negativen Umweltfolgen und Gesundheitsbeeinträchtigungen in den Nachbarstaaten führen können.³⁶ Aus der **universellen Geltung der Menschenrechte** folge, dass auch im Bereich der Menschenrechte diese Schutzpflicht nicht zwingend nur auf das Territorium eines Staates beschränkt sein müsse.³⁷ Für die Reichweite dieser Schutzpflicht wird auf die Kriterien der Einflussnahme und der Vorhersehbarkeit bezüglich potentieller Menschenrechtsverletzungen verwiesen.³⁸ Geht man von einer solchen extraterritorialen Schutzpflicht aus, endet die menschenrechtliche Schutzpflicht nicht an der Staatsgrenze, sondern verpflichtet Staaten mitunter auch zum Erlass **innerstaatlicher Maßnahmen**, welche die Aktivitäten inländischer Unternehmen mit Auswirkungen in Drittstaaten regeln.³⁹ Anknüpfungspunkt ist hierbei die staatliche Zugriffsmöglichkeit auf inländische Unternehmen.

Daran schließt sich die Frage an, welche Anforderungen an eine entsprechende Schutzpflicht mit Blick auf das Recht auf Privatheit beim Export digitaler Überwachungstechnologie zu stellen wären. Grundsätzlich wird man davon ausgehen können, dass Staaten zur Erfüllung der Schutzpflicht dazu angehalten sind, für die entsprechende Spionagesoftware ein **Exportkontrollsystem** zu errichten und die Erteilung der **Exportgenehmigung an bestimmte Mindeststandards** zu knüpfen, damit die Dual-Use Technologie nicht in falsche Hände gerät.⁴⁰ Dazu gehören etwa der Erlass

36 Vgl. *Markus Krajewski*, „Völkerrechtliche Verpflichtung der Bundesrepublik zum Erlass eines Lieferkettengesetzes“, Verfassungsblog vom 5. Juni 2020, <https://verfassungsblog.de/voelkerrechtliche-verpflichtung-der-bundesrepublik-zum-erlass-eines-lieferkettengesetzes/>

37 So *Markus Krajewski*, „Völkerrechtliche Verpflichtung der Bundesrepublik zum Erlass eines Lieferkettengesetzes“, Verfassungsblog vom 5. Juni 2020, <https://verfassungsblog.de/voelkerrechtliche-verpflichtung-der-bundesrepublik-zum-erlass-eines-lieferkettengesetzes/>.

38 *David Furger*, „Due Diligence bei der Waffenausfuhr genehmigung. Zu den völkerrechtlichen Anforderungen an die nationale Kriegsmaterialkontrolle,“ *Sicherheit und Technik* 2018, S. 171-184 (180 ff.), <https://static1.squarespace.com/static/5c38c18e9d5abbbf46544669/t/5c4ee56e1ae6cfaa21fca215/1548674417239/Furger+-+Due+Diligence.pdf>.

Siehe auch *Markus Krajewski*, „Völkerrechtliche Verpflichtung der Bundesrepublik zum Erlass eines Lieferkettengesetzes“, Verfassungsblog vom 5. Juni 2020, <https://verfassungsblog.de/voelkerrechtliche-verpflichtung-der-bundesrepublik-zum-erlass-eines-lieferkettengesetzes/>.

39 Siehe dazu auch: *Christine Kaufmann, Christoph Good, Sabrina Ghielmini, Charlotte Blattner*, Extraterritorialität im Bereich Wirtschaft und Menschenrechte. „Extraterritoriale Rechtsanwendung und Gerichtsbarkeit in der Schweiz bei Menschenrechtsverletzungen durch transnationale Unternehmen“, Schweizerisches Kompetenzzentrum für Menschenrechte, 15. August 2016, S. 33, <https://www.skmr.ch/de/themenbereiche/wirtschaft/publikationen/unternehmen-extraterritorialitaet.html>.

Daniel Augenstein, Symposium, Business and Human Rights, „Extraterritoriale Regulierung als Staatenpflicht“, Völkerrechtsblog vom 3. August 2018, <https://voelkerrechtsblog.org/de/extraterritoriale-regulierung-als-staatenpflicht/>.

40 Vgl. dazu *David Furger*, „Due Diligence bei der Waffenausfuhr genehmigung. Zu den völkerrechtlichen Anforderungen an die nationale Kriegsmaterialkontrolle,“ *Sicherheit und Technik* 2018, S. 171-184 (181), <https://static1.squarespace.com/static/5c38c18e9d5abbbf46544669/t/5c4ee56e1ae6cfaa21fca215/1548674417239/Furger+-+Due+Diligence.pdf>.

Siehe auch: *Daniel Mossbrucker*, „Kriterien für die Exportkontrolle von Überwachungstechnologie zum wirksamen Schutz der Privatheit sowie der Meinungs- und Pressefreiheit“, *Humanitäres Völkerrecht*, 2018, S. 69-91 (83).

von entsprechenden Gesetzen und Verordnungen sowie die Anwendung der Vorgaben durch die zuständigen Behörden. Mit Blick auf die Anforderungen an die Vorhersehbarkeit des menschenrechtswidrigen Einsatzes von Spionagesoftware ist darauf hinzuweisen, dass den Behörden ein **großer Ermessensspielraum** bei der Prüfung der Sorgfaltspflicht zukommt.⁴¹

Auch wenn man der Annahme einer **extraterritorialen Schutzpflicht** folgt, ließe sich daher für den vorliegenden Fall unter Zugrundelegung der genannten Kriterien wohl **keine völkerrechtliche Sorgfaltspflichtverletzung Israels durch die Erteilung der Exportgenehmigung für die Pegasus-Software** annehmen. Nach Angaben der *Neuen Züricher Zeitung* erteilt das für die Exportgenehmigung zuständige israelische Verteidigungsministerium eine Genehmigung nur dann, wenn die Spionagesoftware an staatliche Behörden verkauft und von diesen ausschließlich zur Verfolgung von Terroristen und Kriminellen eingesetzt wird.⁴² Auch wird eine gesetzliche Grundlage für den Einsatz gefordert.⁴³ Unabhängig davon, dass die Bestimmungen über die israelische Exportkontrolle den Wissenschaftlichen Diensten nicht vorliegen, kann nicht viel mehr verlangt werden, als dass **menschenrechtliche Mindeststandards bei der Exportkontrolle** eingehalten und regelmäßig überprüft werden. Internationale Standards zum Export digitaler Überwachungstechnologie gibt es gerade nicht (siehe 2.). Angesichts des **weiten Ermessensspielraums** wird man es daher als ausreichend erachten müssen, dass Israel von den Empfängerstaaten eine Zusage erhält, die Software nicht menschenrechtswidrig einzusetzen. Israel hat zudem angekündigt, die Regeln für die Ausfuhr von Spionagesoftware zu prüfen und gegebenenfalls zu verschärfen.⁴⁴

Ferner sollte berücksichtigt werden, dass sich eine **unmittelbare Kausalität** zwischen der Erteilung der Exportgenehmigung durch Israel und dem menschenrechtswidrigen Einsatz durch Drittstaaten mit Blick auf das Handeln weiterer Akteure **kaum begründen lässt**. Die Produkte der NSO Group werden nach einem Bericht von Menschenrechtsorganisationen etwa auch aus Zypern und Bulgarien exportiert.⁴⁵ Eine Weitergabe der Produkte durch die Empfängerstaaten lässt sich

41 Vgl. dazu *David Furger*, „Due Diligence bei der Waffenausfuhrgenehmigung. Zu den völkerrechtlichen Anforderungen an die nationale Kriegsmaterialkontrolle,“ *Sicherheit und Technik* 2018, S. 171-184 (183). <https://static1.squarespace.com/static/5c38c18e9d5abbbf46544669/t/5c4ee56e1ae6cfaa21fca215/1548674417239/Furger+-+Due+Diligence.pdf>. *Furger* verweist hierzu auf ein Urteil des High Court of Justice des Vereinigten Königreichs aus dem Jahr 2017. In dem Verfahren hatten verschiedene Nichtregierungsorganisationen „geltend gemacht, dass die wiederholten Waffenexporte aus dem Vereinigten Königreich an Saudi-Arabien gegen die Kriterien des gemeinsamen Standpunkts der EU verstießen, da die Waffen im bewaffneten Konflikt in Jemen völkerrechtswidrig eingesetzt würden. [...] Das Gericht wies die Klage ab, insbesondere mit Verweis auf den weiten Ermessensspielraum der Genehmigungsbehörde.“

42 Neue Züricher Zeitung vom 29. Juli 2021, „Spyware Pegasus: Israelische Behörden führen bei der umstrittenen NSO Group eine Inspektion durch“, <https://www.nzz.ch/technologie/spyware-pegasus-das-israelische-verteidigungsministerium-fuehrt-bei-der-nso-group-eine-inspektion-durch-ld.1636705>.

43 Ebd.

44 The Guardian vom 22. Juli 2021, „Israel to examine whether spyware export rules should be tightened“, <https://www.theguardian.com/news/2021/jul/22/israel-examine-spyware-export-rules-should-be-tightened-nso-group-pegasus>.

45 Amnesty International, Privacy International and The Centre for Research on Multinational Corporations, „Operating from the shadows. Inside NSO Group’s corporate structure“, 2021, <https://www.privacyinternational.org/sites/default/files/2021-06/DOC1041822021EN.pdf>.

zudem nicht ausschließen und Israel hat nur technisch begrenzte Möglichkeiten die Einhaltung der Exportbedingungen überhaupt im Nachhinein zu überprüfen.

4. Fazit

Spezielle **völkerrechtlich verbindliche Vorgaben für den Export digitaler Überwachungstechnologie fehlen** bislang. Eine **Mitverantwortung Israels** für den menschenrechtswidrigen Einsatz der Spionage-Software Pegasus **lässt sich nicht begründen**. Allein die Tatsache, dass die Software aus Israel exportiert wurde, führt nicht zu einer unmittelbaren Verantwortung Israels für den missbräuchlichen Einsatz in Drittstaaten. Dem israelischen Staat die Handlungen des israelischen Softwareherstellers *NSO Group* zuzurechnen, kommt ebenfalls nicht in Betracht.

Die Ausspähangriffe mittels der Pegasus-Software greifen in den Schutzbereich des Menschenrechts auf Privatsphäre (privacy) ein, das unter anderem in Art. 17 VN-Zivilpakt verankert ist. Staaten sind völkerrechtlich grundsätzlich dazu verpflichtet, Personen in ihrem Hoheitsgebiet oder unter ihrer Herrschaftsgewalt Schutz vor Menschenrechtsverletzungen zu gewähren. Folgt man der Annahme einer **extraterritorialen Schutzpflicht** könnte man zwar eine Schutzpflicht Israels hinsichtlich des Exports digitaler Überwachungstechnologie annehmen, die sich auch auf den Schutz von Personen in Drittstaaten erstreckt. Dieser **Verpflichtung zum Erlass innerstaatlicher Maßnahmen** käme Israel jedoch mittels **gesetzlicher Mindeststandards an eine Exportbewilligung** für die Spionagesoftware nach. Die Staaten verfügen diesbezüglich über einen weiten **Ermessensspielraum**, so dass sich hier wohl kein Verstoß gegen eine menschenrechtliche Schutzpflicht feststellen lässt.

Die Enthüllungen über den menschenrechtswidrigen Einsatz der Pegasus-Software haben gezeigt, dass eine **effektive und rechtlich verbindliche globale Kontrolle** digitaler Überwachungssoftware dringend erforderlich ist. Bis entsprechende internationale **menschenrechtskonforme** rechtliche Rahmenbedingungen für **Transparenz- und Genehmigungspflichten** geschaffen werden, wird daher von Menschenrechtsexperten der Vereinten Nationen sowie von Menschenrechtsorganisationen gefordert, den Verkauf, die Weitergabe und den Einsatz von Überwachungstechnologie zu untersagen.⁴⁶ Auf europäischer Ebene wurde am 11. Juni 2021 die neue EU Dual-Use-Verordnung veröffentlicht, die auch Vorgaben zum Export digitaler Überwachungssoftware enthält. Kritikern gehen die Regelungen aber nicht weit genug.⁴⁷ Auch wird gefordert, Regelungen zu etablieren,

46 VN-Menschenrechtsausschuss, Pressemitteilung vom 12. August 2021, „Spyware scandal: UN experts call for moratorium on sale of ‘life threatening’ surveillance tech“, <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27379&LangID=E>. Tagesschau.de vom 19. Juli 2021, „Markt außer Kontrolle“, <https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-markt-101.html>.

47 Siehe etwa Netzpolitik.org vom 10. November 2020, „Dual-Use-Verordnung. EU verwässert neue Regeln für Überwachungsexporte“, <https://netzpolitik.org/2020/dual-use-verordnung-eu-verwaessert-neue-regeln-fuer-ueberwachungsexporte/>.

die dafür sorgen, dass private Hersteller von Überwachungssoftware in der Verantwortung stehen, wenn sie ihr Produkt an autoritäre Regime verkaufen.⁴⁸

48 Vgl. Süddeutsche Zeitung vom 19. Juli 2021, Interview mit dem ehemaligen VN-Sonderberichterstatter für Meinungsfreiheit, *David Kaye*, „Die Überwachungsindustrie ist außer Kontrolle“, https://projekte.sueddeutsche.de/artikel/politik/pegasus-project-ueberwachungsindustrie-ausser-kontrolle-e717512/?utm_source=twitter&utm_medium=twitterbot&utm_content=e717512&reduced=true.