AMNESTY INTERNATIONAL ÖSTERREICH
Lerchenfelder Gürtel 43/4/3 1160 Wien
T: +43 1 78008 F: +43 1 78008-44 office@amnesty.at www.amnesty.at

SPENDENKONTO 316326 BLZ 20111 Erste Bank
IBAN: AT142011100000316326 BIC: GIBAATWWXXX
DVR: 460028 ZVR: 407408993

STELLUNGNAHME

zum Ministerialentwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienstgesetz geändert wird

24. September 2024

Amnesty International Österreich bezieht zu Gesetzesentwürfen nur im Rahmen ihres Mandats, sohin nur insoweit Stellung, als menschenrechtliche Implikationen gegeben sind.

GRUNDSÄTZLICHES

Amnesty International untersucht seit mehreren Jahren, gemeinsam mit Partnerorganisationen, den Einsatz und die technischen Möglichkeiten von Überwachungs- und Spionagesoftware (im Folgenden „Spyware" genannt).[1] So ist jegliche Spyware, die Amnesty International bis heute untersucht hat, eine hochinvasive Spyware. Das bedeutet eine Spyware, die

- standardmäßig uneingeschränkten Zugriff auf ein Gerät erlaubt und nicht auf solche Funktionen eingeschränkt werden kann, die notwendig und verhältnismäßig in Bezug auf einen spezifischen Einsatz und Ziel ist, oder
- nicht überprüft und unabhängig kontrolliert werden kann.

Hochinvasive Spyware kann zu Menschenrechtsverletzungen in großem Umfang führen und dazu benutzt werden, um auch Journalist*innen, Aktivist*innen und Menschenrechtsverteidiger*innen ins Visier zu nehmen und zum Schweigen zu bringen.[2]

Sobald eine hochinvasive Spyware in ein Gerät eingedrungen ist, hat sie ungehinderten Zugang zum gesamten System, so z.B. auch zu dessen Mikrofon und Kamera, sowie zu allen Daten, wie Kontakten, Nachrichten, Fotos und Videos, ohne dass die*der Benutzer*in davon etwas mitbekommt. Das gilt auch für verschlüsselte Chats. In Zeiten, in denen Smartphones und Computer quasi ein Abbild unseres Lebens sind und sohin Einblick in alle – auch höchstpersönlichen – Lebensbereiche gewähren, kommt dies dem geheimen Eindringen in eine Wohnung, ihrer kompletten Durchsuchung sowie der laufenden verdeckten Überwachung der Räumlichkeiten, ihrer Bewohner*innen und Besucher*innen gleich. Dies ohne Wissen der*des Betroffenen und ohne wirksame Überprüfung durch ein unabhängiges Gericht. Ein derart invasiver Eingriff in das Menschenrecht auf Privatsphäre kann nicht verhältnismäßig sein und ist daher abzulehnen.

In diesem Sinne stellte auch der Europäische Datenschutzbeauftragte in Bezug auf hochinvasive Spyware im Jahr 2022 fest, dass „[d]as Ausmaß des Eingriffs in das Recht auf Privatsphäre so schwerwiegend [ist], dass der Einzelne tatsächlich seines Rechts beraubt wird. Mit anderen Worten: Das Recht ist in seinem Kern betroffen. Daher kann ihre Anwendung nicht als verhältnismäßig angesehen werden - unabhängig davon, ob die Maßnahme als notwendig erachtet werden kann."[3] Auch die ehemalige Sonderberichterstatterin für Terrorismusbekämpfung der Vereinten Nationen sagte klar und deutlich, dass Spionagesoftware, die in ihrer Funktionalität nicht sinnvoll eingeschränkt werden kann und deren Einsatz nicht unabhängig überprüft werden kann, nicht menschenrechtskonform ist.[4]

Aufgrund der menschenrechtlichen Implikationen einer solchen Maßnahme bringt Amnesty International Österreich ihre menschenrechtliche Expertise in entsprechende Prozesse ein; so geschehen im Rahmen des Begutachtungsprozesses zum Ministerialentwurf des Strafprozessänderungsgesetz 2017[5] bzw. zur Regierungsvorlage 2018[6] („Staatstrojaner"). Seit den zwischenzeitlich aufgehobenen Bestimmungen zum „Staatstrojaner" hat Amnesty International neue Erkenntnisse zum Einsatz von (auch neuerer) Spyware gewonnen, die Amnesty International Österreich nun auch im Rahmen des aktuellen Begutachtungsverfahrens zum Ministerialentwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienstgesetz geändert werden soll, dazu veranlasst, sich zu äußern.

---

[1] Siehe Annex
[2] Siehe Annex
[3] Europäischer Datenschutzbeauftragter, *Preliminary Remarks on Modern Spyware*, 15.2.2022, Seite 8 https://www.edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf
[4] VN-Sonderberichterstatterin für Terrorismusbekämpfung, *Position Paper, Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*, Dezember 2022, Rn 66, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf
[5] https://www.parlament.gv.at/dokument/XXV/SNME/30495/imfname_667813.pdf
[6] https://cdn.amnesty.at/media/2652/stellungnahme-sicherheitspaket-2018.pdf

ZUSAMMENFASSUNG

Der vorliegende Gesetzesentwurf ist ein neuerlicher Versuch, eine Rechtsgrundlage für den Einsatz von Überwachungs- und Spionagesoftware (im Folgenden Spyware) von verschlüsselter Kommunikation zu schaffen.

Amnesty International verkennt nicht die Notwendigkeit, den Strafverfolgungsbehörden, insbesondere in Hinblick auf die Prävention möglicher terroristischer Straftaten, im wohl begründeten Einzelfall taugliche Ermittlungsinstrumente und -maßnahmen zur Verfügung zu stellen.

Gemäß der Rechtsprechung des Europäischen Gerichtshof für Menschenrechte (EGMR) ist jegliche Überwachungsmaßnahmen geschützter elektronischer Individualkommunikation ein Eingriff in die Korrespondenzfreiheit (iSd Artikel 8 EMRK).[7] Eingriffe sind nur dann zulässig, wenn sie gesetzlich vorgesehen, zur Verfolgung eines legitimen Zieles in einer demokratischen Gesellschaft notwendig sind und einer Verhältnismäßigkeitsprüfung standhalten sowie das gelindeste Mittel darstellen.

Bei geheimen staatlichen Maßnahmen gilt ein höherer Maßstab an die hinreichende Bestimmtheit und die Vorhersehbarkeit des Gesetzes. Es müssen zudem angemessene und wirksame Garantien gegen Missbrauch vorhanden sein.[8] Maßnahmen zur systematischen verdeckten Überwachung sind gemäß Rechtsprechung des EGMR zudem unter unabhängige (in der Regel gerichtliche) Aufsicht zu stellen, um die Rechte der von der Überwachung Betroffenen zu wahren.[9]

Amnesty International Österreich geht angesichts des vorliegenden Gesetzesentwurfs davon aus, dass die Behörden eine hochinvasive Spyware einsetzen möchten. Das ist Spyware, die standardmäßig den uneingeschränkten Zugriff auf ein Gerät erlaubt und deren Einsatz nicht adäquat und unabhängig überprüft werden kann.

Amnesty International Österreich lehnt den Einsatz von hochinvasiver Spyware aus den folgenden Gründen entschieden ab:

Erstens hat eine derartige Spyware, sobald sie in ein Gerät eingedrungen ist, ungehinderten Zugang zum gesamten System, so z.B. auch zu dessen Mikrofon und Kamera, sowie zu allen Daten wie Kontakten, Nachrichten, Fotos und Videos, ohne dass die*der Benutzer*in davon etwas mitbekommt. Das gilt auch für verschlüsselte Chats. In Zeiten, in denen Smartphones und Computer quasi ein Abbild unseres Lebens sind und sohin Einblick in alle – auch höchstpersönlichen – Lebensbereiche gewähren, ist das Recht auf Privatsphäre (Artikel 8 EMRK, Artikel 17 Internationaler Pakt über bürgerliche und politische Rechte (IPbpR)) in seinem Kern betroffen. Ein derart massiver Eingriff kann nicht verhältnismäßig sein.

Zweitens sind die sogenannten Exploits, auf die sich die Hersteller*innen von Spyware stützen, sehr wertvoll und werden daher wie Geschäftsgeheimnisse behandelt. Es wäre nicht im Interesse der Hersteller*innen, den Quellcode dieser Exploits ihren staatlichen Kunden gegenüber offenzulegen. Folglich ist es nicht möglich, den menschenrechtskonformen Einsatz von Spyware unabhängig zu überprüfen.

Drittens setzt die erfolgreiche Anwendung von Spyware zur Überwachung verschlüsselter Nachrichten nicht zuletzt voraus, dass es Sicherheitslücken in der IT-Infrastruktur gibt. Wenn der Staat zwecks Installation von Spyware technische Sicherheitslücken absichtlich offenlässt, kann das zu Menschenrechtsverletzungen führen.

Amnesty International lehnt daher die Einführung einer Rechtsgrundlage für den Einsatz von potenziell hochinvasiver Spyware entschieden ab.

---

[7] EGMR, 14.3.2013, Bernh Larsen Holding AS u.a. / Norwegen, Z. 105 ; VfSlg 20.356/2019 Rn 171
[8] EGMR, 8.4.2014, Blaj / Rumänien, Z. 128, 133; EGMR Klass u.a. / Deutschland Z 48ff; VfSlg 20.356/2019 Rn 171
[9] EGMR 4.5.2000, Rotaru / Rumänien, Z. 59

MENSCHENRECHTLICHE BEWERTUNG EINZELNER AUSGEWÄHLTER BESTIMMUNGEN

§11 Abs. 1 Z 9 SNG

Im gegenständlichen Gesetzesentwurf wird vorgeschlagen, dass zum Überwachen verschlüsselter Nachrichten ein „Programm in ein Computersystem eingebracht wird“. Dies soll gemäß den Erläuterungen „ohne Kenntnisnahme des Betroffenen“ geschehen.[10] Dies wird auch als gezielte digitale Überwachung mithilfe von Spyware bezeichnet.

Wie aus den Erläuterungen zum Gesetzesentwurf zu entnehmen ist, wird Deutschland als Beispiel genannt,[11] wo die hochinvasive Spyware „Pegasus“ bekanntlich vom Bundeskriminalamt und dem Bundesnachrichtendienst eingesetzt wurde. Dabei wurden laut der Tageszeitung „Die Zeit“ möglicherweise Daten an die Hersteller*innen von Pegasus, der NSO Group, weitergeleitet.[12]

Basierend auf diesen Erläuterungen und auch den bisherigen Untersuchungen bzw. Erkenntnissen von Amnesty International in Kooperation mit technischen Expert*innen zum Einsatz von Spyware ist in diesem Fall davon auszugehen, dass in Österreich der Einsatz hochinvasiver Spyware vorgesehen ist.[13]

Dafür scheint es in einem ersten Schritt notwendig zu sein, über ein Befehlsprogramm, das die Sicherheitslücken und Fehlfunktionen von Computersystemen ausnutzt, sogenannter Exploit, die vollständige Kontrolle über das Gerät zu erlangen, um Nachrichten lesen zu können. Amnesty International Österreich sieht für ein Gericht keine Möglichkeit zu überprüfen, ob die Spyware ihre Fähigkeit, nur die autorisierten Nachrichten vom Gerät abzufangen, in Folge tatsächlich einschränkt.

Der Einsatz von Spyware kann weder überprüft noch unabhängig kontrolliert werden

Der Gesetzesentwurf sieht eine gerichtliche Anordnung durch das Bundesverwaltungsgericht (BVwG) sowie eine laufende Kontrolle durch den Rechtsschutzbeauftragten vor.[14] Dafür müssten Behörden und unabhängige Gerichte, unter anderen, neben ausreichender IT-Expertise und Ressourcen, vollen Zugriff und Kontrolle über den Quellcode der eingesetzten Software haben.

Allgemein ist aber davon auszugehen, dass es nicht im Interesse der Hersteller*innen bzw. Verkäufer*innen von Spyware ist, ihren Kund*innen den Quellcode ihres Produkts offen zu legen. Wenn Spyware von einem privaten Unternehmen oder einem anderen Staat zugekauft wird, haben die kontrollierenden Stellen, ohne den Quellcode, keine Möglichkeit zu sehen, was die Spyware tatsächlich macht. Sie könnten nicht kontrollieren, ob sich die Spyware auf die im Gesetz vorgesehenen Funktionalitäten beschränkt und welche Daten sie tatsächlich ausliest, speichert, löscht etc. Ohne Quellcode kann auch nicht wirksam überprüft werden, ob die Spyware iSd § 15a Abs. 5 Z 3 SNG nach Beendigung der Ermittlungsmaßnahme tatsächlich entfernt wurde bzw. funktionsunfähig ist.

Mangels Transparenz und Einsicht in die technischen Gegebenheiten ist eine effektive Kontrolle durch Gerichte nicht möglich. Es besteht insbesondere ein mangelnder Schutz vor potenzieller Datenweitergabe an Dritte, wodurch ein Eingriff in das Recht auf Privatsphäre erfolgt. Die Behörden könnten nämlich gar nicht überprüfen bzw. sehen, ob Daten im Hintergrund nicht missbräuchlich weitergegeben werden bzw. die Lücke im System, die für die Einschleusung der Spyware notwendig ist,

[10] 350/ME XXVII. GP – Erläuterungen, Seite 5
[11] 350/ME XXVII. GP – Erläuterungen, Seite 3
[12] Die Zeit, *Bundesnachrichtendienst setzt umstrittene Cyberwaffe ein*, 8.10.2021 https://www.zeit.de/politik/deutschland/2021-10/pegasus-spionage-software-bnd-kaeufer-einsatz-israel?
[13] Amnesty International, *A Web of Surveillance: Unravelling a murky network of spyware exports to Indonesia*, 1.5.2024 https://securitylab.amnesty.org/latest/2024/05/a-web-of-surveillance/
[14] § 14 Abs. 4 SNG

nicht auch für andere Zwecke genutzt wird.[15] Mangels tatsächlicher Kontrolle kann der Staat außerdem seiner Rechenschaftspflicht gegenüber der Öffentlichkeit nicht nachkommen.

Ohne wirksame Kontrolle des Quellcodes könnte die Spyware alle Daten am Handy der Person, die gezielt überwacht wird, auswerten und auf Kameras und Mikrofon zugreifen. Damit könnten auch Informationen über Menschen, die sowohl online als auch offline mit der zu überwachenden Person in Kontakt stehen, bzw. Gespräche mit ihnen, gesammelt und z.B. an Dritte ausgespielt werden. Es besteht somit das Risiko, dass Menschen, die selbst nicht das Ziel der Überwachung sind, aber in Kontakt mit einer Person stehen, die gezielt überwacht wird, auch selbst (rechtswidrig) überwacht werden.

Hacker*innen verwenden dieselben Sicherheitslücken wie Behörden

Jeder Staat, der eine gesetzliche Grundlage für die Anwendung einer Spyware einführt, schafft ein Sicherheitsrisiko in der für alle Menschen immer wichtiger werdenden IT-Infrastruktur.

Die erfolgreiche Anwendung von Spyware zur Überwachung verschlüsselter Nachrichten setzt voraus, dass es Sicherheitslücken in der IT-Infrastruktur gibt. Dafür werden Befehlsprogramme geschrieben, die die Sicherheitslücken und Fehlfunktionen von Computersystemen ausnutzen, um ihn sie einzudringen (Exploits). Die staatlichen Behörden sind also auf diese Sicherheitslücken angewiesen, um in fremde Computersysteme eindringen zu können. Sie werden daher – zumindest in gewissen Fällen – kein Interesse an einem Schließen aller Sicherheitslücken haben, weil sonst auch die Verwendung von Spyware zur Überwachung verschlüsselter Nachrichten nutzlos wäre. Das führt aber dazu, dass sie diese Sicherheitslücken nicht frühzeitig an Softwarehersteller*innen oder Unternehmen, die Software nutzen, melden werden.

Anstatt daran zu arbeiten, wie man Sicherheitslücken schließen kann, um Menschen vor Hacker*innen zu schützen, werden sie absichtlich offengelassen. Dies führt wiederum dazu, dass diese Sicherheitslücken – trotz Kenntnis des Staates – auch von Dritten genützt werden können, um sich z.B. in einen Computer zu hacken, ihn komplett zu blockieren und allenfalls auch Menschen zu erpressen.

Ein Beispiel dafür, welche schwerwiegenden Konsequenzen das Offenlassen von Sicherheitslücken haben kann, ist der Trojaner „WannaCry“: Der US-amerikanische Auslandsgeheimdienst „National Security Agency“ (NSA) kannte Sicherheitslücken bei Microsoft und ließ sie bewusst offen, anstatt sie sofort zu melden. Die Folge: Im Mai 2017 nutzte WannaCry diese Sicherheitslücken aus und infizierte über 230.000 Computer in 150 Ländern. Der Trojaner blockierte die Geräte und verlangte Lösegeldzahlungen. Er legte damit weltweit wichtige IT-Systeme lahm – in Fabriken, Behörden und Krankenhäusern. Ärzt*innen konnten computergesteuerte und lebenswichtige Geräte nicht mehr in Betrieb nehmen und Patient*innen mussten abgewiesen werden.[16]

Diese Beispiele zeigen deutlich, dass, wenn Staaten zwecks Installation von Spyware technische Sicherheitslücken absichtlich offenlassen, es in Folge zu Menschenrechtsverletzungen kommen kann.

Eingriff in die Menschenrechte aller (potenzieller) Nutzer*innen: „Chilling effect“

Wenn Staaten keine angemessenen Sicherheitsvorkehrungen treffen, um Menschen vor rechtswidriger Überwachung zu schützen, kann es unmöglich sein, herauszufinden, wer überwacht wird, wie oder warum. Untersuchungen belegen, dass Journalist*innen und Menschenrechtsverteidiger*innen, die befürchten überwacht zu werden, weniger bereit sind, sich kritisch über die Regierung zu äußern, friedliche Proteste zu organisieren, sich frei mit Kolleg*innen zu treffen, ihre Quellen oder Angehörige zu kontaktieren, zu telefonieren oder E-Mails zu versenden. Dies aus dem Grund, dass sie nicht wissen, wie diese Aktivitäten später gegen sie verwendet werden könnten oder sie vielleicht andere Menschen

[15] Futurezone, *Bundestrojaner überall? Wie in Europa Chats überwacht werden*, 29.6.2023 https://futurezone.at/amp/netzpolitik/bundestrojaner-staatstrojaner-whatsapp-chats-ueberwachung/402505407
[16] Der Spiegel, *"WannaCry"-Attacke - Fakten zum globalen Cyberangriff*, 13.5.2017 https://www.spiegel.de/netzwelt/web/wannacry-attacke-fakten-zum-globalen-cyber-angriff-a-1147523.html ; https://de.wikipedia.org/wiki/WannaCry

in Gefahr bringen.[17] Sie halten sich bei der Ausübung ihrer Menschenrechte, insbesondere der Meinungsäußerungs- und Versammlungsfreiheit zurück, aus Angst, dass sie rechtswidrig überwacht werden könnten (sogenannter „chilling effect").[18]

In Bezug auf das Recht auf Privat- und Familienleben (Artikel 8 EMRK) hielt der EGMR eindeutig fest, dass der „*chilling effect*" ein Eingriff in dieses Recht sein kann: „der weit verbreitete Verdacht und die Besorgnis in der Öffentlichkeit, dass geheime Überwachungsbefugnisse missbraucht werden, [sind] nicht unberechtigt [...]. Unter solchen Umständen kann die Bedrohung durch die Überwachung an sich als Einschränkung der freien Kommunikation über die Post- und Telekommunikationsdienste geltend gemacht werden und stellt somit für alle (potenziellen) Nutzer*innen einen unmittelbaren Eingriff in das Recht [auf Privat- und Familienleben] dar."[19]

Wenn die Schutzmaßnahmen unzureichend sind, werden also nicht nur die Rechte jener Menschen beeinträchtigt, die überwacht werden, sondern die Rechte aller, die aufgrund der unzähligen und unvorhersehbaren Möglichkeiten, wie Daten über ihre Aktivitäten gegen sie verwendet werden könnten, unter anderem auf die Ausübung ihrer Rechte auf freie Meinungsäußerung und Versammlungsfreiheit verzichten.

Vor diesem Hintergrund lehnt Amnesty International eine Rechtsgrundlage für den Einsatz von potenziell hochinvasiver Spyware ab. In Zeiten, wo Smartphones und Computer ein Abbild sämtlicher Lebensbereiche darstellen, höhlt der Einsatz von Spyware, die auf das gesamte Gerät Zugriff verschafft, das Grundrecht auf Privatsphäre aus.

§ 11 Abs. 1 Z 8 SNG

Wie bereits betont, verkennt Amnesty International nicht die Notwendigkeit den Strafverfolgungsbehörden, insbesondere in Hinblick auf die Prävention möglicher terroristischer Straftaten, im wohl begründeten Einzelfall taugliche Ermittlungsinstrumente und -maßnahmen zur Verfügung zu stellen.

Menschenrechtlicher Rahmen

Gemäß der Rechtsprechung des EGMR ist jedoch jegliche Überwachungsmaßnahme geschützter elektronischer Individualkommunikation ein Eingriff in die Korrespondenzfreiheit (Artikel 8 EMRK).[20] Eingriffe sind nur dann zulässig, wenn sie gesetzlich vorgesehen, zur Verfolgung eines legitimen Zieles in einer demokratischen Gesellschaft notwendig sind und einer Verhältnismäßigkeitsprüfung standhalten sowie das gelindeste Mittel darstellen. Überwachungsmaßnahmen können zudem einen sogenannten „chilling effect" auf die Ausübung anderer Menschenrechte wie z.B. die Meinungsäußerungsfreiheit (Artikel 10 EMRK, Artikel 19 IPbpR)[21] und die Versammlungsfreiheit (Artikel 11 EMRK, Artikel 21 IPbpR) haben.

Bei geheimen staatlichen Maßnahmen gilt ein höherer Maßstab an die hinreichende Bestimmtheit und die Vorhersehbarkeit des Gesetzes. Es müssen zudem angemessene und wirksame Garantien gegen Missbrauch vorhanden sein.[22] Maßnahmen zur systematischen verdeckten Überwachung sind gemäß

[17] Amnesty International, *Belarus: "It's enough for people to feel it exists" : Civil society, secrecy and surveillance in Belarus*, 7.7.2016, https://www.amnesty.org/en/documents/eur49/4306/2016/en/
[18] OHCHR, *Report: The Right to Privacy in the Digital Age*, 30.6.2014, UN Doc. A/HRC/27/37, Rn 20, https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021
[19] EGMR, Roman Zakharov v. Russia, Z 171; Das Phänomen des „chilling effect"s beim Einsatz der Spyware Pegasus wurde auch in der vom PEGA-Ausschuss des Europäischen Parlaments beauftragten Studie von Giovanni SARTOR und Andrea LOREGGIA, *Die Auswirkungen von Pegasus auf Grundrechte und demokratische Prozesse*, bestätigt (https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_DE.pdf).
[20] EGMR, 14.3.2013, Bernh Larsen Holding AS u.a. / Norwegen, Z. 105 ; VfSlg 20.356/2019 Rn 171
[21] Siehe auch VN-Sonderberichterstatter für Meinungs- und Meinungsäußerungsfreiheit, *Surveillance and human rights*, 28.5.2019, A/HRC/41/35, Rn 46 https://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur
[22] EGMR, 8.4.2014, Blaj / Rumänien, Z. 128, 133; EGMR Klass u.a. / Deutschland Z 48ff; VfSlg 20.356/2019 Rn 171

Rechtsprechung des EGMR zudem unter unabhängige (in der Regel gerichtliche) Aufsicht zu stellen, um die Rechte des von der Überwachung Betroffenen zu wahren.[23]

Überwachung von Daten, auch von Dritten

Die „Überwachung von Nachrichten" umfasst laut auf den im Gesetzesentwurf verwiesenen § 134 Z 3 StPO Nachrichten und Informationen, die von einer natürlichen Person über ein Kommunikationsnetz oder einen Dienst der Informationsgesellschaft gesendet, übermittelt oder empfangen werden. Es handelt sich um unverschlüsselte Daten, die über das Kommunikationsnetz des Betreibers ausgeleitet werden können.

Von einer Überwachung wären somit nicht nur, wie öffentlich diskutiert, „Chats" erfasst. Vielmehr sollen dadurch alle Nachrichten und Informationen, die über internetbasierte Apps übermittelt werden, überwacht werden können. Denkbar sind unter anderen Textnachrichten, Skype-Telefonate, Dateien, Fotos, allenfalls auch Kalendereinträge, E-Mails, oder Chatnachrichten. Gemäß den Erläuterungen sind davon auch Datenpakete, die von einem Cloud-Diensteanbieter an einen Cloud-Server übermittelt werden, umfasst. Somit könnten auch Bilder, Dateien und sonstige Daten, die „händisch" (also nicht automatisch) in eine Cloud (z.B. OneDrive, Google Drive, Dropbox, etc.) hochgeladen werden, zum Beispiel um sie zu sichern oder zu teilen, überwacht werden. Das könnte auch Daten aus dem höchstpersönlichen Lebensbereich betreffen, wie z.B. gesundheitliche Befunde des Menschen, der gezielt überwacht wird, aber auch anderer Menschen in seinem*ihrem persönlichen Umfeld.

Im Zuge der geheimen Überwachungsmaßnahme werden zudem nicht nur Daten der zu überwachenden Person umfasst, sondern auch Daten von Menschen, die mit dieser Person im Kontakt stehen. Somit könnten auch Menschen betroffen sein, die nicht notwendigerweise eines verfassungsgefährdenden Angriffs verdächtig sind bzw. von denen nicht eine schwere Gefahr für die öffentliche Sicherheit verbundener Kriminalität ausgeht.

Bei der Überwachung von Nachrichten und Informationen nach dem vorgesehenen § 11 Abs. 1 Z 8 SNG würde somit besonders intensiv in individuelle Freiheiten von Menschen eingegriffen, die selbst nicht das Ziel der Überwachung sind. Die menschenrechtlichen Folgen dieses Eingriffes in die Korrespondenzfreiheit (Artikel 8 EMRK) werden in den Erläuterungen nicht behandelt und es wird keine Rechtfertigung für diesen Eingriff geliefert. Es ist daher nicht nachvollziehbar und bleibt fragwürdig, ob und inwiefern hier die menschenrechtlich erforderliche Verhältnismäßigkeitsprüfung durchgeführt wurde und ob evaluiert wurde, ob es sich um das geeignete und zugleich gelindeste Mittel handelt, um den an sich legitimen Zweck, nämlich die Prävention möglicher terroristischer Straftaten, zu erreichen.

Die Rolle des Rechtsschutzbeauftragten

Wenn sich laut dem vorgeschlagenen § 15a Abs. 8 SNG ein begründeter Gefahrenverdacht „für einen anderen" verfassungsgefährdenden Angriff, als für jenen, für den die Überwachung ursprünglich vom BVwG bewilligt wurde, ergibt, dann ist diese Überwachung vom Rechtsschutzbeauftragten zu genehmigen. Es ist nicht nachvollziehbar, wieso der Rechtsschutz hier schwächer ausgeprägt ist und nicht zusätzlich eine richterliche Bewilligung durch das BVwG erforderlich ist.

Die laufende Prüfung, Bewilligung und Kontrolle der Durchführung der Überwachung soll nach § 11 Abs. 1 Z 8 SNG durch den Rechtsschutzbeauftragten erfolgen. § 14 Abs. 4 SNG sieht zudem vor, dass dem Rechtsschutzbeauftragten drei Tage zustehen, um sich zum Antrag auf Bewilligung der DSN an das BVwG zu äußern.

Durch diese Gesetzesänderung würde der Rechtsschutzbeauftragte umfassende neue Aufgaben bekommen und für die Kontrolle einer Menge neuer Daten zuständig sein. Dies (angenommen der Fiktion, dass es überhaupt möglich ist) soll neben der höchstaufwendigen Kontrolle des Einsatzes von Spyware, die für sich alleine schon eine hohe IT-Expertise und ausreichende Ressourcen verlangt, erfolgen. Der Gesetzesentwurf sieht keinerlei organisatorischen Maßnahmen vor, wie sichergestellt

[23] EGMR 4.5.2000, Rotaru / Rumänien, Z. 59

werden soll, dass der Rechtsschutzbeauftragte ausreichend IT-Expertise, Ausstattung sowie personelle und zeitliche Ressourcen zur Verfügung hat, um die Kontrolle von der Überwachung von Unmengen an Daten auch wirksam durchzuführen.

Angesichts des fortschreitenden Ausbaus polizeilicher Überwachungsbefugnisse hat Amnesty International Österreich Bedenken, inwiefern der Rechtsschutzbeauftragte – dessen tatsächliche Unabhängigkeit dahingestellt bleiben soll – angesichts immer neuer und technisch anspruchsvollerer Überwachungsmaßnahmen tatsächlich effektiven Rechtsschutz gewährleisten kann. Diese Bedenken äußerte auch der Verfassungsgerichtshof, als er die Bestimmungen zum Einsatz des Bundestrojaners als verfassungswidrig aufhob.[24]

§ 11 Abs. 1 Z 5 und Z 7 SNG

Amnesty International Österreich hat zum Einsatz von IMSI-Catchern bereits im Rahmen der Strafrechtsreformen 2017 bzw. 2018 Stellung genommen und aus menschenrechtlicher Sicht kritisch bewertet.

Weder in den Erläuterungen noch im Gesetz wird ausgeführt, durch welche technische Mittel „IMSI" festgestellt werden sollen. Es ist aber anzunehmen, dass dafür sogenannte „IMSI-Catcher" eingesetzt werden sollen. Das ist ein Gerät, das ein Mobilfunknetzwerk simuliert und in dem sich alle Mobiltelefone in einem gewissen Umkreis aufgrund ihres stärksten Signals einbuchen. Diese ermöglichen die präzise Ortung eines Mobiltelefons innerhalb einer Funkzelle ohne Mitwirkung der Kommunikationsdiensteanbieter*innen. Aus menschenrechtlicher Perspektive ist vorauszuschicken, dass die Verwendung dieser Ermittlungsmaßnahme in das Privatleben aller Personen eingreift, die sich im Umkreis des Geräts befinden. Somit auch Personen, die nicht notwendigerweise eines verfassungsgefährdenden Angriffs verdächtig sind bzw. von denen nicht eine schwere Gefahr für die öffentliche Sicherheit verbundener Kriminalität ausgeht. Es werden etwa zwangsläufig die Daten von sämtlichen im Netzbereich des „IMSI-Catchers" befindlichen Personen erfasst. „IMSI-Catcher" ermöglichen den Sicherheitsbehörden in technischer Hinsicht neben der Lokalisierung des angesteuerten Endgerätes auch die Überwachung – also das Mithören – von Mobiltelefongesprächen.

Es besteht somit die immanente Gefahr, dass die Sicherheitsbehörden „IMSI-Catcher" für Ermittlungen zur Gewinnung von Nachrichteninhalten heranziehen, ohne dass ein für die Ermittlungsmaßnahme vorausgesetzter Verdacht oder Gefahr iSd § 6 Abs. 1 und 2 SNG gegeben ist. Das öffnet die Tür für Missbrauch und Massenüberwachung. Dem Gesetzesentwurf oder den Erläuterungen sind keine geeigneten rechtlichen, technischen und organisatorischen Maßnahmen zu entnehmen, mit denen solch ein Missbrauch vorgebeugt werden kann. Unbeteiligte Menschen werden auch nicht sofort darüber informiert, dass sie von dieser Ermittlungsmaßnahme betroffen sind und ein Eingriff in ihre Korrespondenzfreiheit erfolgt.

Ähnlich verhält es sich mit der Ermittlungsmaßnahme in § 11 Abs. 1 Z 7. Laut den Erläuterungen sollen insbesondere WLAN-Catcher eingesetzt werden, um ohne Mitwirkung der Anbieter*innen Verkehrsdaten, Zugangsdaten und Standortdaten zu beschaffen. Dadurch können Metadaten von allen Geräten ausgelesen werden, die sich im gegenständlichen Netz befinden. Auch hier befürchtet Amnesty International Österreich, dass davon völlig unbeteiligte Personen betroffen sein könnten, die mit ihren Endgeräten das WLAN benutzen und so, ohne darüber Kenntnis zu erlangen, überwacht werden können.

Amnesty International Österreich befürchtet, dass sowohl der Einsatz von IMSI-Catcher, als auch der Einsatz von WLAN-Catcher dazu geeignet sein könnten, unverhältnismäßig in die Menschenrechte von Dritten einzugreifen.

[24] VfSlg 20.356/2019

ANNEX: AMNESTY INTERNATIONALS UNTERSUCHUNGEN UND POSITION ZUM EINSATZ VON HOCHINVASIVER SPYWARE IM DETAIL

Pegasus, Predator & Co: Überwachung von Zivilgesellschaft, Menschenrechtsverteidiger*innen und Journalist*innen mit ernsthaften Folgen.

Überwachungstechnologien eröffnen viele Möglichkeiten, Menschen bis in ihr Innerstes zu überwachen, inklusive ihrer intimsten Geheimnisse. Die Macht dieser Tools verleitet daher sehr leicht zu Missbrauch. Untersuchungen und aktuelle Medienberichte zeigen, wie hochinvasive Spyware weltweit missbräuchlich gegen die Zivilgesellschaft, Menschenrechtsverteidiger*innen und Journalist*innen eingesetzt wird.

Im Juli 2021 deckte Amnesty International gemeinsam mit dem Journalist*innennetzwerk Forbidden Stories auf, wie Staaten weltweit die von der NSO Group verkaufte Spyware Pegasus in massivem Ausmaß dazu nutzten, um Journalist*innen, Anwält*innen, Menschenrechtsverteidiger*innen, NGO-Mitarbeiter*innen, Beamt*innen und Politiker*innen, inklusive Staatsoberhäupter, ins Visier zu nehmen und widerrechtlich zu überwachen. Die Untersuchung hatten mindestens 180 Journalist*innen in 20 Ländern identifiziert, die zwischen 2016 und Juni 2021 für potenzielle Angriffe mit der NSO-Spyware ausgewählt wurden, darunter in Aserbaidschan, Ungarn, Indien und Marokko – alles Länder, in denen das harte Durchgreifen gegen unabhängige Medien verstärkt wurde.

Pegasus wurde zum Beispiel auch auf den Telefonen von Personen im Umfeld des saudischen Journalisten Jamal Khashoggi entdeckt, der in Istanbul ermordet wurde. Ihre Telefone, ihre physische Umgebung und ihre Kommunikation mit Khashoggi konnten so – teilweise über Jahre hinweg – von saudischen Agenten überwacht werden. Auch nach seinem Tod wurden Familienangehörige und Kolleg*innen weiterhin überwacht.[25]

Danach begannen zwar das Europäische Parlament und einige EU-Mitgliedstaaten Untersuchungen und machten öffentliche Erklärungen, Empfehlungen und Versprechen, um gegen den Missbrauch von Spyware vorzugehen. Trotz dieser Maßnahmen gibt es bis heute keine sinnvolle Regelung zur Verhinderung des Missbrauchs von Spyware. Die betroffenen Personen, deren Geräte unrechtmäßig mittels Spyware infiltriert wurden und die sohin von unrechtmäßiger gezielter und menschenrechtswidriger Überwachung betroffen, waren mit einem eklatanten Mangel an Rechenschaftspflicht, Abhilfe bzw. Wiedergutmachung von Seiten der Verursacher*innen konfrontiert. Zahlreiche Staaten haben Ermittlungen auf Eis gelegt und verabsäumt, für Transparenz zu sorgen.[26]

Seither dokumentieren Forscher*innen der Zivilgesellschaft weiterhin Fälle von unrechtmäßiger gezielter Überwachung und Missbrauch von Spyware. Berichten zufolge wurde zum Beispiel zwischen April und August 2021 eine Mitarbeiterin der Menschenrechtsorganisation Human Rights Watch aufgrund ihrer Arbeit mit Pegasus überwacht.[27]

Im Oktober 2023 enthüllten Untersuchungen von Amnesty International und dem EIC-Mediennetzwerk zudem, dass die Europäische Union beim Verkauf von hochentwickelter Überwachungstechnologien weiterhin keine wirksamen Kontrollen von Unternehmen vornimmt. So verkaufte die Gruppe Intellexa alliance ihre hochinvasive Spyware Predator weltweit auch an Staaten, die sie einsetzen, um

---

[25] Amnesty International, *Pegasus-Projekt in Zusammenarbeit mit Amnesty: Aktivist*innen, Journalist*innen und Politiker*innen weltweit mit NSO-Spyware ausgespäht*, 19.7.2021 https://www.amnesty.at/news-events/news/pegasus-projekt-in-zusammenarbeit-mit-amnesty-aktivist-innen-journalist-innen-und-politiker-innen-weltweit-mit-nso-spyware-ausgespaeht/
Wikipedia, *Pegasus (Spyware)*, https://de.wikipedia.org/wiki/Pegasus_(Spyware)

[26] Amnesty International, *The Predator Files: caught in the net*, 9.10.2023, Seite 40
https://www.amnesty.org/en/documents/act10/7245/2023/en/

[27] https://www.hrw.org/de/news/2022/01/26/human-rights-watch-mittels-pegasus-spyware-ueberwacht

Menschenrechte, wie zum Beispiel Pressefreiheit zu unterdrücken. Zu den 25 Ländern, in die die Technologien verkauft wurden, gehörten auch Österreich, Deutschland und die Schweiz.[28]

Im Dezember 2023 deckten Untersuchungen von Amnesty International und The Washington Post auf, wie indische Journalist*innen mit der Spyware Pegasus ins Visier genommen und überwacht wurden.[29]

Im Februar 2024 wurden Berichten zufolge auch Mitglieder des Europäischen Parlaments im Vorfeld der Europawahlen im Juni mit Spyware ausgespäht.[30] Im April 2024 wurde bekannt, dass die frühere polnische Regierung offenbar auch die damalige Opposition während des Wahlkampfes höchstwahrscheinlich unrechtmäßig mit der Spyware Pegasus hatte überwachen lassen.[31]

Hochinvasive Spyware wird nachweislich von Staaten weltweit missbraucht, um Zivilgesellschaft, Journalist*innen und Menschenrechtsverteidiger*innen zu verfolgen. Der Einsatz von hochinvasiver Spyware muss aufgrund der damit verbundenen Risiken für die Menschenrechte weltweit verboten werden.

[28] heise.de, *Predator Files: Wie deutsche Geldgeber und der Staat mächtige Spyware fördern,* 7.10.2023 https://www.heise.de/news/Predator-Files-Wie-deutsche-Geldgeber-und-der-Staat-maechtige-Spyware-foerdern-9327419.html ; Amnesty International, *Amnesty-Untersuchung „Predator Files" enthüllt Angriffe durch Überwachungssoftware auf die Zivilgesellschaft, Politiker*innen und staatliche Stellen*, 9.10.2023 https://www.amnesty.at/presse/amnesty-untersuchung-predator-files-enthuellt-angriffe-durch-%C3%BCberwachungssoftware-auf-die-zivilgesellschaft-politiker-innen-und-staatliche-stellen/
Amnesty International, *The Predator Files: caught in the net*, 9.10.2023 https://www.amnesty.org/en/documents/act10/7245/2023/en/

[29] Amnesty International, *India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists*, 28.12.2023 https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/
Der Standard, *Indien überwacht Journalisten mit Pegasus-Software*, 28.12.2023 https://www.derstandard.at/story/3000000201146/indien-ueberwacht-journalisten-mit-pegasus-software

[30] Politico, *Brussels spyware bombshell: Surveillance software found on officials' phones*, https://www.politico.eu/article/parliament-defense-subcommittee-phones-checked-for-spyware/

[31] Der Spiegel, *Polnische PiS-Regierung hat Pegasus wohl hundertfach im eigenen Land eingesetzt*, 17.4.2024 https://www.spiegel.de/ausland/polen-pis-regierung-setzte-israelische-spionagesoftware-pegasus-wohl-hundertfach-ein-a-cc6953d8-0e92-4291-aa76-15484f9ea12b