Sachstand

Fragen zu sogenannter Spionagesoftware

Fragen zu sogenannter Spionagesoftware

Aktenzeichen: WD 3 - 3000 - 140/22, WD 7 - 3000 - 096/22, WD 8 - 3000 - 075/22
Abschluss der Arbeit: 28.10.2022
Fachbereich: WD 3: Verfassung und Verwaltung (Punkt 1.1 und 2.1)
WD 7: Zivil-, Straf- und Verfahrensrecht, Bau und Stadtentwicklung (Punkt 1.2, 2.2 und 2.3, Punkt 3)
WD 8: Umwelt, Naturschutz, Reaktorsicherheit, Bildung und Forschung (Punkt 4)

(Stand aller Internetquellen: 25.10.2022)

Inhaltsverzeichnis

1. Rechtlicher Rahmen für den Einsatz von sogenannter Spionagesoftware

Die deutsche Rechtsordnung unterscheidet in Bezug auf den Einsatz sogenannter Spionagesoftware zwischen der sogenannten Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und der sogenannten Online-Durchsuchung. Das Instrument der Quellen-TKÜ steht den Nachrichtendiensten des Bundes, dem Bundeskriminalamt (BKA) sowie den Strafverfolgungsbehörden im Ermittlungsverfahren zur Verfügung. Letztere sind auch zur Durchführung von Online-Durchsuchungen berechtigt. Gleiches gilt für das BKA zum Zwecke der Abwehr von Gefahren des internationalen Terrorismus. Zu nachrichtendienstlichen Zwecken darf die Online-Durchsuchung hingegen nur in sehr beschränktem Maße eingesetzt werden.

1.1. Einsatz durch Nachrichtendienste und Bundeskriminalamt

Organisation, Aufgaben und Befugnisse der drei Nachrichtendienste des Bundes, der **Bundesnachrichtendienst (BND)**, das **Bundesamt für Verfassungsschutz (BfV)** und der **Militärische Abschirmdienst (MAD)**, sind jeweils im Gesetz über den Bundesnachrichtendienst[1], dem Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz[2] sowie dem Gesetz über den Militärischen Abschirmdienst[3] geregelt. Nach Maßgabe des Artikel 10-Gesetzes[4] sind die Verfassungsschutzbehörden des Bundes und der Länder, der MAD und der BND unter bestimmten Voraussetzungen berechtigt, insbesondere zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes die Telekommunikation zu überwachen und aufzuzeichnen (vgl. § 1 Abs. 1 Artikel 10-Gesetz).

Durch eine Änderung des Artikel 10-Gesetzes im Jahr 2021 wurde die sogenannte erweiterte Quellen-TKÜ für die Nachrichtendienste eingeführt (vgl. § 11 Abs. 1a Artikel 10-Gesetz). Diese dient der Überwachung von Kommunikation über Kommunikationsprogramme, die standardmäßig eine Verschlüsselung ihrer Kommunikationsdaten und -inhalte nutzen. Die Quellen-TKÜ erfasst Kommunikation, bevor diese verschlüsselt oder nachdem diese entschlüsselt wurde bzw. ermöglicht deren Entschlüsselung, indem sie auf das verwendete Endgerät (die „Quelle“) zugreift.[5] Dazu bedarf es einer **speziellen Überwachungssoftware**, welche umgangssprachlich als Staatstrojaner bezeichnet

---

1 Gesetz über den Bundesnachrichtendienst vom 20.12.1990 (BGBl. I S. 2954, 2979), zuletzt geändert durch Artikel 3 des Gesetzes vom 05.07.2021 (BGBl. I S. 2274).

2 Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz vom 20.12.1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Artikel 1 des Gesetzes vom 05.07.2021 (BGBl. I S. 2274).

3 Gesetz über den militärischen Abschirmdienst vom 20.12.1990 (BGBl. I S. 2954, 2977), zuletzt geändert durch Artikel 2 des Gesetzes vom 05.07.2021 (BGBl. I S. 2274).

4 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses vom 26.06.2001 (BGBl. I S. 1254, 2298; 2017 I S. 154), zuletzt geändert durch Artikel 6 Absatz 4 des Gesetzes vom 05.07.2021 (BGBl. I S. 2274).

5 Bundeskriminalamt, Quellen-TKÜ und Online-Durchsuchung: Notwendigkeit, Sachstand und Rahmenbedingungen, abrufbar unter https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/Quellentkue-Onlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html.

wird.[6] Dabei erlaubt § 11 Abs. 1a Satz 1 Artikel 10-Gesetz die Überwachung und Aufzeichnung der **laufenden Kommunikation.** § 11 Abs. 1a Satz 2 gestattet darüber hinaus auch die Überwachung der auf dem informationstechnischen System des Betroffenen ab dem Zeitpunkt der Anordnung gespeicherten Inhalte und Umstände der Kommunikation **(ruhende Kommunikation)**, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätte überwacht und aufgezeichnet werden können Bei diesem Zugriff auf ruhende Kommunikation, zu dem § 11 Abs. 1a Satz 2 Artikel 10-Gesetz ermächtigt, handelt es sich um die **„erweiterte" Quellen-TKÜ**, die insofern zum Teil auch als eine beschränkte Online-Durchsuchung bezeichnet und bewertet wird.[7] Der Zugriff auf das zu überwachende Gerät kann auch aus der Ferne, das heißt nicht physisch, erfolgen, indem Sicherheitslücken im System des Endgeräts ausgenutzt werden, um die Installation einer Überwachungssoftware zu ermöglichen.[8]

Neben der Quellen-TKÜ gibt es zudem die sogenannte verdeckte **Online-Durchsuchung**, bei der die Behörde ebenfalls mit technischen Mitteln in die von der betroffenen Person genutzte informationstechnische Systeme (IT-Systeme) eingreift und aus ihnen Daten erhebt. Sie unterscheidet sich von der Quellen-TKÜ darin, dass sie nicht auf die Überwachung laufender Telekommunikation beschränkt ist. Eine Online-Durchsuchung ist nur bei Bestehen einer besonderen gesetzlichen Ermächtigung zulässig.[9] Seit einer Gesetzesänderung[10] des Bundesnachrichtendienstgesetzes im Jahr 2021 ist der BND zu Online-Durchsuchungen bei Ausländern im Ausland berechtigt (vgl. § 34 BNDG). Das BfV und der MAD dürfen keine Online-Durchsuchungen durchführen, soweit man nicht die erweiterte Quellen-TKÜ nach § 11 Abs. 1a Satz 2 Artikel 10-Gesetz als Online-Durchsuchung einstuft.

Zur Abwehr von Gefahren des internationalen Terrorismus kann auch das **BKA** auf IT-Systeme zugreifen. Dazu kann es das **Mittel der Quellen-TKÜ einsetzen** (§ 51 Abs. 2 BKAG). Zur Durchführung

---

6 Wissenschaftliche Dienste des Deutschen Bundestages, Ausarbeitung WD 3 - 3000 - 293/20, Verfassungsrechtliche Fragen zur Regelung des Einsatzes von Quellen-Telekommunikationsüberwachung durch Nachrichtendienste - Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts der Bundesregierung, S. 4, abrufbar unter: https://www.bundestag.de/resource/blob/830002/3a1ed4b31d92b8575b3f31e496128d8f/WD-3-293-20-pdf-data.pdf.

7 Poscher/Kappler, Staatstrojaner für Nachrichtendienste – Zur Einführung der Quellen-Telekommunikationsüberwachung im Artikel 10-Gesetz, Verfassungsblog, 06.07.2021 (https://verfassungsblog.de/staatstrojaner-nachrichtendienste/); vgl. auch Wissenschaftliche Dienste des Deutschen Bundestages, Ausarbeitung WD 3 - 3000 - 293/20, Verfassungsrechtliche Fragen zur Regelung des Einsatzes von Quellen-Telekommunikationsüberwachung durch Nachrichtendienste - Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts der Bundesregierung, S. 7.

8 Martini/Fröhlingsdorf, Catch me if you can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik, Netzpolitik.org, 06.02.2021, https://netzpolitik.org/2021/catch-me-if-you-can-quellen-telekommunikationsueberwachung-zwischen-recht-und-technik/.

9 BVerfGE 120, 274.

10 Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts vom 19.04.2021 (BGBl. I S. 771).

dieser und weiterer Maßnahmen verfügt das BKA sowohl über eigenentwickelte als auch über kommerzielle Software.[11] Darüber hinaus kann es Online-Durchsuchungen durchführen (vgl. § 49 BKAG). Laut eigener Angaben werden die hierzu verwendeten Softwares einem umfangreichen Testverfahren unterzogen.[12]

Die zu Quellen-TKÜ oder Online-Durchsuchungen befugten Sicherheitsbehörden sind gemäß geltendem Recht an die jeweiligen inhaltlichen **Tatbestandsvoraussetzungen** gebunden.[13] Ein Einsatz von Überwachungssoftware außerhalb dieses gesetzlichen Rahmens ist nicht gestattet.

1.2. Einsatz durch Strafverfolgungsbehörden

Zudem kann Spionagesoftware im Rahmen eines **Ermittlungsverfahrens durch Strafverfolgungsbehörden** eingesetzt werden. Abhängig von der konkreten Funktionsweise der Software kommt eine Zulässigkeit der Verwendung als Telekommunikationsüberwachung nach § 100a der Strafprozessordnung (StPO)[14] oder als Onlinedurchsuchung nach § 100b StPO in Betracht. Die Vorschriften sind **technikneutral** formuliert und können daher grundsätzlich auch den Einsatz von Spionagesoftware rechtfertigen.[15] Allerdings unterliegen diese Ermittlungsmaßnahmen strengen Voraussetzungen. So setzen sie etwa den Verdacht einer schweren oder besonders schweren Straftat voraus (§ 100a Abs. 1 Satz 1 Nr. 1, Abs. 2 StPO, § 100b Abs. 1 Nr. 1, Abs. 2 StPO). Weiter sind die Maßnahmen unzulässig, wenn Anhaltspunkte vorliegen, dass durch die Maßnahmen allein Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung erlangt werden (§ 100d Abs. 1 StPO). Zudem kann eine Anordnung dieser Maßnahmen grundsätzlich allein auf Antrag der Staatsanwaltschaft durch das Gericht erfolgen (§ 100e Abs. 1 Satz 1 StPO).

Wird die Spionagesoftware **durch Unberechtigte** eingesetzt, können Straftatbestände einschlägig sein. Zwar sieht das deutsche Strafrecht keine Vorschrift vor, die allein die unbefugte Verwendung einer Spionagesoftware unter Strafe stellt. Doch können Straftatbeständen erfüllt sein, die allgemein der Abwehr von Daten- und Cyberkriminalität dienen. Die strafrechtliche Bewertung hängt

---

11 Bundeskriminalamt, Quellen-TKÜ und Online-Durchsuchung: Notwendigkeit, Sachstand und Rahmenbedingungen, abrufbar unter https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html.

12 Bundeskriminalamt, Quellen-TKÜ und Online-Durchsuchung: Notwendigkeit, Sachstand und Rahmenbedingungen, abrufbar unter https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html.

13 Antwort der Bundesregierung, EU-Maßnahmen gegen Verschlüsselung unter deutscher Beteiligung, BT-Drs. 19/26112, S. 5.

14 Strafprozessordnung in der Fassung der Bekanntmachung vom 07.04.1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 des Gesetzes vom 25.03.2022 (BGBl. I S. 571) geändert worden ist, abrufbar unter: https://www.gesetze-im-internet.de/stpo/.

15 Antwort der Bundesregierung, Einsatz der Spionagesoftware „Pegasus“ in Deutschland, BT-Drs 19/32246, S. 5, abrufbar untrer: https://dserver.bundestag.de/btd/19/322/1932246.pdf.

maßgeblich von den **Umständen des Einzelfalls** ab. Denkbar erscheinen insbesondere die folgenden Delikte:

Verschafft sich der Täter durch den Einsatz einer Spionagesoftware unbefugt Zugang zu Daten, kommt eine Strafbarkeit wegen des **Ausspähens von Daten** (§ 202a Strafgesetzbuch – StGB[16]) in Betracht, wenn die Daten nicht für den Täter bestimmt und gegen einen fremden Zugang besonders gesichert sind. Daneben könnte eine Strafbarkeit wegen des **Abfangens von Daten** (§ 202b StGB) vorliegen, wenn der Täter sich oder Dritten unbefugt und unter Anwendung technischer Mittel Daten verschafft, die nicht für ihn bestimmt sind und aus einer nicht-öffentlichen Datenübermittlung oder eine Datenverarbeitungsanlage stammen. Im Kontext dieser Delikte steht auch § 202c StGB, der die **Vorbereitung** der Straftaten nach den §§ 202a, 202b StGB unter Strafe stellt, wenn entweder Passwörter und sonstige Sicherungscodes oder Computerprogramme, die dem Ausspähen oder Abfangen von Daten dienen, hergestellt, verschafft, verkauft, überlassen, verbreitet oder sonst zugänglich gemacht werden.

Werden durch den Einsatz der Spionagesoftware Daten auf dem betroffenen Endgerät geändert, unterdrückt, gelöscht oder unbrauchbar gemacht, kann eine Strafbarkeit wegen **Datenveränderung** nach § 303a StGB vorliegen. Wird durch die Spionagesoftware auch die Datenverarbeitung des betroffenen Endgeräts erheblich gestört, könnte im Einzelfall eine **Computersabotage** (§ 303b StGB) anzunehmen sein.

Weiter kann eine Strafbarkeit wegen der **Verletzung der Vertraulichkeit des Wortes** (§ 201 StGB) begründet sein, wenn die Spionagesoftware die Aufnahme des nicht-öffentlich gesprochenen Wortes einer anderen Person ermöglicht.

Werden Daten, die durch einen rechtswidrigen Einsatz von Spionagesoftware erlangt wurden, Dritten zugänglich gemacht, kann eine Strafbarkeit wegen **Datenhehlerei** (§ 202d StGB) vorliegen, wenn die betroffenen Daten nicht ohnehin allgemein zugänglich sind.

Sind personenbezogene Daten betroffen, kommt auch eine Strafbarkeit nach dem **Bundesdatenschutzgesetz** (BDSG)[17] in Betracht, wenn entweder gewerbsmäßig personenbezogenen Daten einer großen Anzahl an Personen Dritten zugänglich gemacht wurden (§ 42 Abs. 1 BDSG) oder personenbezogene Daten gegen ein Entgelt oder mit Bereicherungsabsicht unrechtmäßig verarbeitet oder erschlichen wurden (§ 42 Abs. 2 BDSG).

16 Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), das zuletzt durch Artikel 1 des Gesetzes vom 11.07.2022 (BGBl. I S. 1082) geändert worden ist, abrufbar unter: https://www.gesetze-im-internet.de/stgb/.

17 Bundesdatenschutzgesetz (BDSG) vom 30.06.2017 (BGBl. I S. 2097), das zuletzt durch Artikel 10 des Gesetzes vom 23.06.2021 (BGBl. I S. 1858; 2022 I 1045) geändert worden ist, abrufbar unter: https://www.gesetze-im-internet.de/bdsg_2018/.

2. Vorkehrungen, Rechtsmittel und Kompensation bei rechtswidrigen Eingriffen

Die Rechtsmittel der Betroffenen hängen im Wesentlichen davon ab, ob der Einsatz der Spionagesoftware durch den Staat oder durch Private erfolgte.

2.1. Einsatz durch Nachrichtendienste und Bundeskriminalamt

Sofern der **Zugriff auf ein informationstechnisches System durch den Staat** erfolgt und sich auf die laufende Kommunikation bezieht, ist die Maßnahme an Art. 10 Grundgesetz (GG)[18] zu messen, welcher das **Telekommunikationsgeheimnis** gewährleistet.

Die darüber hinaus gehende Überwachung der Nutzung eines informationstechnischen Systems als solches oder die Durchsuchung von Speichermedien des Systems muss den gesteigerten Anforderungen des **Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sogenanntes IT-Grundrecht)** gerecht werden, welches das Bundesverfassungsgericht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG abgeleitet hat.[19]

Die **Zulässigkeitsvoraussetzungen** für die Durchführung einer Quellen-TKÜ oder einer Online-Durchsuchung durch die Nachrichtendienste oder das BKA sind in den jeweiligen Gesetzen geregelt. Diese stellen insbesondere auch technische Voraussetzungen an die eingesetzten Mittel.[20] Die Voraussetzungen gelten jeweils für alle Formen der Quellen-TKÜ und Online-Durchsuchungen, also auch solche, die gegebenenfalls mithilfe von Spionagesoftwares durchgeführt werden. Der Einsatz solcher Softwares muss sich jedoch an den rechtlichen Maßgaben der Befugnisnormen orientieren. Bedenken hinsichtlich hochkompetenter Softwares resultieren daraus, dass diese zu weitgehenden Eingriffen fähig sind, die über den Rahmen rechtlich zulässiger Maßnahmen hinausgehen.[21]

Zudem enthalten die Gesetze Vorschriften zur **Mitteilung oder Benachrichtigung der betroffenen Personen**. Die Durchführung einer Quellen-TKÜ durch die Nachrichtendienste ist dem Betroffenen nach ihrer Einstellung mitzuteilen. Dies kann jedoch unterbleiben, solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann oder solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist (§ 12 Abs. 1 Satz 1 und 2 Artikel 10-Gesetz). Zudem ist der Rechtsweg vor der Mitteilung gemäß § 13 Artikel 10-Gesetz ausgeschlossen. Hinsichtlich Quellen-TKÜ und Online-Durchsuchungen durch das BKA finden sich ähnliche Mitteilungspflichten in § 74 BKAG. Werden hingegen personenbezogene Daten von

---

18 Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 1 des Gesetzes vom 28.06.2022 (BGBl. I S. 968).

19 BVerfGE 120, 274 ff.

20 Vgl. etwa § 11 Abs. 1a Satz 3 Nr. 1 Artikel-10 Gesetz; § 49 Abs. 2 BKAG, auf den auch § 51 Abs. 2 BKAG verweist; § 34 Abs. 4 BNDG.

21 Vgl. etwa Baars/Flade/Mascolo, Pegasus-Software: Darf's ein bisschen mehr sein, Tagesschau, 19.07.2021, abrufbar unter: https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-deutschland-101.html.

Ausländern im Ausland durch den BND erhoben, erfolgt grundsätzlich keine Mitteilung an die betroffene Person (§ 59 Abs. 1 BNDG).

Eine **Kompensation** im Falle von Eingriffen in Grundrechte durch Überwachungsmaßnahmen ist in den Gesetzen der Nachrichtendienste bzw. des BKA nicht vorgesehen. Sofern eine Maßnahme der Sicherheitsbehörden unrechtmäßig ist, kommen für den Betroffenen jedoch die Instrumente des allgemeinen Staatshaftungsrechts in Betracht.

Die Tätigkeit des BKA und der deutschen Nachrichtendienste unterliegt **gerichtlicher Kontrolle** sowie der **Fach- und Rechtsaufsicht** der für sie zuständigen Regierungsressorts (Bundeskanzleramt, Bundesministerium des Innern und für Heimat, Bundesministerium der Verteidigung). Für die **parlamentarische Kontrolle** der nachrichtendienstlichen Tätigkeit des Bundes gibt es zudem das Parlamentarische Kontrollgremium des Bundestages nach § 14 Artikel 10-Gesetz. Das Parlamentarische Kontrollgremium wiederum wählt die Mitglieder der sogenannten **G 10-Kommission**. Telekommunikationsüberwachungsmaßnahmen der Nachrichtendienste dürfen grundsätzlich nur mit ihrer vorherigen Zustimmung durchgeführt werden (vgl. § 15 Artikel 10-Gesetz). Online-Durchsuchungen des BND bedürfen grundsätzlich der vorherigen Zustimmung durch einen **Unabhängigen Kontrollrat**, der aus ehemaligen Richtern des Bundesgerichtshofs und des Bundesverwaltungsgerichts besteht, die auf Vorschlag der Bundesregierung vom Parlamentarischen Kontrollgremium des Bundestags gewählt werden (§ 37 Abs. 4, § 43 BNDG). Daneben unterliegt die Tätigkeit der Nachrichtendienste auch dem allgemeinen parlamentarischen Fragerecht, der Kontrolle der für das jeweilige Regierungsressort zuständigen Fachausschüsse sowie gegebenenfalls vom Bundestag eingesetzter Untersuchungsausschüsse. Telekommunikationsüberwachungen und Online-Durchsuchungen durch das BKA bedürfen der vorherigen **richterlichen Genehmigung** (§ 49 Abs. 4, § 51 Abs. 3 BKAG).

2.2. Einsatz durch Strafverfolgungsbehörden

Wurde die Spionagesoftware von **Strafverfolgungsbehörden** im Rahmen von **Ermittlungsmaßnahmen** nach den §§ 100a, 100b StPO eingesetzt, müssen betroffene Personen von den Ermittlungsbehörden über die Maßnahmen informiert werden, sobald der Untersuchungszweck der Ermittlungsmaßnahmen hierdurch nicht mehr gefährdet wird (§ 101 Abs. 1, Abs. 4 Nr. 3, 4, Abs. 5 StPO). Die betroffenen Personen können bis zu zwei Wochen nach dieser Benachrichtigung eine **gerichtliche Überprüfung** der Rechtmäßigkeit der Maßnahmen sowie der Art und Weise ihres Vollzugs beantragen (§ 101 Abs. 7 Satz 2 StPO).

2.3. Einsatz durch Private

Hat eine **private Person** eine Spionagesoftware zum Nachteil einer anderen Person eingesetzt, kommt zur unmittelbaren Abwehr des Einsatzes der Spionagesoftware zunächst ein zivilrechtlicher **Unterlassungsanspruch** aus § 1004 Abs. 1 Satz 1 des Bürgerlichen Gesetzbuchs (BGB)[22] in Betracht. Denn durch den unbefugten Einsatz der Spionagesoftware könnte eine Störung des Eigentums (oder des Besitzes) an dem Endgerät vorliegen, zu deren Duldung der Betroffene nicht verpflichtet ist. Als

22 Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 02.01.2002 (BGBl. I S. 42, 2909; 2003 I S.738), das zuletzt durch Artikel 4 des Gesetzes vom 15.07.2022 (BGBl. I S. 1146) geändert worden ist, abrufbar unter: https://www.gesetze-im-internet.de/bgb/.

Rechtsfolge könnte der Betroffene die Beseitigung der Beeinträchtigung verlangen und – soweit weitere Beeinträchtigungen zu besorgen sind – den Verwender zu einer künftigen Unterlassung verpflichten (§ 1004 Abs. 1 Satz 2 BGB).

Daneben könnte den Betroffenen ein zivilrechtlicher Anspruch auf **Schadensersatz** gegen die Verwender der Spionagesoftware zustehen. Taugliche Anspruchsgrundlagen könnten insbesondere die deliktischen Schadensersatzansprüche des § 823 Abs. 1 BGB und des § 823 Abs. 2 BGB (in Verbindung mit verletzten Schutzgesetzen) sowie die Schadensersatzpflicht wegen einer vorsätzlichen sittenwidrigen Schädigung nach § 826 BGB sein. Gemein ist den Schadensersatzansprüchen, dass sie einen **ersatzfähigen Schaden** voraussetzen. Ein solcher liegt jedenfalls dann vor, wenn dem Betroffenen durch den Einsatz der Spionagesoftware ein **Vermögensschaden** (materieller Schaden) entstanden ist, denn dieser ist nach den §§ 249 ff. BGB ersatzfähig.[23]

Fraglich ist hingegen, ob ein Schadensersatzanspruch auch dann bestehen kann, wenn durch den Einsatz der Spionagesoftware allein das **Allgemeine Persönlichkeitsrecht** der betroffenen Person verletzt wurde, ohne dass ein Vermögensschaden entstanden ist. Dann läge ein sogenannter **Nicht-Vermögensschaden** (immaterieller Schaden) vor, der grundsätzlich allein in gesetzlich vorgeschriebenen Fällen ersatzfähig ist (§ 253 Abs. 1 BGB). In § 253 Abs. 2 BGB werden diejenigen Rechtsgüter aufgezählt, deren Verletzung auch bei Nicht-Vermögensschäden eine Geldentschädigung zur Folge haben können. Da das Allgemeine Persönlichkeitsrecht dort nicht aufgeführt ist und die Auflistung der Rechtsgüter abschließend ist, liegt nach dem Gesetzeswortlaut kein ersatzfähiger Schaden vor.[24]

Gleichwohl kann nach höchstrichterlicher Rechtsprechung eine **erhebliche Persönlichkeitsrechtsverletzung** die Verpflichtung zu einer Geldentschädigung begründen. Als Anspruchsgrundlage wird dabei der grundrechtliche Schutzauftrag des Allgemeinen Persönlichkeitsrechts aus den Art. 1, Art. 2 Abs. 1 GG herangezogen.[25] So soll auch zivilrechtlich ein hinreichender Schutz des Persönlichkeitsrechts gewährleistet werden.[26] Hat der Einsatz der Spionagesoftware im Einzelfall eine erhebliche Verletzung des Persönlichkeitsrechts verursacht, kann dem Betroffenen demnach ein Anspruch auf eine Geldentschädigung auch dann zustehen, wenn ein bloßer Nicht-Vermögensschaden vorliegt.

---

23 Oetker, in: Münchener Kommentar zum BGB, 9. Auflage 2022, Kommentierung zu § 249 BGB, Rn. 24.

24 Oetker, in: Münchener Kommentar zum BGB, 9. Auflage 2022, Kommentierung zu § 253 BGB, Rn. 27.

25 Bundesgerichtshof (BGH), Urteil vom 15.11.1994, Az.: VI ZR 56/94, Neue Juristische Wochenschrift (NJW) 1995, 861 (864, 865); so ausdrücklich auch die Begründung zum Gesetzentwurf der Bundesregierung zur Änderung schadensersatzrechtlicher Vorschriften, BT-Drs. 14/7752, 07.12.2001, Seiten 24, 25, abrufbar unter: https://dserver.bundestag.de/btd/14/077/1407752.pdf.

26 Bundesgerichtshof (BGH), Urteil vom 15.11.1994, Az.: VI ZR 56/94, Neue Juristische Wochenschrift (NJW) 1995, 861 (864, 865).

Schließlich kommt ein Schadensersatzanspruch aus Art. 82 Datenschutz-Grundverordnung (DSGVO)[27] in Betracht, wenn den dortigen Vorgaben zuwider personenbezogene Daten erhoben wurden. Dieser Anspruch umfasst seinem Wortlaut nach materielle und immaterielle Schäden.

3. Rechtliche Regelungen zu sogenannten Zero-Day-Schwachstellen

Sogenannte **Zero-Day-Schwachstellen** sind Software- oder Sicherheitslücken in einem IT-System, die dem Hersteller oder Entwickler unbekannt sind und von Hackern ausgenutzt werden können. Der Ausdruck „Zero-Day" bezieht sich auf die Tatsache, dass der Hersteller oder Entwickler erst nach dem ersten Angriff von Sicherheitslücken erfährt und damit „Null Tage" Zeit hat, ihn zu beheben. Sicherheitslücken können von jedem ausgenutzt werden, was sie für organisierte Kriminalität und Hacker, aber auch Staaten, etwa im Rahmen nachrichtendienstlicher Tätigkeiten, interessant machen kann. Informationen zu solchen Sicherheitslücken werden daher zu hohen Preisen auf Schwarzmärkten verkauft.[28]

Der Verkauf oder die Vermarktung von Zero-Day-Schwachstellen ist in Deutschland nicht ausdrücklich geregelt.

In **strafrechtlicher Hinsicht** kann der Verkauf oder die Vermarktung von Zero-Day-Schwachstellen als **Vorbereiten des Ausspähens und Abfangens von Daten** von § 202c StGB erfasst sein. § 202c StGB lautet seinem Wortlaut nach:

> § 202c Vorbereiten des Ausspähens und Abfangens von Daten
>
> (1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
>
> 1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
>
> 2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,
>
> herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
>
> (2) § 149 Abs. 2 und 3 gilt entsprechend.

Wenn im Einzelfall durch den Verkauf oder die Vermarktung keine Strafbarkeit nach § 202c StGB vorliegt, kann eine Strafbarkeit wegen der **Beihilfe** (§ 27 StGB) zu Straftaten einer dritten Person

---

27 Datenschutz-Grundverordnung (DSGVO) – Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016, abrufbar unter: https://dsgvo-gesetz.de/.

28 Bundesamt für Sicherheit in der Informationstechnik, Zero-Day-Exploits, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/Z/Zero-Day-Exploits.html.

vorliegen, wenn sich der Haupttäter beispielsweise nach den §§ 202a, 202b StGB strafbar gemacht hat.

Schließlich könnte eine Strafbarkeit wegen des **Betreibens krimineller Handelsplattformen im Internet** gemäß § 127 Abs. 1 StGB vorliegen, wenn der Täter eine Plattform im Internet betreibt, deren Zweck auf die Ermöglichung oder Begehung rechtswidriger Taten gerichtet ist. Nach dem Gesetzeswortlaut sind die §§ 202a ff. StGB und die §§ 303a ff. StGB als rechtswidrige Taten im Sinne des § 127 StGB erfasst. § 127 Abs. 1 StGB lautet seinem Wortlaut nach:

> § 127 Betreiben krimineller Handelsplattformen im Internet
>
> (1) Wer eine Handelsplattform im Internet betreibt, deren Zweck darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten zu ermöglichen oder zu fördern, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Rechtswidrige Taten im Sinne des Satzes 1 sind
>
> 1.Verbrechen,
>
> 2.Vergehen nach
>
> a) den §§ 86, 86a, 91, 130, 147 und 148 Absatz 1 Nummer 3, den §§ 149, 152a und 176a Absatz 2, § 176b Absatz 2, § 180 Absatz 2, § 184b Absatz 1 Satz 2, § 184c Absatz 1, § 184l Absatz 1 und 3, den §§ 202a, 202b, 202c, 202d, 232 und 232a Absatz 1, 2, 5 und 6, nach § 232b Absatz 1, 2 und 4 in Verbindung mit § 232a Absatz 5, nach den §§ 233, 233a, 236, 259 und 260, nach § 261 Absatz 1 und 2 unter den in § 261 Absatz 5 Satz 2 genannten Voraussetzungen sowie nach den §§ 263, 263a, 267, 269, 275, 276, 303a und 303b, (…).

4. Förderung von Forschung zur IT-Sicherheit

Die Bundesregierung stärkt seit Juni 2021 mit dem Rahmenprogramm „Digital. Sicher. Souverän.“ die **Forschung für IT-Sicherheit**. Für die Umsetzung werden dafür bis 2026 mindestens 350 Millionen Euro bereitgestellt. Das Programm baut auf dem Vorläuferprogramm der IT-Sicherheitsforschung „Selbstbestimmt und sicher in der digitalen Welt 2015-2020“ auf und berücksichtigt die Digitalisierung in ihrer Gesamtheit und deren Auswirkung auf den gesellschaftlichen Wandel. Im Rahmen des vorliegenden Programms werden spezifische Fördermaßnahmen für Klein- und Mittelständische Unternehmen (KMU) sowie Start-ups weiterentwickelt und im Austausch mit verschiedenen Akteuren neue Formate gestaltet. Besonders wichtig sind dabei Vernetzungsformate, um den Transfer zwischen Start-ups untereinander sowie zu potenziellen Kunden und Investoren zu stärken und zu beschleunigen. Auf diese Weise sollen innovative Produkte schneller marktreif werden. Detailliertere Informationen finden sich im Internet unter:

> https://www.bmbf.de/SharedDocs/Publikationen/de/bmbf/5/31672_Digital_Sicher_Souveraen.html#:~:text=Die%20Bundesregierung%20st%C3%A4rkt%20mit%20dem,Souver%C3%A4nit%C3%A4t%20in%20Deutschland%20und%20Europa.

Eine ausführliche Darstellung des Programms findet sich in einer Broschüre des Bundesministeriums für Bildung und Forschung unter:

> https://www.bmbf.de/SharedDocs/Publikationen/de/bmbf/5/31672_Digital_Sicher_Souveraen.pdf?__blob=publicationFile&v=4.

In der Förderdatenbank des Bundes sind derzeit 179 Beiträge zum Stichwort IT-Sicherheit abrufbar. Davon entfallen 52 auf Bundesförderung, 26 auf EU-Förderung und 100 auf Landesförderung, wobei Mischförderungen möglich sind. 17 Vorhaben richten sich an Existenzgründer, 16 an Privatpersonen und 128 an Unternehmen. Die Programme sind im Internet abrufbar unter:

> https://www.foerderdatenbank.de/SiteGlobals/FDB/Forms/Suche/Expertensuche_Formular.html?submit=Suchen&filterCategories=FundingProgram&filterCategories=FundingOrganisation&templateQueryString=IT-Sicherheit.

In welchem Ausmaß spezifisch der Aspekt von „Spyware“ in den einzelnen geförderten Projekten zum Tragen kommt, ist nicht verschlagwortet und konnte in diesem Zusammenhang nicht ermittelt werden.

***