Einstrahlung aufgrund von Fehlern bei der (Eigen-) Installation oder defekten Bauteilen infolge von Alterungs- und Abnutzungsprozessen, müssten insoweit außer Betracht bleiben, weil die Marktaufsicht diese Störungsursachen weder verhindern kann noch soll. Wie die beiden dem Senat vorliegenden – jeweils zehn Fälle umfassenden – Stichproben von im November 2004 durch die Beklagte bearbeiteten Störungen des Ton-Rundfunks auf UKW sowie des Fernseh-Rundfunks zeigen, ist der Anteil der vorgenannten anderen Störungsursachen bei diesen beiden Nutzergruppen auch nicht unerheblich. Er macht vielmehr weit mehr als die Hälfte der 20 vorgelegten Störungsfälle aus. Dieses Stichprobenergebnis ist vor dem Hintergrund der insoweit in der Tendenz übereinstimmenden, erfahrungsbasierten Erläuterungen der Beteiligten ohne weiteres plausibel. Es ist vor allem durch die jedenfalls in den streitbefangenen Jahren noch anzutreffende „soziale Praxis" der Störungsmeldung und die gerade in Privathaushalten eher zu erwartenden Installationsmängel leicht zu erklären. Eine solche gravierende Abweichung zwischen Umfang der Störungsbearbeitung und Störungsursachen, denen die Marktaufsicht entgegen wirken kann, führte in den betreffenden Jahren offenbar zu einer überproportionalen Belastung des terrestrischen Rundfunks. Dies stellt die beiden im vorliegenden Verfahren streitbefangenen Beitragssätze in Frage.

Darüber hinaus müssten in die Ermittlung der Störempfindlichkeit als Verteilungsmaßstab für die Verteilung der (nicht bereits durch Gebühren gedeckten) Marktaufsichtskosten auch die Störungsbearbeitungskosten einbezogen werden, die schuldhaft durch der Marktaufsicht nach dem EMVG unterliegende, den Anforderungen nach dem EMVG bei Markteintritt aber nicht genügende Geräte verursacht worden sind. Denn die Marktaufsicht soll gerade auch vor derartigen Störungen schützen, denen ein Verschulden der Inverkehrbringer oder Anbieter der Geräte zugrunde liegt.

Diese Anforderungen, die aus Sicht des Senats aus Art. 3 Abs. 1 GG und dem Erfordernis der Vorteilsgerechtigkeit in Bezug auf den Zweck der hier maßgeblichen Verordnungsermächtigung folgen, lassen sich auch ohne übermäßigen Verwaltungsaufwand umsetzen. Hinsichtlich der Einbeziehung schuldhafter Verstöße gegen das EMVG folgt dies schon daraus, dass die erforderlichen Daten der Beklagten vorliegen und bereits in die vorgelegte Alternativberechnung einbezogen werden konnten. Die Ermittlung des Anteils der Störungen, die im oben verstandenen Sinne als Maßstab für die Quantifizierung der Störempfindlichkeit berücksichtigungsfähig sind, an den bearbeiteten Störungen erfordert keine vollständige (Nach-) Erhebung sämtlicher in diesem Zusammenhang relevanter Daten. Nach dem derzeitigen Erkenntnisstand spricht alles dafür, dass die Störempfindlichkeit einer Nutzergruppe dergestalt ermittelt werden kann, dass nicht sämtliche Störungsvorgänge ausgewertet werden müssen, sondern nur eine repräsentative Stichprobe untersucht wird. Auf der Basis einer solchen Stichprobe könnte dann der Kostenanteil für die Bearbeitung von Störungen der jeweiligen Nutzergruppe, die durch der Marktaufsicht nach dem EMVG unterliegende, den Anforderungen nach dem EMVG bei Markteintritt aber nicht genügende Geräte verursacht worden sind, hinreichend verlässlich ermittelt und für die Zukunft jedenfalls solange zugrunde gelegt werden, bis aufgrund geänderter Umstände Anlass zu der Annahme besteht, dass sich im Verhältnis der Nutzergruppen Änderungen ergeben haben könnten. (...)

Eingesandt vom OVG Nordrhein-Westfalen

Report und Technik

Aufsätze

Thomas Hoeren / Stefan Pinelli

Die Überprüfung von Software auf sicherheitsrelevante Fehler

Eine erste Analyse nach Urheberrecht, Geschäftsgeheimnisgesetz und Patentrecht

Ausgehend vom Interesse des Nutzers an der Sicherheit erworbener Software und an deren Überprüfung (I.) untersucht der Beitrag, ob und inwieweit eine sorgfältige Analyse von Software auf sicherheitsrelevante Mängel nach Urheberrecht (II.), nach dem Recht für Geschäftsgeheimnisse (III.) und nach dem Patentrecht (IV.) zulässig ist.

I. Ausgangslage

Regelmäßig ist es im Interesse von Nutzern komplexer soft- 1
waregestützter Produkte, die in ihrer Branche zum Einsatz kommende Software zu unterschiedlichen Zwecken zu testen. Vor dem Hintergrund hochkomplexer Softwareentwicklungen, die unterschiedlichste Software miteinander kombinieren, mitunter Echtzeitdaten verarbeiten und den Nutzer von software-

gestützten Produkten bei deren Handhabung teilweise oder vollumfänglich anleiten (können), spielt insbesondere die Gewährung von Produktqualität in Gestalt von Sicherheit eine gewichtige Rolle. Gerade in den aktuellen Diskussionen um Cybersecurity-, sonstige IT-Sicherheits- und Datenschutz-Vorfälle zeigt sich, wie wichtig es ist dafür zu sorgen, dass frühzeitig Erkenntnisse über die Eigenschaften und Funktionen von Software mit Blick auf IT-Sicherheit vorliegen und zweckentsprechend genutzt werden können. Die nachstehenden Ausführungen gehen auf die urheber-, patentrechtlichen und geschäftsgeheimnisrelevanten Rahmenbedingungen von Softwareuntersuchungen ein, die nicht Open Source Software zum Gegenstand haben. Die Bewertung von Softwareuntersuchungen in strafrechtlicher Hinsicht ist ebenfalls nicht Gegenstand dieses Beitrages, wobei gleichwohl darauf hinzuweisen ist, dass strafrechtliche Implikationen im Einzelfall durchaus zu beachten sind.

2 Ziel von Softwareuntersuchungen kann es somit sein zu ermitteln, inwieweit die gelieferte Software gesetzliche Anforderungen erfüllt, den vereinbarten Vorgaben (Eigenschaften und Funktionen) des Käufers bzw. Bestellers entspricht und (unverbindliche) Leitlinien von Behörden und anderen Institutionen befolgt. Im Rahmen der Untersuchungen kann eine ganze Bandbreite an Maßnahmen in Betracht kommen:

3 Bei der *Überwachung und Systemüberwachung* soll die Kommunikation von Software zu Software beziehungsweise von Software zu Hardware zwecks Prüfung „abgefangen" werden.[1] Weiterhin wird der Programmablauf bei Eingabe verschiedener Befehle untersucht, ohne dass dabei aber ein Zugriff auf interne Softwarestrukturen erfolgt (sog. *Black Box Testing*[2]). Im Zuge der Untersuchungen werden durchaus *Debugger*[3], Line-Tracing-Tools, Speicherabzüge und *ähnliche Analysetools* eingesetzt sowie *Last- und Stresstests* durchgeführt. Durch *Penetration Testing*, also das beauftragte professionelle „auf den Prüfstand stellen" der Sicherheit von IT-Systemen sollen etwaige Sicherheitsschwachstellen erkannt werden. Zu den Untersuchungsmaßnahmen können weiterhin die *Manipulation und Erweiterung des Quellcodes* zählen, etwa in Form eines dekompilierten Codes und Binärcodes. Darüber hinaus können einzelne Softwarekomponenten untersucht werden oder die Software durch *Dekompilierung* analysiert werden. Teilweise kann für die technische Prüfung auch eine *Umgehung technischer Schutzmaßnahmen* erforderlich sein.

4 Beschränkungen oder Verbote solcher Inspektionsmaßnahmen könnten sich insbesondere aus den Vorschriften zum Schutz von Computerprogrammen ergeben (§§ 69a ff. UrhG). Darüber hinaus könnten das Patentrecht (PatG) und das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), welches die EU-Richtlinie 2016/943 umsetzt, weitere Einschränkungen enthalten. Das Verhältnis der Schutzsysteme im Einzelnen muss außerdem erörtert werden.

II. Schutz von Computerprogrammen nach §§ 69a ff. UrhG

5 Zwecks Umsetzung der EU-Richtlinie 2009/24/EG zum Schutz von Computerprogrammen sind in den §§ 69a ff. UrhG spezielle Regelungen für Computerprogramme vorgesehen.

1. Umfang

§§ 69a ff. UrhG schützen Programme in jeder Gestalt, einschließlich des Entwurfsmaterials, § 69a Abs. 1 UrhG. Während die einem Element eines Computerprogramms zugrunde liegenden Ideen und Grundsätze generell nicht geschützt werden (vgl. § 69a Abs. 2 S. 2 UrhG), werden Computerprogramme überhaupt nur unter der Voraussetzung geschützt, dass sie das Ergebnis einer geistigen Schöpfung des Urhebers sind, § 69a Abs. 3 UrhG.[4] 6

Im Regelfall erfüllen Computerprogramme, und daher wohl auch die in der Praxis zu untersuchenden Programme, die Schutzvoraussetzungen und der Anwendungsbereich der §§ 69a ff. UrhG ist eröffnet.[5] 7

2. Zustimmungspflichtige Maßnahmen

§ 69c UrhG nennt die ausschließlichen Rechte des Rechtsinhabers. Relevant sind hier insbesondere das Recht zur Vervielfältigung des Computerprogramms (§ 69c Nr. 1 UrhG) sowie das Recht zur Nachbearbeitung (§ 69c Nr. 2 UrhG). 8

a) Reproduktion des Programms

Gemäß § 69c Nr. 1 UrhG hat der Rechtsinhaber das ausschließliche Recht zur dauerhaften oder vorübergehenden Vervielfältigung eines Computerprogramms, unabhängig von Mittel und Form oder etwa nur teilweiser Reproduktion. „*Vervielfältigung*" meint dabei jede Handlung, die Programmdaten für den Menschen sichtbar macht, sei es durch Kopieren auf einen anderen Datenträger, Ausdrucken oder Speichern des Quell- oder Programmcodes.[6] Ist im Zusammenhang mit der Ausführung des Computerprogramms, etwa beim Laden, Anzeigen, Ablaufen, Übertragen oder Speichern, eine Vervielfältigung erforderlich, bedarf auch diese der Zustimmung des Rechtsinhabers, § 69c Nr. 1 S. 2 UrhG. Wird durch das Laden eines Programms in den Arbeitsspeicher eine zusätzliche Nutzung durch weitere Kopien des Programms ermöglicht, liegt bereits darin eine Vervielfältigung.[7] 9

Im Rahmen der oben beschriebenen Untersuchungen erfolgen u.a. Vervielfältigungen des Computerprogramms, wobei im Falle von sog. Embedded Software-Lösungen nicht immer zwingend eine Vervielfältigung erfolgen muss. Eine Beschränkung der Untersuchungen auf die Einhaltung des Programmablaufs ist unerheblich, da auch im Zusammenhang mit der 10

1 *Triebe*, WRP 2018, 795 (796).
2 Ausführlich zu den unterschiedlichen Blackbox-Verfahren: *Schmidt* in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 1 Rz. 300 ff.
3 *Schmidt* in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 1 Rz. 72.
4 Für Schutzanforderungen im Zusammenhang mit Verschlüsselungsalgorithmen s. *Triebe*, WRP 2018, 795 (796).
5 *Czychowski* in Fromm/Nordemann, Urheberrecht, 12. Aufl. 2018, § 69a Rz. 18; *Raubenheimer*, CR 1996, 69 (69).
6 *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69c Rz. 4; *Redeker*, IT-Recht, 6. Aufl. 2017, Rz. 45.
7 BGH, Urt. v. 3.2.2011 – I ZR 129/08, CR 2011, 223 m. Anm. *Rössel* = WRP 2011, 480 (482) – UsedSoft.

Ausführung erstellte Vervielfältigungen zustimmungsbedürftig sind, § 69c Nr. 1 S. 2 UrhG.

11 Zumindest im Falle von Maßnahmen wie Überwachung, Systemüberwachung, Blackbox-Tests sowie Last- und Stresstests sind in der Regel Reproduktionen erforderlich. Auch durch den Einsatz anderer Analyse-Tools entstehen regelmäßig Duplikate. Im Rahmen einer Analyse eines einzelnen Programmteils erscheint es insofern sinnvoll, dieses zuvor zu extrahieren und zu duplizieren.

b) Änderung des Programms

12 Gemäß § 69c Nr. 2 UrhG hat der Rechtsinhaber weiterhin das ausschließliche Recht zur Übersetzung, zur Bearbeitung, zum Arrangement und zu anderen Umarbeitungen eines Computerprogramms sowie zur Vervielfältigung der Ergebnisse. Dabei ist schon die Nachbearbeitung selbst zustimmungsbedürftig, nicht erst die Veröffentlichung des Ergebnisses.[8] Zweck dieser Regelung ist der Schutz des Know-hows des Rechtsinhabers.[9] Umarbeitung ist weit zu verstehen, nämlich als alle Änderungen am Programm.[10] Dafür ist ein Eingriff in den Programmstoff erforderlich.[11] Beispielhaft nennt § 69c Nr. 2 UrhG Formen der Umarbeitung. Übersetzung bezieht sich dabei auf die Übertragung des Programms in eine andere Programmiersprache.[12]

13 In die Kategorie der Übersetzung fällt etwa die Rückübersetzung von Objektcode in Quellcode.[13] Auch bei Manipulation, Veränderung und Erweiterung des Quellcodes[14] und Penetrationstests wird in die Programmsubstanz eingegriffen, so dass ein Fall der Umarbeitung vorliegt.

14 Bei Überwachungen, Systemüberwachungen, Blackbox-Tests sowie Last- und Stresstests, Speicherabzügen und Leitungsabtastung hingegen erfolgt grundsätzlich kein Eingriff in den Programmstoff, so dass auch keine Umarbeitung i.S.d. § 69c Nr. 2 UrhG vorliegt. Der Einsatz von Debuggern bedarf – in Abhängigkeit von der jeweiligen Debugging-Methode – einer Analyse des Einzelfalls.

3. Zustimmung des Urheberrechtsinhabers

15 Um die aufgeführten Prüfungshandlungen vorzunehmen, ist daher die Zustimmung des jeweiligen Rechtsinhabers erforderlich. In Ermangelung einer ausdrücklichen Zustimmung genügt hinsichtlich des Schutzes von Computerprogrammen schon eine *konkludente Einwilligung* (bzw. Einräumung von Nutzungsrechten) den Anforderungen. Für die Annahme einer konkludenten Rechteeinräumung sind aber stets alle Umstände des Einzelfalls maßgeblich. Vor allem muss der Vertragszweck zweifelsfrei festzustellen sein und es ist auf die vorangegangene Vertragspraxis sowie die Branchenüblichkeit abzustellen.[15]

16 Ob im Einzelfall eine konkludente Einwilligung vorliegt, muss sorgfältig festgestellt werden. Zwar sind Untersuchungsmaßnahmen durchaus branchenüblich, allerdings erheben Verträge zwischen Softwarelieferant und Softwareabnehmer aufgrund ihrer umfangreichen Regelungen im Hinblick auf ihre Nutzungsrechte einen Anspruch auf Vollständigkeit, was zusätzlichen konkludenten Einwilligungen grundsätzlich entgegenstehen könnte ~~dürfte~~. Die Annahme einer konkludenten Einräumung von Nutzungsrechten, die über das ausdrücklich Vereinbarte hinausgeht, widerspricht im Zweifel der Absicht der Parteien. Das ergibt sich schon aus dem Zweckübertragungsgrundsatz, der auch auf Computerprogramme anzuwenden ist, §§ 69a Abs. 4, 31 Abs. 5 UrhG.[16] Danach werden im Zweifel keine Rechte eingeräumt, die über den Vertragszweck hinausgehen.[17]

17 Diese Auffangregel für die Auslegung ändert sich auch nicht durch die Tatsache, dass ein Großteil der Vereinbarungen zu Nutzungsrechten regelmäßig durch AGB geregelt wird. Zwar ist äußerst umstritten, ob es sich beim Zweckübertragungsgrundsatz um eine *bloße Auslegungsregel* handelt oder um eine *Inhaltsnorm* mit dem darüber hinausgehenden Regelungsgehalt, dass vertragliche Abweichungen vom gesetzlichen Umfang und Inhalt der Nutzungsrechte nur unter besonderen Voraussetzungen zulässig sind.[18] Dies wirkt sich jedoch nur insofern aus, als Vereinbarungen bestehen, die über den Vertragszweck hinausgehen, oder eine Inhaltskontrolle bei AGB vorgenommen werden soll.[19] Da über die Funktion des Zweckübertragungsgrundsatzes (zumindest) als Auslegungsregel Einigkeit besteht, bleibt bei einer hinreichend ausdifferenzierten Vertragsgestaltung üblicherweise wenig Raum für eine konkludente Einwilligung für ungeregelte Nutzungsarten, weil im Zweifel die Rechte beim Urheber verbleiben sollen.[20] Eine konkludente Einwilligung des Rechtsinhabers liegt daher in der Regel nicht vor.

4. Bestimmungsgemäßer Gebrauch gem. § 69d Abs. 1 UrhG

18 Sofern die Inspektionsmaßnahmen einer besonderen Ausnahme nach §§ 69d, 69e UrhG unterfallen, könnten sie dennoch rechtmäßig sein.

19 Gemäß § 69d Abs. 1 UrhG sind die in § 69c Nr. 1, 2 UrhG genannten Handlungen nicht zustimmungsbedürftig, soweit keine (wirksame) besondere vertragliche Regelung[21] erfolgt ist

---

8 *Dreier* in Dreier/Schulze, Urheberrechtsgesetz, 6. Aufl. 2018, § 69c Rz. 14; *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69c Rz. 17.

9 *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69c Rz. 17.

10 *Dreier* in Dreier/Schulze, UrhG, 6. Aufl. 2018, § 69c Rz. 15; *Redeker*, IT-Recht, 6. Aufl. 2017, Rz. 61.

11 LG Hamburg, Urt. v. 3.5.2016 – 408 O 46/16, CR 2016, 782 (783); *Dreier* in Dreier/Schulze, UrhG, 6. Aufl. 2018, § 69c Rz. 16.

12 *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69c Rz. 18.

13 *Dreier* in Dreier/Schulze, Urheberrechtsgesetz, 6. Aufl. 2018, § 69c Rz. 16; *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69c Rz. 18.

14 Ergänzung des Quellcodes als klassische Form der Bearbeitung, *Czychowski* in Fromm/Nordemann, Urheberrecht, 12. Aufl. 2018, § 69c Rz. 21.

15 OLG Frankfurt, Urt. v. 29.10.2013 – 11 U 47/13, CR 2014, 506 = MMR 2014, 661 (662).

16 *Dreier* in Dreier/Schulze, Urheberrechtsgesetz, 6. Aufl. 2018, § 69a Rz. 34.

17 *Wiebe* in Spindler/Schuster, Elektronisches Mediengesetz, 3. Aufl. 2015, § 31 UrhG Rz. 12.

18 Zum Ganzen *Schulze* in Dreier/Schulze, Urheberrechtsgesetz, 6. Aufl. 2018, § 31 Rz. 114 ff. m.w.N.; *Wiebe* in Spindler/Schuster, Elektronisches Mediengesetz, 3. Aufl. 2015, § 31 UrhG Rz. 12.

19 *Schulze* in Dreier/Schulze, Urheberrechtsgesetz, 6. Aufl. 2018, § 31 Rz. 114.

20 *Schulze* in Dreier/Schulze, Urheberrechtsgesetz, 6. Aufl. 2018, § 31 Rz. 114.

21 Für die Grenzen solcher Vereinbarungen s. *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69d Rz. 33 ff.

und wenn sie für eine bestimmungsgemäße Benutzung des Computerprogramms, einschließlich der Fehlerberichtigung, durch jeden zur Verwendung einer Kopie des Programms Berechtigten, notwendig sind. Normzweck ist die Herstellung eines angemessenen Gleichgewichts zwischen den Interessen des legitimen Nutzers und denen des Rechtsinhabers,[22] wobei das Nutzungsinteresse des berechtigten Nutzers die Interessen des Rechtsinhabers insoweit überwiegt.[23]

a) Legitimität

20 Berechtigt in diesem Sinne ist jede Person, der vom Rechtsinhaber ein entsprechendes Nutzungsrecht eingeräumt wurde. Das erfasst jeden, der einen wirksamen Lizenzvertrag abgeschlossen hat, nicht nur Käufer.[24] Die Berechtigung ergibt sich im Regelfall durch den rechtmäßigen Erwerb bzw. Bezug der Software (Kaufvertrag oder Werkvertrag) oder auch die Berechtigung, die Software im Testbetrieb zu nutzen.

b) Bestimmungsgemäßer Gebrauch

21 Die Herausforderung bei der Barrierebestimmung ist das konstitutive Element der bestimmungsgemäßen Benutzung. Zur Ermittlung einer bestimmungsgemäßen Benutzung stellt die vorherrschende Meinung in Rechtsprechung und Literatur auf den Übertragungszweck und weitere vertragliche Umstände ab.[25] Ergänzend müssen die entgegenstehenden Interessen der Parteien umfassend abgewogen werden.

22 *Aktive Softwareanalyse:* Der Vertrag, aus dem sich die Berechtigung zur Verwendung der Software ergibt, wird entweder ein Softwarekaufvertrag (nur für Standardsoftware) oder ein Softwareentwicklungsvertrag sein,[26] welcher grundsätzlich als Werkvertrag zu kategorisieren ist[27]. Bei zeitlich befristet überlassener Software dürfte regelmäßig ein Mietvertrag vorliegen. Die Prüfung der Software verfolgt zumeist den Zweck einer Mängeluntersuchung. Wenn die Software gesetzliche Anforderungen nicht erfüllt oder den spezifischen (rechtmäßigen) Vorgaben des Käufers nicht entspricht, liegt – je nach Vertragsart – ein Mangel im Sinne von etwa § 633 BGB oder § 434 BGB vor.[28] Vor diesem Hintergrund stellt sich die Frage, ob auch die aktive Prüfung auf Softwarefehler eine bestimmungsgemäße Benutzung i.S.d. § 69d Abs. 1 UrhG darstellt. Bisher schweigt die Literatur augenscheinlich zu dieser Frage.

23 *Erst-Recht-Schluss zum „Ob":* Nach Ansicht der Verfasser können solche Maßnahmen, die für die Fehlersuche erforderlich sind, im Einzelfall eine bestimmungsgemäße Benutzung darstellen. § 69d Abs. 1 UrhG räumt dem Berechtigten ausdrücklich das Recht zur Fehlerberichtigung ein. Im Rahmen der Fehlerberichtigung erfolgt stets ein signifikanter Eingriff in die Programmsubstanz.[29] Die ausschließliche Fehlersuche, die erheblich eingriffsschwächer als die Berichtigung ist, muss daher *erst recht* zulässig sein. Im Falle eines Mangels stehen dem Softwarenutzer als Käufer bzw. Besteller Gewährleistungsrechte nach § 437 BGB oder § 634 BGB zu; ein Recht zur Untersuchung auf Mängel lässt sich daher aus den zugrunde liegenden Verträgen begründen. Nach § 377 HGB, der auch für den Kauf von Software gilt[30], ist der gewerbliche Käufer sogar zur unverzüglichen Untersuchung der Kaufsache verpflichtet. Im Falle eines Werkvertrags führt eine Abnahme trotz Kenntnis eines Mangels zu einer Beschränkung der Gewährleistungsrechte gem. § 640 Abs. 3 BGB. Auch in diesem Fall besteht also eine gewisse Verpflichtung zur Untersuchung auf Mängel. Es ist dem Käufer auch nicht zumutbar, warten zu müssen, bis ein Mangel entdeckt wird; insbesondere wäre er dadurch der Gefahr der Verjährung seiner Ansprüche ausgesetzt. Daher begründet bereits der Werk- oder Kaufvertrag über die Software das Recht zur aktiven Prüfung auf Mangelfreiheit. Diese Argumentation lässt sich im Grundsatz entsprechend auf den Mietvertrag übertragen, da aus der Sicht des Nutzers ebenfalls ein Bedürfnis besteht, die Software als Mietsache auf Mängel zu untersuchen.

Interessenabwägung zum „Wie": Welche Untersuchungsmaß- 24
nahmen konkret zulässig sind, ist in einem darüber hinausgehenden Interessenausgleich zwischen den Vertragsparteien festzustellen. Im Rahmen dieser Interessenabwägung sind zugunsten des Käufers etwa mögliche Haftungsrisiken oder Reputationsschäden zu berücksichtigen. Bei speziellerer Verwendung der Software sind je nach Verwendung individuelle Erwägungen anzustellen. So ist zu berücksichtigen, dass etwa der Einsatz von Software in sensiblen teil- oder vollautomatisierten Bereichen erfolgt und dass darüber hinaus durch Softwaremängel unter Umständen Rechtsgüter wie Leib und Leben gefährdet werden könnten. Den Interessen der Softwareerwerber steht das Interesse des Softwarelieferanten am Schutz seines Know-hows gegenüber. Je nach Interessenlage im Einzelfall kann der Schutz des Lieferanten oder des Käufers, Bestellers oder Mieters überwiegen.

Vor diesem Hintergrund muss gelten, dass alle Prüfungsmaß- 25
nahmen, die zur Erkennung sicherheitsrelevanter Softwarefehler dienen, bestimmungsgemäße Benutzungen i.S.d. § 69d Abs. 1 UrhG sind. Eine Dekompilierung kann allerdings in keinem Fall eine bestimmungsgemäße Benutzung sein, da die Sondervorschrift des § 69e UrhG nicht umgangen werden darf.[31]

---

22 Vgl. *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69d Rz. 1, 3.

23 *Dreier* in Dreier/Schulze, Urheberrechtsgesetz, 6. Aufl. 2018, § 69d Rz. 5.

24 *Witte/Auer-Reinsdorff* in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 5 Rz. 211; *Dreier* in Dreier/Schulze, Urheberrechtsgesetz, 6. Aufl. 2018, § 69d Rz. 6.

25 OLG Düsseldorf, Urt. v. 29.5.2001 – 20 U 166/00, CR 2002, 95 (96 f.); *Wiebe* in Spindler/Schuster, Elektronisches Mediengesetz, 3. Aufl. 2015, § 69d UrhG Rz. 11; *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69d Rz. 7.

26 OLG Frankfurt, Urt. v. 17.8.2017 – 5 U 152/16, CR 2017, 639 = CR 2017, 646 = MMR 2018, 100 (101).

27 *Czychowski* in Fromm/Nordemann, Urheberrecht, 12. Aufl. 2018, § 69c Rz. 39.

28 Vgl. OLG Köln, Hinweisbeschluss v. 20.12.2017 – 18 U 112/17, NJW-RR 2018, 373.

29 Zur Fehlerberichtigung ist wenigstens eine Bearbeitung des Programms nötig, *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69d Rz. 17.

30 BGH, Urt. v. 12.12.1999 – VIII ZR 299/98, NJW 2000, 1415 (1415).

31 *Dreier* in Dreier/Schulze, UrhG, 6. Aufl. 2018, § 69d Rz. 10.

5. Beobachtung, Prüfung und Untersuchung nach § 69d Abs. 3 UrhG

26 Gemäß § 69d Abs. 3 UrhG kann der Berechtigte ohne Zustimmung des Rechtsinhabers das Funktionieren des Programms beobachten, untersuchen oder testen, um die einem Programmelement zugrunde liegenden Ideen und Grundsätze zu ermitteln, wenn dies durch Handlungen zum Laden, Anzeigen, Ablaufen, Übertragen oder Speichern des Programms, d.h. im Rahmen der normalen Programmausführung, erfolgt. Diese Ausnahme beschränkt sich auf den Zweck der Ermittlung der Ideen und Prinzipien; weitergehende Reproduktionen und Anpassungen werden nicht erfasst.[32]

27 Inhaltliche Eingriffe in die Programmsubstanz werden von der Ausnahme nicht erfasst.[33] Die Identifizierung und Untersuchung des Quellcodes ist ebenso kein ohne Weiteres zulässiger Gegenstand der Untersuchung.[34]

28 § 69d Abs. 3 UrhG umfasst gängige Analysemaßnahmen wie Monitoring, Systemüberwachung, Blackbox-Tests[35], Last- und Stresstests, Speicherabzug[36] und Leitungsverfolgung.[37] Ob der Einsatz von Debuggern zulässig ist, hängt von der Art des jeweiligen Debuggers und den von ihm vorgenommenen Eingriffen in die Programmsubstanz ab.[38] Eine Dekompilierung hingegen ist nach § 69 Abs. 3 UrhG nicht zulässig.[39]

6. Zulässige Dekompilierung nach § 69e UrhG

29 § 69e UrhG regelt den speziellen Fall der Dekompilierung; diese ist zum Zweck der Herstellung von *Interoperabilität* mit anderen Programmen zustimmungsfrei erlaubt. Der Zweck ist erschöpfend geregelt; weitergehende Zwecke werden nicht erfasst.[40]

30 Sofern die Untersuchungen primär dazu dienen, die Einhaltung gesetzlicher Standards oder vertraglicher Vorgaben zu überprüfen, wird ein anderer Zweck verfolgt. Eine Dekompilierung in diesem Rahmen wird nicht von § 69e UrhG erfasst.

7. Umgehung technischer Schutzmaßnahmen

31 Die rechtliche Zulässigkeit von Untersuchungsmaßnahmen, die auf die Umgehung technischer Schutzmaßnahmen gerichtet ist, wird durch § 69f Abs. 1 und 2 UrhG bestimmt. § 95a UrhG gilt gem. § 69a Abs. 5 UrhG nicht für Computerprogramme.[41]

32 Gemäß § 69f Abs. 2 UrhG hat der Rechtsinhaber einen Anspruch darauf, dass alle Mittel, die allein dazu bestimmt sind, die unerlaubte Beseitigung oder Umgehung technischer Programmschutzmechanismen zu erleichtern, vernichtet werden. Daraus wird überwiegend der Schluss gezogen, dass im Gegensatz zu § 95a UrhG die Verwendung der Mittel nicht als solche erfasst werden sollte.[42]

33 In einigen Fällen wird jedoch vom *sog. indirekten Schutz der Schutzmaßnahmen* ausgegangen. Danach liegt ein Verstoß gegen § 69c UrhG vor, wenn die Nutzung der Mittel eine zustimmungspflichtige Handlung darstellt.[43] Dabei ist die Reproduktion und Umarbeitung des Programms von besonderer Bedeutung. Die Werknutzung kann aber wiederum durch §§ 69d, 69e UrhG gerechtfertigt sein.[44]

Unter technischen Programmschutzmechanismen werden z.B. 34
Dongles, Kopierschutzmechanismen, Passwortabfragen, Programmblöcke, Zeitblöcke, etc. verstanden.[45] § 69f Abs. 2 UrhG erfasst schon Maßnahmen, die die Umgehung nur erleichtern. Andererseits müssen sie zweckmäßig ausschließlich zur Umgehung bestimmt sein; Mittel die auch zur rechtmäßigen Verwendung gedacht sind, werden nicht erfasst.[46]

III. Schutz von Geschäftsgeheimnissen nach GeschGehG

Die Umsetzung der EU-Geschäftsgeheimnisrichtlinie[47] hat die 35
früher in den §§ 17 ff. UWG bestimmte Haftung zu einem weitaus differenzierteren Schutzsystem für Geschäftsgeheimnisse geführt. Der entsprechende Entwurf der *Bundesregierung* für ein Gesetz zum Schutz von Geschäftsgeheimnissen (nachfolgend GeschGehG genannt) wurde im *Bundestag* noch modifiziert und trat Ende April in Kraft.[48]

---

32 *Wiebe* in Spindler/Schuster, Elektronisches Mediengesetz, 3. Aufl. 2015, § 69d UrhG Rz. 28; *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69d Rz. 64.

33 *Czychowski* in Fromm/Nordemann, Urheberrecht, 12. Aufl. 2018, § 69d Rz. 28; *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69d Rz. 63.

34 *Ritzel*, WRP 2018, 795 (799).

35 *Czychowski* in Fromm/Nordemann, Urheberrecht, 12. Aufl. 2018, § 69d Rz. 29.

36 *Kaboth/Spies* in BeckOK, Urheberrecht, 23. Ed. 15.1.2019, § 69d Rz. 15.

37 *Wiebe* in Spindler/Schuster, Elektronisches Mediengesetz, 3. Aufl. 2015, § 69d UrhG Rz. 28 m.w.N.

38 So auch *Triebe*, WRP 2018, 795 (798); für die Zulässigkeit der Fehlersuche *Kaboth/Spies* in BeckOK, Urheberrecht, 23. Ed. 15.1.2019, § 69d Rz. 15; *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69d Rz. 63.

39 *Czychowski* in Fromm/Nordemann, Urheberrecht, 12. Aufl. 2018, § 69d Rz. 28; *Kaboth/Spies* in BeckOK, Urheberrecht, 23. Ed. 15.1.2019, § 69d Rz. 15; *Wiebe* in Spindler/Schuster, Elektronisches Mediengesetz, 3. Aufl. 2015, § 69d UrhG Rz. 28.

40 *Czychowski* in Fromm/Nordemann, Urheberrecht, 12. Aufl. 2018, § 69e Rz. 1, 8 f.; *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69e Rz. 7.

41 *Czychowski* in Fromm/Nordemann, Urheberrecht, 12. Aufl. 2018, § 69f Rz. 15.

42 Ähnlich *Grützmacher* in Wandtke/Bullinger, UrhR, 4. Aufl. 2014, § 69f Rz. 13.

43 Dazu *Kreutzer*, CR 2006, 804 (806).

44 *Kreutzer*, CR 2006, 804 (806 ff.).

45 *Kaboth/Spies* in BeckOK, Urheberrecht, 23. Ed. 15.1.2019, § 69f Rz. 9.

46 Vgl. LG München I, Urt. v. 13.3.2008 – 7 O 16829/07, MMR 2008, 839 (841); *Kaboth/Spies* in BeckOK, Urheberrecht, 23. Ed. 15.1.2019, § 69f Rz. 10; auf den Hauptzweck des Umgehungsmittels abstellend *Czychowski* in Fromm/Nordemann, Urheberrecht, 12. Aufl. 2018, § 69f Rz. 11.

47 Richtlinie (EU) 2016/943 zum Schutz vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor unrechtmäßigem Erwerb, unrechtmäßiger Verwendung und Weitergabe. Verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0943&from=DE, zuletzt abgerufen 1.3.2019.

48 BGBl. I 2019, 466 gültig ab 26.4.2019; Regierungsentwurf verfügbar unter https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_GeschGehG.pdf;jsessionid=38047E8EF10338EF53661CFC7627E69F.2_cid324?__blob=publicationFile&v=1, zuletzt abgerufen 1.6.2019.

1. Konzept des Geschäftsgeheimnisses

36 Gemäß § 2 Nr. 1 GeschGehG sind Geschäftsgeheimnisse Informationen, die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich und daher von wirtschaftlichem Wert sind. Darüber hinaus müssen die Informationen Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber sein. Die Maßnahmen sind vom Inhaber des Geschäftsgeheimnisses nachzuweisen.[49] Die Definition selbst ist Gegenstand vielfacher Rechtsstreitigkeiten, die im Rahmen dieses Beitrags nicht geklärt werden können.[50]

37 Jedoch kann man annehmen, dass im Einzelfall die zu inspizierende Software, der Quellcode selbst oder einzelne Teile Geschäftsgeheimnisse in diesem Sinne enthalten bzw. darstellen können. Die Informationen dürfen dabei nicht leicht zugänglich sein, was sich mit Hinblick auf die Personen bestimmt, die normalerweise mit solchen Informationen in Kontakt kommen *(Fachkreise)*. Solche Sachverhalte, die von einem Durchschnittsfachmann ermittelt werden können, fallen daher aus dem Anwendungsbereich des GeschGehG heraus.[51] Allerdings gilt, dass Reverse-Engineering-Maßnahmen Informationen nicht ohne weiteres zugänglich machen, denn anderenfalls würde § 3 Abs. 1 Nr. 2 GeschGehG seines Regelungsgehalts beraubt.

38 Im Folgenden wird auch wegen der aktuellen Schwierigkeiten einer rechtssicheren Handhabung der Definition, davon ausgegangen, dass im Rahmen der Untersuchung Geschäftsgeheimnisse offengelegt oder zumindest verwendet werden.

2. Schutzumfang

39 Gemäß § 4 GeschGehG darf ein Geschäftsgeheimnis nicht durch unbefugten Zugang zu, unbefugte Aneignung oder unbefugte Reproduktion von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen es abgeleitet werden kann, erlangt werden, § 4 Abs. 1 Nr. 1 GeschGehG. Liegt eine Zustimmung des Rechtsinhabers vor, ist die Erlangung nicht unbefugt.

40 Ein Geschäftsgeheimnis darf weiterhin nicht durch ein sonstiges Verhalten, das unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheiten entspricht, erlangt werden, § 4 Abs. 1 Nr. 2 GeschGehG. Dieser Tatbestand ist konturlos und kann ohne einen Rückgriff auf die rhetorische Praxis kaum erörtert werden.[52] Jedenfalls solche Handlungen, die bereits nach den §§ 69a ff. UrhG zulässig sind (s. II.4.–7. oben), gelten nicht als Verletzungshandlungen. Darüber hinaus lässt sich eine Beurteilung der Marktüblichkeit der beabsichtigten Untersuchungsmaßnahmen noch nicht rechtssicher vornehmen.

3. Barriere des Reverse Engineering

41 Gemäß § 3 Abs. 1 Nr. 2 GeschGehG ist die Erlangung von Geschäftsgeheimnissen durch ein Beobachten, Untersuchen, Rückbauen oder Testen eines Produkts oder Gegenstands erlaubt. Das Produkt oder der Gegenstand muss dabei entweder öffentlich verfügbar gemacht worden sein (lit. a) oder sich im rechtmäßigen Besitz desjenigen befinden, der die entsprechenden Maßnahmen vornimmt (lit. b):

- *Öffentlich Verfügbar (lit. a):* Falls die Software frei auf dem Markt verfügbar ist, gilt ersteres, so dass der Erlaubnistatbestand nach lit. a einschlägig ist und Maßnahmen nach Nr. 2 grundsätzlich zulässig sind.

- *Rechtmäßiger Besitz (lit. b):* Sofern der Lieferant die Software speziell für den Käufer anfertigt und diese nicht auf dem freien Markt anbietet, gilt lit. b. In diesem Fall des rechtmäßigen Besitzes kann die Prüffreiheit auch schon vertraglich beschränkt werden, § 3 Abs. 1 Nr. 2 lit. b GeschGehG.

In der Praxis werden durch den Lieferanten häufig Standard- 42
produkte individualisiert und auf die Bedürfnisse des Kunden zugeschnitten. In diesem Fall ist zwar die Einordnung unter die Tatbestandsalternativen der Nr. 2 nicht eindeutig, im Ergebnis aber unerheblich, da in jedem Fall ein Erlaubnistatbestand erfüllt ist.

Das bedeutet im Hinblick auf die möglichen Untersuchungs- 43
handlungen, dass diese hinsichtlich des Geheimnisschutzes teilweise zulässig sind. Im Rahmen der Überwachung, Systemüberwachung, Leitungsüberwachung und Speicherauslagerung wird das Programm normal ausgeführt, mithin nur beobachtet. Bei Blackbox- sowie Last- und Stresstests werden künstliche Befehle eingegeben, daher sind diese der Prüfung bzw. dem Testen im obigen Sinne zuzuordnen. Dasselbe gilt für den Einsatz von Debuggern. Die Dekompilierung von Software kann als Dekonstruktion bzw. Rückbau eingestuft werden.

Auch ein durch Reverse Engineering gewonnenes Geschäfts- 44
geheimnis darf, anders als nach bisheriger Regelung[53], verwendet werden, sofern es rechtmäßig erlangt wurde. Das Nutzungsverbot aus § 4 Abs. 2 GeschGehG umfasst nur Fälle in denen das Geheimnis rechtswidrig erlangt wurde (gem. Abs. 1, s. 2. oben) oder in denen eine Verpflichtung zur Geheimhaltung besteht. Eine Manipulation und Erweiterung des Quellcodes ist daher nur bei rechtmäßiger Erlangung des Quellcodes zulässig, wenn dieser ein Geheimnis darstellt oder enthält.

IV. Schutz von Software nach dem Patentrecht

Das Patentrecht steht den hier thematisierten möglichen Prü- 45
fungsmaßnahmen nicht im Wege, da die zu prüfende Software

49 *Grohmann*, GRUR-Prax. 2019, 27 (29); *Hiéramente/Golzio*, CCZ 2018, 262 (263); *Hoeren/Münker*, WRP 2018, 150 (152); *von Busekist/Racky*, ZRP 2018, 135 (137).

50 Vgl. etwa *Müllmann*, ZRP 2019, 25 (26); *Partsch*, Stellungnahme zum GeschGehG, verfügbar unter https://www.transparency.de/fileadmin/Redaktion/Aktuelles/Stellungnahmen/2018/18-12-11_Stellungnahme_Umsetzung_der_EU-Richtlinie_zu_GeschGehG.pdf, zuletzt abgerufen 12.3.2019.

51 Siehe *Hoeren/Münker*, WRP 2018, 150 (151); s. *Kalbfus*, GRUR 2016, 1009 (1010).

52 *Hoeren/Münker*, WRP 2018, 150 (152).

53 *Köhler* in Köhler/Bornkamm/Feddersen, UWG, 37. Aufl. 2019, Vorb. §§ 17-19 Rz. 47; *Trebeck/Schulte-Wissermann*, NZA 2018, 1175 (1179).

nach deutschem Recht[54] in der Regel nicht dem Patentschutz unterliegt.

46 Für ein Computerprogramm als solches kann kein Patentschutz erlangt werden; Computerprogramme sind aber dann patentfähig, wenn sie einen technischen Inhalt haben, der über die erforderliche Interaktion mit der Hardware hinausgeht.[55] Als maßgebliches Kriterium dafür wird im Rahmen computerimplementierter Erfindungen überwiegend gesehen, ob die Software neben der Steuerung der Hardware noch eine zusätzliche darüberhinausgehende technische Funktion übernimmt.[56]

47 Handelt es sich um ein nach dem Patentgesetz schutzfähiges Computerprogramm und wurde ein Patent erteilt, so handelt es sich um ein Produktpatent, das es anderen Personen als dem Patentinhaber gem. § 9 Abs. 2 Nr. 1 PatG verbietet, das Produkt herzustellen, zum Verkauf anzubieten, zu vermarkten oder zu verwenden oder es für die vorgenannten Zwecke zu importieren oder zu besitzen.

48 Da die Softwarekopie aber mit Zustimmung des Patentinhabers (Lieferanten) in den Verkehr gebracht wurde, gilt der auch im Patentrecht anerkannte Erschöpfungsgrundsatz[57], so dass der Patentinhaber die Nutzung des jeweiligen Objekts nicht untersagen kann.[58]

49 Außerdem ist das Patent in seiner Wirkung gem. § 11 Nr. 2 PatG eingeschränkt, so dass Handlungen zu Versuchszwecken vorgenommen werden dürfen, die sich auf den Gegenstand der patentierten Erfindung beziehen. Es liegt aber kein Versuch in diesem Sinne vor, wenn nur vorhandene Informationen bestätigt werden sollen.[59]

V. Fazit

50 Die hier beschriebenen Schutzsysteme stehen gleichberechtigt nebeneinander. Computerprogramme können daher gleichzeitigen Schutz mehrerer dieser Systeme genießen.[60] Insbesondere kann die Reverse-Engineering-Barriere nach dem GeschGehG nicht auf die anderen Schutzsysteme übertragen werden. Das ergibt sich bereits aus der Begründung zum seinerzeitigen Gesetzesentwurf.[61] Außerdem besteht in jedem Schutzsystem auch ein differenziertes Barrieresystem, das nicht durch Übertragung systemfremder Barrieren umgangen werden darf.[62] Erwägungsgrund 38 der Geheimhaltungsrichtlinie führt aus, dass die Richtlinie der Anwendung anderer einschlägiger Rechtsvorschriften, einschließlich der Vorschriften des Urheberrechts, nicht entgegensteht.

51 Es zeigt sich, dass eine Vielzahl von Prüfungsmaßnahmen, die zur Erkennung sicherheitsrelevanter Softwarefehler dienen, bestimmungsgemäße Benutzungen i.S.d. § 69d Abs. 1 UrhG sind. Diese Wertung des Urheberrechts gilt es in das neue Geschäftsgeheimnisgesetz und das Patentgesetz zu transferieren, was allerdings nach der differenzierten Regelung des Geschäftsgeheimnisgesetzes sehr schwierig sein dürfte. Hier wird man die weitere Rechtsentwicklung abwarten müssen, um ein einheitliches System des immaterialgüterrechtlichen Schutzes im Hinblick auf die Voraussetzungen und Grenzen der Softwareuntersuchung zu etablieren.

Prof. Dr. Thomas Hoeren

Universitätsprofessor und Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht der Uni Münster (ITM)

Informationsrecht, Urheberrecht, Gewerblicher Rechtsschutz

hoeren@uni-muenster.de

www.uni-muenster.de/jura.itm/hoeren

RA Stefan Pinelli

Leiter der Hauptabteilung Recht Digital im Konzernrechtswesen der Volkswagen AG

Rechtliche Beratung von Digitaltechnologien

54 Eine spannende Frage ist noch, wie sich US-Patente für Software auswirken. Eine Erörterung würde den Rahmen des Aufsatzes sprengen. Gleiches gilt für die Frage, wie die Untersuchungspflichten im Umfeld der DSGVO und von KRITIS unter dem Gesichtspunkt der Informationssicherheit zu betrachten wären.

55 *Bacher* in Benkard, PatG, 11. Aufl. 2015, § 1 Rz. 105.

56 *Baldus* in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 5 Rz. 112; *Osterrieth*, Patentrecht, Rz. 377.

57 Beispielhaft BGH, Urt. v. 26.9.1996 – X ZR 72/94, GRUR 1997, 116 – Prospekthalter; *Scharen* in Benkard, PatG, 11. Aufl. 2015, § 9 Rz. 16.

58 *Schweyer*, The Legal Evaluation of Reverse Engineering in Deutschland und den USA, S. 317.

59 *Scharen* in Benkard, PatG, 11. Aufl. 2015, § 11 Rz. 6.

60 *Triebe*, WRP 2018, 795 (796).

61 RegE S. 24, verfügbar unter https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_GeschGehG.pdf?__blob=publicationFile&v=1, zuletzt abgerufen 12.3.2019.

62 Siehe *Kaboth/Spies* in BeckOK, Urheberrecht, 23. Ed. 15.1.2019, § 69c Rz. 1; s. auch *Triebe*, WRP 2018, 795 (804).