Schriften zum geistigen Eigentum
und zum Wettbewerbsrecht 131

Armin Strobel

Reverse Engineering im Spannungsfeld der Sonderschutzrechte

Eine urheber-, patent- und lauterkeitsrechtliche Analyse
des Reverse Engineering vor dem Hintergrund
des harmonisierten Geheimnisschutzrechts

Nomos

Schriften zum geistigen Eigentum
und zum Wettbewerbsrecht

Herausgegeben von

Prof. Dr. Christian Berger, Universität Leipzig
Prof. Dr. Horst-Peter Götting, Techn. Universität Dresden

Band 131

Armin Strobel

Reverse Engineering im Spannungsfeld der Sonderschutzrechte

Eine urheber-, patent- und lauterkeitsrechtliche Analyse des Reverse Engineering vor dem Hintergrund des harmonisierten Geheimnisschutzrechts

Nomos

Erster Berichterstatter: Prof. Dr. Thomas Hoeren
Zweiter Berichterstatter: Prof. Dr. Jochen Bühling
Dekan: Prof. Dr. Matthias Casper
Tag der mündlichen Prüfung: 13.04.2021

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Münster (Westf.), Univ., Diss. der Rechtswissenschaftlichen Fakultät, 2021

ISBN 978-3-8487-8364-9 (Print)
ISBN 978-3-7489-2747-1 (ePDF)

Onlineversion
Nomos eLibrary

D6

1. Auflage 2022

Vorwort

Das Vorwort meiner Arbeit möchte ich gerne dazu nutzen, mich bei all meinen Unterstützerinnen und Unterstützern für ihre unterschiedlichsten Beiträge zu bedanken. Naturgemäß können dabei an dieser Stelle nur ein paar von ihnen namentlich genannt werden.

Traditionell gilt der erste Dank meinem Doktorvater *Prof. Dr. Thomas Hoeren* für die Möglichkeit zur Erstellung dieser Arbeit und die fortlaufende Betreuung. Auch für die gute Zusammenarbeit in der zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) möchte ich mich auf diesem Wege noch einmal bei allen Beteiligten bedanken. Ich durfte hier nicht nur spannende und lehrreiche Erfahrungen sammeln, sondern in Form meiner dortigen Kolleginnen und Kollegen auch gute Freunde finden. Der schon viel beschriebene Spirit dieses Instituts ist und bleibt besonders.

Anschließen soll sich mein Dank an *Prof. Dr. Jochen Bühling*, der nicht nur die Zweitbegutachtung meiner Arbeit übernommen hat, sondern mit seiner Vorlesung und dem Seminar zum gewerblichen Rechtsschutz auch den Grundstein für mein Interesse an diesem spannenden Rechtsgebiet wesentlich mitgelegt hat.

Prof. Dr. Christian Berger und *Prof. Dr. Horst-Peter Götting, LL.M.* danke ich für die Aufnahme in diese Schriftenreihe.

Der größte und wichtigste Dank gebührt jedoch meinen Eltern *Gisela* und *Gustav*. Sie haben nicht nur den Grundstein für diese Arbeit gelegt, sondern mich in jeder Lebenslage unterstützt und bestärkt. Hierfür empfinde ich nicht nur tiefe Dankbarkeit, sondern auch ein besonderes Glück. Gleiches gilt dabei für meine Brüder und meine Schwägerin.

Besonders hervorheben möchte ich zudem *Dr. Matthias Mörike* und *Dr. Karsten Müller*. Sowohl die fachlichen Anregungen zu meiner Arbeit als auch die gemeinsame Zeit abseits der Bibliothek möchte ich in keinerlei Hinsicht missen.

Dr. Kirsten Krug und *Dr. Franziska Leinemann* danke ich insbesondere für die schnelle und zugleich sorgfältige Durchsicht meines Manuskripts. Die Arbeit wesentlich mitgeprägt haben auch die wertvollen Impulse von *Dr. Julia Dreyer* und *Daniel Ziegenrücker*. *Dipl.-Ing. Roland Adam* und *Heinrich Kenter* haben zudem dafür gesorgt, dass auch der Blick über den juristischen Tellerrand hinaus nicht verloren ging.

Die vielfältige Unterstützung war die Grundlage dafür, dass die Arbeit im Sommersemester 2020 von der Rechtswissenschaftlichen Fakultät der Westfälischen Wilhelms-Universität Münster als Dissertation angenommen wurde. Gesetzgebung, Rechtsprechung und Literatur wurden dabei bis August 2020 berücksichtigt.

Düsseldorf, im Juni 2021 *Armin Dieter Friedrich Strobel*

Inhaltsverzeichnis

Abkürzungsverzeichnis

Kirchner, Hildebert, Abkürzungsverzeichnis der Rechtssprache, 9. Aufl., Berlin 2018.

A. Einleitung

Das Fundament einer innovativen und damit wirtschaftlich erfolgreichen Betätigung eines Unternehmens bildet das Know-how, das dieses von seinen Wettbewerbern abgrenzt.[1] In den Aufbau, die Weiterentwicklung und den Schutz dieses Wissens investieren Unternehmen daher viel Aufwand, Zeit und Geld.[2] Aufgebaut wird das Know-how dabei nicht nur durch Grundlagenforschung, die völlig neues Wissen hervorbringt, sondern auch durch das Übernehmen und Weiterentwickeln von vorherigen Entdeckungen und Erfindungen.[3] Eine in der wirtschaftlichen Praxis gängige Methode des Wissensaufbaus in dieser Form stellt das Phänomen des „Reverse Engineering" dar.[4] Hierbei wird ein Produkt eines anderen Unternehmens detailliert analysiert, um das in dem Produkt verkörperte Wissen aus diesem zu extrahieren. Dadurch kann das analysierende Unternehmen von dem Produkt lernen und das verkörperte Wissen in das unternehmenseigene Know-how aufnehmen. Das so gewonnene Wissen kann dann für

---

1 Köhler/Bornkamm/Feddersen/*Alexander*, Vorbemerkungen GeschGehG Rn. 38; *Liebeskind*, Strategic Management Journal 1996, Vol. 17, 93 (93 f.). Ähnlich außerdem *Wurzer*, CCZ 2009, 49 (49 f.).

2 Allein die Forschungs- und Entwicklungsaufwendungen der Wirtschaft belaufen sich nach dem *Bundesministerium für Bildung und Forschung* im Jahr 2017 auf fast 68,8 Milliarden Euro und im Jahr 2018 auf geschätzte 72,1 Milliarden Euro, Bundesbericht Forschung und Innovation 2020 – Daten und Fakten zum deutschen Forschungs- und Innovationssystem, S. 20 (abrufbar unter: https://www.bundesbericht-forschung-innovation.de/files/BMBF_BuFI-2020_Datenband.pdf, letzter Abruf: 21.8.2020). Die Notwendigkeit einer ausreichenden Schutzstrategie erwähnt außerdem *Wessendorf*, GRUR Int. 2013, 876 (876).

3 So auch *BGH*, Urt. v. 4.11.1966 – Ib ZR 77/65, GRUR 1967, 315 (317) – skai-cubana, mit Anmerkung *Reimer*; Hasselblatt/*Deck*, MAH Gewerblicher Rechtsschutz, Teil D § 17 Rn. 3. Dies an Beispielen deutlich machend *Evans*, Marquette Intellectual Property Law Review 2013, Vol. 17, 61 (87 ff.).

4 So schätzen 67 % der befragten Unternehmen im Maschinen- und Anlagenbau, dass Plagiatoren auf das Reverse Engineering zum Wissensgewinn angewiesen sind, VDMA Studie Produktpiraterie 2018, S. 7 und 17 (abrufbar unter: http://pks.vdma.org/documents/105628/6872272/VDMA+Studie+Produktpiraterie+2018_FINAL.pdf/b465efd1-2d62-4402-813a-896526d18da9, letzter Abruf: 21.8.2020). Außerdem *Ohly*, GRUR 2019, 441 (447).

die eigene Forschungs- und Entwicklungsarbeit weiterverwendet werden.[5] Da ein Produkthersteller aber gleichzeitig daran interessiert ist, das in ein Produkt eingeflossene Know-how vor einem unautorisierten Abfluss zu bewahren,[6] steht das Reverse Engineering in einem Spannungsverhältnis zum unternehmerischen Interesse des Produktherstellers, das eigene Know-how zu schützen.[7] Besonders deutlich wird das, wenn das verkörperte Wissen vom Hersteller bewusst geheim gehalten wird und es damit ein Geschäftsgeheimnis darstellt.[8]

Auch wenn das Reverse Engineering im Wirtschaftsleben ein gängiges Verfahren darstellt, um Informationen aus einem Produkt zu gewinnen, wurde es von der Rechtsprechung bisher als unzulässig eingestuft.[9] Hintergrund ist eine Entscheidung des *Reichsgerichts* aus dem Jahr 1935, die unter dem Namen „Stiefeleisenpresse"-Entscheidung[10] bekannt wurde.

Gegenstand der Entscheidung war eine Auseinandersetzung zwischen zwei Unternehmen über eine Maschine, die in einem Arbeitsschritt gebrauchsfertige Stiefeleisen, also U-förmig gebogene Beschläge für Schuh- und Stiefelabsätze, herstellen konnte.[11] Das klagende Unternehmen stellte eine solche Stiefeleisenpresse bereits seit mehreren Jahrzehnten her und vertrieb diese. Nachdem ein Kunde dieses Unternehmens eine zweite Maschine erwerben wollte und ihm der aufgerufene Preis zu hoch war, wandte er sich an ein zweites, das beklagte, Unternehmen. Dieses sollte eine vergleichbare Maschine herstellen, wobei die der Presse zugehörigen Werkzeuge mit denen der originalen Maschine übereinstimmen sollten. Das beklagte Unternehmen zerlegte daraufhin die bereits im Besitz des Kunden befindliche Stiefeleisenpresse, zeichnete die Einzelteile detailliert ab und fertigte von den dazugehörigen Werkzeugen Abdrücke an. Auf Grundlage dieser Dokumentationen stellte es einen Nachbau der Presse

---

5 Zur ausführlichen Definition des Reverse Engineering siehe Teil B.I.1. Außerdem RegE zum GeschGehG, BT-Drucks. 19/4724, S. 25.

6 *Ann*, GRUR 2014, 12 (12 ff.); *Leister*, GRUR-Prax 2019, 175 (175).

7 Siehe auch *Ohly*, GRUR 2014, 1 (7). Zum Know-how-Schutz als Unternehmensinteresse siehe Köhler/Bornkamm/Feddersen/*Alexander,* Vorbemerkungen GeschGehG Rn. 38 ff.; *Ann*, GRUR 2014, 12.

8 Zu den Voraussetzungen eines Geschäftsgeheimnisses siehe beispielhaft Köhler/Bornkamm/Feddersen/*Alexander,* § 2 GeschGehG Rn. 8 ff.; *Reinfeld,* Das neue Gesetz zum Schutz von Geschäftsgeheimnissen, § 1 Rn. 99 ff.

9 Vergleiche hierzu auch *Harte-Bavendamm*, in: Alexander, et al., FS Köhler, 235 (245 ff.).

10 *RG*, Urt. v. 22.11.1935 – II 128/35, GRUR 1936, 183 – Stiefeleisenpresse.

11 Zum Sachverhalt der Entscheidung siehe *RG*, Urt. v. 22.11.1935 – II 128/35, GRUR 1936, 183 (183 f.) – Stiefeleisenpresse.

her und lieferte sie an den Kunden aus. In seiner rechtlichen Würdigung bewertete das *Reichsgericht* dieses Vorgehen des beklagten Unternehmens als eine sittenwidrige Handlung im Sinne des § 17 Abs. 2 UWG a. F., da es die Konstruktionsart der Stiefeleisenpresse als ein „Betriebsgeheimnis" des klagenden Unternehmens einstufte.[12] Konkret warf es dem beklagten Unternehmen vor, dass die Art der Erlangung der Erkenntnisse durch das Zerlegen und Abzeichnen der Presse die durch „das kaufmännische Anstandsgefühl und die Erfordernisse des redlichen Geschäftsverkehrs gesteckten Grenzen" überschritt.[13]

Die Entscheidung des *Reichsgerichts* legte den Grundstein für eine in Deutschland bis zuletzt anhaltende negative Bewertung des Reverse Engineering.[14] Anknüpfungspunkt der rechtlichen Diskussion um dieses Phänomen war und ist dabei auch zukünftig der rechtliche Schutz von Geschäftsgeheimnissen.[15]

I. Anlass und Ziel der Untersuchung

Im Vergleich zu anderen Rechtsordnungen genoss der Geschäftsgeheimnisschutz in Deutschland lange Zeit keinen besonders hohen Stellenwert.[16] Durch die 2016 in Kraft getretene *Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung*[17] (im Folgenden „Know-how-Schutz-Richtlinie")[18] hat sich dies

12 *RG*, Urt. v. 22.11.1935 – II 128/35, GRUR 1936, 183 (185 ff.) – Stiefeleisenpresse.
13 *RG*, Urt. v. 22.11.1935 – II 128/35, GRUR 1936, 183 (187 f.) – Stiefeleisenpresse.
14 *Witz*, in: Ahrens/Büscher/Goldmann/McGuire, FS Harte-Bavendamm, 441 (441 f.); *Rosenthal/Hamann*, NJ 2019, 321 (325).
15 Statt vieler *Witz*, in: Ahrens/Büscher/Goldmann/McGuire, FS Harte-Bavendamm, 441 (441 ff.).
16 So genoss beispielsweise der Geheimnisschutz in den Vereinigten Staaten von Amerika bisher einen höheren Stellenwert als in Deutschland. Siehe hierzu *Wiebe*, JIPITEC 2011, Vol. 2, 89 (92 f.). Außerdem *Maume*, WRP 2008, 1275 (1275); *McGuire*, GRUR 2015, 424 (424 ff.); *Müller*, InTeR 2014, 65 (65).
17 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. L 157 S. 1.
18 Sofern in dieser Untersuchung außerdem nur von „Richtlinie" gesprochen wird, ist ebenfalls die Know-how-Schutz-Richtlinie gemeint. In Verbindung mit Normangaben wird die Richtlinie außerdem mit „Know-how-Schutz-RL" abgekürzt.

grundlegend geändert. Die Richtlinie ist das Ergebnis mehrjähriger Reformanstrengungen, durch die das Geheimnisschutzrecht unionsweit harmonisiert wurde.[19] Der deutsche Gesetzgeber hat die Know-how-Schutz-Richtlinie mit knapp einem Jahr Verspätung durch das *Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)*[20] umgesetzt und damit das Geheimnisschutzrecht erstmals in einem eigenständigen Stammgesetz verankert.[21]

Teil der Reform ist dabei auch § 3 Abs. 1 Nr. 2 GeschGehG, der Art. 3 Abs. 1 lit. b) Know-how-Schutz-RL umsetzt und die Erlangung eines Geschäftsgeheimnisses durch „ein Beobachten, Untersuchen, Rückbauen oder Testen eines Produkts oder Gegenstands, das oder der a) öffentlich verfügbar gemacht wurde oder b) sich im rechtmäßigen Besitz des Beobachtenden, Untersuchenden, Rückbauenden oder Testenden befindet und dieser keiner Pflicht zur Beschränkung der Erlangung des Geschäftsgeheimnisses unterliegt", erlaubt. In verklausulierter Form wird mit dieser Vorschrift eine Reverse Engineering-Freiheit begründet. Basierend auf den unionsrechtlichen Vorgaben wird damit für das deutsche Geheimnisschutzrecht erstmals und entgegen der bisherigen Rechtsprechung das Reverse Engineering ausdrücklich legalisiert.[22] Für die rechtliche Beurteilung dieses Phänomens geht damit ein Paradigmenwechsel einher.[23]

Trotz dieses grundlegenden Wandels in der Beurteilung des Reverse Engineering erfolgte die Auseinandersetzung mit den sich daraus ergebenden Folgen in der rechtswissenschaftlichen Diskussion sehr verhalten. Da die Legalisierung des Reverse Engineering aber eine im Vergleich zu einer Jahrzehnte andauernden Rechtspraxis entscheidende Änderung und Neuausrichtung des (nationalen) Geheimnisschutzrechts bedeutet sowie darüber hinaus auch Auswirkungen auf andere Rechtsgebiete wie dem Lauterkeitsrecht und die Immaterialgüterrechte haben könnte, soll die vorliegende Untersuchung dieses Diskussionsvakuum ausfüllen. Ziel der Arbeit ist es, unter Berücksichtigung der wirtschaftlichen Gegebenheiten, der Interessen der Beteiligten und der Regelungszwecke der Know-how-Schutz-Richtlinie und des GeschGehG, den Paradigmenwechsel hinsicht-

19 Siehe hierzu *Böhm/Nestler*, GRUR-Prax 2018, 181 (181); *Rauer/Eckert*, DB 2016, 1239 (1239). Siehe außerdem *Falce*, IIC 2015, 940.

20 Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) vom 18. April 2019, BGBl. I 2019, S. 466.

21 Siehe auch *Rosenthal/Hamann*, NJ 2019, 321 (321 f.).

22 *Witz*, in: Ahrens/Büscher/Goldmann/McGuire, FS Harte-Bavendamm, 441 (441 f.); *Dumont*, BB 2018, 2441 (2444); *Leister*, GRUR-Prax 2019, 175 (175 f.).

23 *Dann/Markgraf*, NJW 2019, 1774 (1776); *Redeker/Pres/Gittinger*, WRP 2015, 681 (687); *Voigt/Herrmann/Grabenschröer*, BB 2019, 142 (143).

lich der Reverse Engineering-Freiheit interessengerecht und dogmatisch konsequent in die deutsche Rechtsordnung zu integrieren.

II. Gang der Darstellung

Ausgangspunkt der Analyse des Reverse Engineering unter den neuen rechtlichen Vorzeichen soll dabei eine exakte Bestimmung dessen sein, was unter dem Phänomen zu verstehen ist. Das Reverse Engineering beschreibt einen tatsächlichen Handlungskomplex und wird nicht immer einheitlich abgegrenzt,[24] sodass ohne eine solche Definition keine umfassende und präzise Beurteilung möglich ist. Hierbei gilt es auch die Motive und die Methodik eines solchen Vorhabens zu beachten. Mit einem Blick auf die wirtschaftliche Bedeutung des Reverse Engineering soll zudem das Erfordernis einer rechtlichen Neubewertung unterstrichen werden.[25]

Nachdem die tatsächlichen Grundlagen für eine rechtliche Bewertung gelegt wurden, soll die Reverse Engineering-Freiheit des Geheimnisschutzrechts selbst untersucht werden. Hierbei gilt es, die Voraussetzungen, Ziele und Auswirkungen der Legalisierung auf den Schutz von Geschäftsgeheimnissen zu analysieren. Ein besonderes Augenmerk soll dabei auf die rechtspolitische Rechtfertigung der Reverse Engineering-Freiheit geworfen werden, um zu untersuchen, ob ein so weitreichender Paradigmenwandel im deutschen Geheimnisschutzrecht zu begrüßen ist.[26]

Mit einem Reverse Engineering-Vorhaben zielt die handelnde Person auf Know-how ab, das in einem Produkt verkörpert ist. Bereits in dem „Stiefeleisenpresse"-Urteil entschied das *Reichsgericht*, dass es sich hierbei um „Betriebsgeheimnisse" handeln kann.[27] Da das Reverse Engineering damit oftmals auf ein fremdes Geschäftsgeheimnis und damit den Kern des Geheimnisschutzrechts abzielt, soll vor dem Hintergrund der Reverse Engineering-Freiheit anschließend analysiert werden, ob sich hierdurch die Charakterisierung und Bestimmung eines Geschäftsgeheimnisses ändert.[28]

Aber auch über die Grenzen des Geheimnisschutzrechts hinaus kann die Legalisierung des Reverse Engineering Bedeutung gewinnen. Nicht nur

---

24 Hierzu beispielhaft *Harte-Bavendamm*, GRUR 1990, 657 (658).
25 Zur Definition und Bedeutung des Reverse Engineering siehe Teil B.
26 Zur Reverse Engineering-Freiheit des GeschGehG siehe Teil C.
27 *RG*, Urt. v. 22.11.1935 – II 128/35, GRUR 1936, 183 (185 ff.) – Stiefeleisenpresse.
28 Zu den Auswirkungen auf den Geschäftsgeheimnisbegriff siehe Teil D.II.

im Geheimnisschutzrecht, sondern auch in anderen Rechtsgebieten gibt es Vorschriften, die den Schutz von Know-how betreffen. Insoweit stellt sich die Frage, ob die Beurteilung des Reverse Engineering nach diesen Regelungen durch die Reverse Engineering-Freiheit des GeschGehG eine Änderung erfährt.[29]

Zu Beginn ist dabei das Lauterkeitsrecht in den Blick zu nehmen. Bis zum Inkrafttreten des GeschGehG war der Schutz von Geschäftsgeheimnissen in Deutschland im *Gesetz gegen den unlauteren Wettbewerb (UWG)*[30] geregelt und damit lauterkeitsrechtlich ausgestaltet. Die Reform des Geheimnisschutzrechts und die damit verbundenen inhaltlichen Änderungen wirken sich daher unmittelbar auch auf das Lauterkeitsrecht aus.

Mit dem Einsetzen der Digitalisierung und dem Bedeutungsanstieg des Schutzes von Computerprogrammen rückte außerdem das Urheberrecht in den Fokus der rechtlichen Auseinandersetzung mit dem Reverse Engineering. Da hierbei auch immer wieder auf das Geheimnisschutzrecht Bezug genommen wurde, soll vor dem Hintergrund der geheimnisschutzrechtlichen Neubewertung des Reverse Engineering auch dessen urheberrechtliche Beurteilung einer erneuten Analyse unterzogen werden.

Abschließen soll diesen Komplex ein Blick auf das Patentrecht. Mit dessen technischer Ausrichtung und als Paradebeispiel für ein Immaterialgüterrecht, das einem Reverse Engineering-Vorhaben entgegenstehen könnte, nimmt es für eine rechtliche Analyse des Reverse Engineering-Phänomens eine wichtige Stellung ein.

Abschließend werden die vertraglichen Gestaltungsmöglichkeiten des Reverse Engineering untersucht.[31]

---

29 Zur Beurteilung des Reverse Engineering außerhalb des Geheimnisschutzrechts siehe Teil E.

30 Gesetz gegen den unlauteren Wettbewerb (UWG) in der Fassung der Bekanntmachung vom 3. März 2010, BGBl. I 2010, S. 254. Zuletzt geändert durch Art. 5 Gesetz zur Umsetzung der RL (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung vom 18.4.2019, BGBl. I 2019, S. 466.

31 Zu den vertraglichen Gestaltungsmöglichkeiten siehe Teil F.

B. Bedeutung und Ursprung des Reverse Engineering

Die rechtliche Analyse des Reverse Engineering und dessen Legalisierung durch das GeschGehG und der diesem zugrunde liegenden Know-how-Schutz-Richtlinie setzt zunächst eine Definition des Phänomens voraus. Nur mithilfe eines eindeutigen Begriffsverständnisses, was unter dem Reverse Engineering in praktischer Hinsicht zu verstehen ist, kann eine konsistente und umfassende Würdigung der rechtlichen Fragen rund um das Reverse Engineering erfolgen. Zu berücksichtigen gilt es dabei auch die Motive für ein Reverse Engineering-Vorhaben und die Frage, wie dieses im Einzelfall abläuft oder zumindest ablaufen kann. Außerdem soll ein Blick auf die wirtschaftliche und rechtliche Bedeutung des Know-how-Schutzes und des Reverse Engineering geworfen werden, um die Relevanz einer rechtlichen Auseinandersetzung mit dem Phänomen zu unterstreichen.

I. Definition und Herkunft des Begriffs

Hinsichtlich der Begriffsbestimmung ist zwischen dem Phänomen des Reverse Engineering selbst und der Person, die dieses durchführt, zu unterscheiden.

1. Das Phänomen des Reverse Engineering

Beim Reverse Engineering handelt es sich um keinen feststehenden Rechtsbegriff, der in dieser Form einen weitergehenden Einzug in die deutsche[32] oder unionsrechtliche Rechtsordnung gefunden hat.[33] Auch das reformierte, nationale Geheimnisschutzrecht und die Know-how-Schutz-Richtlinie verwenden den Begriff lediglich in den Gesetzesmaterialien

32 Siehe beispielsweise § 6 Abs. 2 Nr. 2 HalblSchG, der den Sachverhalt des Reverse Engineering regelt, ohne den Begriff zu verwenden. Ebenso § 69e UrhG, der Aspekte des Reverse Engineering aus der urheberrechtlichen Perspektive aufgreift.

33 *Wiese,* EU-Richtlinie über den Schutz vertraulichen Know-hows, S. 30.

beziehungsweise den Erwägungsgründen,[34] nicht aber im Gesetzes- oder Richtlinientext selbst. An einer Legaldefinition fehlt es folglich. Besonders anschaulich wird das an § 3 Abs. 1 Nr. 2 GeschGehG und Art. 3 Abs. 1 lit. b) Know-how-Schutz-RL, die sich materiellrechtlich mit dem Reverse Engineering befassen, ohne die Bezeichnung jedoch konkret zu verwenden.[35]

Es handelt sich beim Terminus des „Reverse Engineering" ursprünglich also nicht um einen rechtlichen Begriff, sondern um eine Bezeichnung aus der Praxis, die tatsächliche Handlungskomplexe beschreibt,[36] welche wiederum einer rechtlichen Würdigung bedürfen. Wörtlich übersetzt, lässt es sich als „umgekehrtes Entwickeln" beschreiben,[37] passender ist jedoch der Begriff der „Produktanalyse".[38] Im Ergebnis geht es darum, ein existentes Produkt zu untersuchen, um die in dem Produkt verkörperten Informationen in Erfahrung zu bringen und so dessen Bestandteile, Funktionsweisen und Herstellungsprozesse nachvollziehen zu können.[39] Beim Reverse Engineering wird also der umgekehrte Weg der Produktion gegangen, bei der aus einer Idee am Ende ein Produkt gefertigt wird.[40] Es handelt sich dabei um ein branchenunspezifisches Phänomen,[41] das auf nahezu jeder Entwicklungsstufe eines Produkts zum Einsatz kommen kann.[42] Unterschieden werden kann zwischen einem „Hardware Reverse Engineering" und einem „Software Reverse Engineering".[43] Bei ersterem ist das Analyseobjekt ein körperliches Produkt wie beispielsweise eine Maschine oder ein Stoffgemisch. Beim Software Reverse Engineering wird

---

34 Siehe EG 16 und 17 Know-how-Schutz-RL; RegE zum GeschGehG, BT-Drucks. 19/4724, S. 25 f.

35 Siehe RegE zum GeschGehG, BT-Drucks. 19/4724, S. 25.

36 *Wiese,* EU-Richtlinie über den Schutz vertraulichen Know-hows, S. 30 und 121 f.; *Harte-Bavendamm*, GRUR 1990, 657 (658).

37 Ähnlich auch *Harlacher,* ReWir 11/2012, S. 4.

38 Vergleiche auch *Lange,* Technologische Konkurrenzanalyse, S. 273.

39 Statt vieler: Köhler/Bornkamm/Feddersen/*Alexander,* § 3 GeschGehG Rn. 24; *Kim,* Der Schutz von Geschäfts- und Betriebsgeheimnissen, S. 113; *Kochmann,* Schutz des „Know-how", S. 43; *Aplin*, Current Legal Problems 2013, Vol. 66, 341 (341 ff.). Speziell auf Computerprogramme bezogen: *Ernst*, MMR 2001, 208 (208 f.).

40 *Ohly*, in: Prinz zu Waldeck und Pyrmont, et al., Patents and Technological Progress, 535 (536); *Ilzhöfer*, CR 1990, 578 (579).

41 *Harte-Bavendamm*, GRUR 1990, 657 (658). Dies auch andeutend *Ohly*, in: Prinz zu Waldeck und Pyrmont, et al., Patents and Technological Progress, 535 (537 f.).

42 So zum Software Reverse Engineering auch *Ilzhöfer*, CR 1990, 578 (579).

43 *Ingle,* Reverse Engineering, S. 32 f.; *Harlacher,* ReWir 11/2012, S. 5 ff.; *Pilny*, GRUR Int. 1990, 431 (437 f.).

hingegen ein Computerprogramm der Analyse unterzogen, sodass das Untersuchungsobjekt ein unkörperliches ist.[44] Die Unterscheidung zwischen diesen beiden Formen des Reverse Engineering dient lediglich der sprachlichen Konkretisierung des jeweiligen Vorhabens, ohne dass sich daraus unmittelbar rechtliche Folgen ergäben.

In Teilen der rechtlichen Auseinandersetzung mit der Thematik wird die Definition des Reverse Engineering auf die Produktanalyse beschränkt.[45] Es muss hierbei jedoch berücksichtigt werden, dass diese in der Regel nicht zum Selbstzweck erfolgt.[46] Die Person, die das Reverse Engineering durchführt,[47] verfolgt meist ein konkretes Ziel und möchte die gewonnenen Erkenntnisse in irgendeiner Form für sich fruchtbar machen.[48] Aus diesem Grund sollen dem Begriffsverständnis in dieser Untersuchung nicht nur die Analysehandlungen, sondern auch die Verwertung der dadurch gewonnenen Informationen zugrunde gelegt werden.[49] Erfasst ist also auch das sogenannte „Forward Engineering", das teilweise und insbesondere im Softwarebereich als Fachterminus für die Verwertung der gewonnenen Informationen verwendet wird.[50] Da das Phänomen des Reverse Engineering aber schon deutlich älter als die Digitalisierung ist,[51] bietet sich eine Orientierung an dieser Unterscheidung nicht an. Durch ein vollumfängliches Verständnis des Reverse Engineering, das sowohl die Analyse als auch die anschließende Informationsverwertung erfasst, kann vielmehr eine ganzheitliche Bewertung des Phänomens aus der rechtlichen Perspektive erfolgen, ohne dass ein in der Praxis als Gesamtkomplex auftretender Sachverhalt künstlich auseinandergerissen wird.

---

44 *Kochmann,* Schutz des „Know-how", S. 43.

45 *Kochmann,* Schutz des „Know-how", S. 43 f. In diese Richtung lässt sich auch Büscher/*McGuire,* § 3 GeschGehG Rn. 19 verstehen.

46 So auch Harte-Bavendamm/Ohly/Kalbfus/*Ohly,* § 3 GeschGehG Rn. 20; *Schweyer,* Die rechtliche Bewertung des Reverse Engineering, S. 2.

47 Diese Person kann als „Reverser" bezeichnet werden. Siehe zur Definition auch Teil B.I.3.

48 Zu den Motiven eines Reverse Engineering-Vorhabens siehe Teil B.II.1.

49 So auch *Aigner,* Die Geschäftsgeheimnis-Richtlinie, S. 24; *Schweyer,* Die rechtliche Bewertung des Reverse Engineering, S. 1 f.; *Haberstumpf*, CR 1991, 129 (129). Im Ergebnis wohl auch *Schnell/Fresca*, CR 1990, 157 (157), die eine Aufteilung der beiden Ebenen zumindest andeuten.

50 Siehe auch *Eilam,* Reversing, S. 3 f. Eine Unterscheidung beispielsweise vornehmend, aber nicht abschließend: *Kochmann,* Schutz des „Know-how", S. 44; *Chikofsky/Cross*, IEEE Software 1990, Vol. 7, 13 (14 f.).

51 *Eilam,* Reversing, S. 3. Siehe zum Ursprung des Reverse Engineering außerdem Teil B.I.2.

Als Grundlage dieser Untersuchung ergibt sich für das Reverse Engineering daraus die folgende, zweiteilige Definition:

> *„Reverse Engineering" ist die Analyse eines existenten Produkts, um die in diesem verkörperten Informationen in Erfahrung zu bringen und so dessen Bestandteile und Funktionsweisen nachvollziehen zu können (1. Ebene), und die anschließende Verwertung der auf diesem Wege ermittelten Informationen (2. Ebene).*

Unbeschadet dieses weiten Begriffsverständnisses kann bei der rechtlichen Beurteilung des Reverse Engineering im Einzelnen hinsichtlich der beiden Ebenen weiterhin differenziert werden.

2. Ursprung des Reverse Engineering

Der historische Ursprung des Reverse Engineering in tatsächlicher Hinsicht lässt sich nicht sicher bestimmen. Die Untersuchung von Produkten, um ihre Zusammensetzung und Funktionsweise zu verstehen, ist ebenso so alt wie die Herstellung von Waren und Gütern selbst.[52] Jedenfalls lässt sich das Konzept aber bis auf die Zeit der industriellen Revolution zurückführen.[53]

Die Bezeichnung als „Reverse Engineering" wurde hingegen aus den Vereinigten Staaten von Amerika übernommen,[54] wo es als Bestandteil des *fair use*-Grundsatzes gilt und durch den *U.S. Supreme Court*[55] höchstrichterlich definiert wurde und erlaubt ist.[56] In der deutschen Rechtsprechung trat das Phänomen des Reverse Engineering erstmals 1935 durch das bereits erwähnte „Stiefeleisenpresse"-Urteil[57] des *Reichsgerichts* bedeutsam in Erscheinung, wobei natürlich nicht diese Begrifflichkeit verwendet wurde.

---

52 *England and Wales High Court (Patents Court)*, Urt. v. 11.6.1999, FSR 138 (2000) – Mars UK Ltd. v. Teknowledge Ltd.; *Eilam,* Reversing, S. 3 f.; *Ohly*, in: Prinz zu Waldeck und Pyrmont, et al., Patents and Technological Progress, 535 (535).

53 *Eilam,* Reversing, S. 3; *Harlacher,* ReWir 11/2012, S. 2. Die lange Historie des Reverse Engineering außerdem ansprechend *Samuelson/Scotchmer*, The Yale Law Journal 2002, Vol. 111, 1575 (1577 f.).

54 *Schweyer,* Die rechtliche Bewertung des Reverse Engineering, S. 1 und 5.

55 *U.S. Supreme Court*, Urt. v. 13.5.1974 – No. 73-187, 416 U.S. 470 (476) – Kewanee Oil Co. v. Bicron Corp.

56 Siehe auch *Samuelson/Scotchmer*, The Yale Law Journal 2002, Vol. 111, 1575 (1577 f.).

57 *RG*, Urt. v. 22.11.1935 – II 128/35, GRUR 1936, 183 – Stiefeleisenpresse. Siehe hierzu auch Teil A.

Beginnend mit dem *Halbleiterschutzgesetz (HalblSchG)*[58] erlebte die Thematik durch die Verabschiedung der *Richtlinie über den Rechtsschutz von Computerprogrammen (Computerprogramm-Richtlinie)*[59] im Jahr 1991 vor dem Hintergrund des Urheberrechts einen Aufschwung.[60] Hierbei etablierte sich auch in Deutschland die Begrifflichkeit des Reverse Engineering in der rechtlichen Diskussion.

3. Der Reverser

Anders als für das Reverse Engineering selbst gibt es für die Person, die dieses durchführt, keine einheitliche oder zumindest verbreitete Bezeichnung. Um dennoch eine griffige Benennung dieser Person zu ermöglichen, soll sie in Anlehnung an *Eilam* und *Kochmann* als „Reverser" bezeichnet werden.[61]

Des Weiteren sind im Einklang mit § 3 Abs. 1 Nr. 2 GeschGehG nur Fälle des Reverse Engineering Gegenstand dieser Untersuchung, bei denen das Analyseobjekt öffentlich verfügbar gemacht wurde oder anderweitig in den rechtmäßigen Besitz des Reversers gelangt ist.[62] Ansonsten droht schon durch die unrechtmäßige Inbesitznahme des Analyseobjekts durch den Reverser eine Rechtsverletzung.[63]

---

58 Gesetz über den Schutz der Topographien von mikroelektronischen Halbleitererzeugnissen (Halbleiterschutzgesetz – HalblSchG) vom 22. Oktober 1987, BGBl. I 1987, S. 2294. Zuletzt geändert durch Art. 12 Gesetz zur Änderung des BundesversorgungsG und anderer Vorschriften vom 17.7.2017, BGBl. I 2017, S. 2541.

59 Richtlinie 91/250/EWG des Rates vom 14. Mai 1991 über den Rechtsschutz von Computerprogrammen, ABl. L 122 S. 42.

60 *Schweyer,* Die rechtliche Bewertung des Reverse Engineering, S. 10 f. Siehe außerdem beispielhaft *Haberstumpf*, CR 1991, 129; *Ilzhöfer*, CR 1990, 578; *Schnell/Fresca*, CR 1990, 157.

61 *Eilam,* Reversing, S. 10; *Kochmann,* Schutz des „Know-how", S. 43.

62 Zu den einzelnen Voraussetzungen der geheimnisschutzrechtlichen Reverse Engineering-Freiheit siehe Teil C.I.

63 *Schweyer,* Die rechtliche Bewertung des Reverse Engineering, S. 4 f.; *Wiese,* EU-Richtlinie über den Schutz vertraulichen Know-hows, S. 122 f.; *Uhrich*, Michigan Telecommunications and Technology Law Review 2001, Vol. 7, 147 (155 ff.).